HÖGSKOLAN DALARNA

Examensarbete

Kandidatuppsats

Rollbaserad åtkomstkontroll med geografisk avgränsning

En systematisk litteraturgenomgång av det befintliga kunskapstillståndet inom ämnesområdet

Författare: Jerker Andersson

Handledare: Pär Douhan och Johan Håkansson

Examinator: Bo Sundgren

Ämne/huvudområde: Informatik

Kurskod: IK2017

Poäng: 15 hp

Ventilerings-/examinationsdatum: 3 juni 2015

HÖGSKOLAN DALARNA

EXAMENSARBETE
Grundnivå 2 i Informatik

Rollbaserad åtkomstkontroll med geografisk avgränsning

- En systematisk litteraturgenomgång av det befintliga kunskapstillståndet inom ämnesområdet

Ämne:
Informatik, grundnivå 2

Omfattning:
15 högskolepoäng

Författare:
Jerker Andersson

Månad/år:
juni 2015

Examinator:
Bo Sundgren

Handledare:
Pär Douhan och Johan Håkansson

Samarbetspartner:
Triona

Handledare hos samarbetspartner:
Anna Mårsell

Nyckelord: *Rollbaserad åtkomstkontroll*, *RBAC, geografisk avgränsning, spatial avgränsning, säkerhet*

Sammanfattning

Rollbaserad åtkomstkontroll är en standardiserad och väl etablerad modell för att hantera åtkomsträttigheter i informationssystem. Den vedertagna ANSI-standarden 359-2004 saknar dock stöd för att geografiskt avgränsa rollbehörigheter. Informationssystem som behandlar geografiska data och de senaste årens ökade spridning av mobila enheter påkallar ett behov av att sådana rumsliga aspekter diskuteras inom kontexten av rollbaserad åtkomstkontroll. Arbetet syftar till att bringa klarhet i hur det befintliga kunskapstillståndet inom ämnesområdet rollbaserad åtkomst kontroll med geografisk avgränsning ser ut, och vilka aspekter hos detta som står i behov av vidare utveckling. Genom de teoretiska referensramar som skapats vid inledande litteraturstudier har en efterföljande systematisk litteraturgenomgång möjliggjorts, där vetenskapligt material selekterats genom fördefinierade urvalskriterier. Sammanställningen och analysen av den systematiska litteraturgenomgångens resultat har i samverkan med de teoretiska referensramarna lett fram till arbetets huvudsakliga kunskapsbidrag: en områdesöversikt där ämnets *state-of-the-art* presenteras och en strukturerad lista över angelägna forsknings- och utvecklingsbehov inom området.

Abstract

Role-based Access Control is a standardized and well established model in terms of handling access rights. However, the accepted ANSI standard 359-2004 lacks the support of geographically delimiting role authorizations. Information systems handling geographical data together with the increasing use of mobile devices call for a need to discuss such spatial aspects within the context of Role-Based Access Control. This thesis seeks to shed light on the current state of knowledge within the subject area as well as to identify aspects of it that are in need of further development. The theoretical framework conceived by the initial literature review has made the conduction of a systematic literature review possible, and the synthesis and analysis of the data together with the theoretical framework have led to the work's contributions of knowledge: an overview of the subject where the state-of-the art in the area is presented and a structured list of desirous needs of research and development within the area of study.

Förord

Arbetet har genomförts som ett examensarbete på kandidatnivå på Systemvetenskapliga programmet vid Högskolan Dalarna under våren 2015. Examensarbetets omfattning har varit 15 högskolepoäng eller tio veckors heltidsstudier.

Jag vill framföra ett stort tack till Anna Mårsell, min handledare på samarbetspartnern Triona, som varit till mycket stor hjälp när hon noggrant granskat det jag skrivit och bidragit med synpunkter på detta. Jag vill också tacka mina handledare på Högskolan Dalarna, Pär Douhan och Johan Håkansson, som hjälpt mig styra uppsatsen mot ett godkännande! Tack så mycket!

Borlänge, juni 2015

Jerker Andersson

Figurförteckning

Tabellförteckning

1. Inledning

I inledningskapitlet ges en grundläggande introduktion till arbetets ämnesområde, i avsikt att förbättra läsarens grund för att följa med rapportens efterföljande kapitel. Här specificeras också arbetets problemformulering och de frågor som arbetet ämnar besvara.

1.1 Bakgrund

För en ensam datoranvändare finns inget behov av åtkomstkontroll. Användaren äger själv sina filer och kan läsa, förändra, eller dela dessa med andra efter sina egna önskemål. När användaren börjar arbeta i ett informationssystem med stöd för flera användare uppstår dock behov för att skydda data och begränsa åtkomsten till denna. Kanske vill användaren inte att andra ska kunna läsa dennes filer, och förmodligen inte att andra ska kunna förändra innehållet i dem. Även om systemets alla användare är pålitliga nog att hålla sig borta från andra användares data kan misstag ske, och det kan vara lätt hänt att en användare tar bort eller förändrar innehållet i en annan användares fil i tron att filen är hans egen. Att begränsa och kontrollera användares behörighet med åtkomstkontroll skyddar mot liknande olyckor. (Lehtinen, Russell, & Gangemi Sr., 2011)

Åtkomstkontroll kan te sig på många olika sätt, och förutom att bedöma en användares åtkomsträttigheter till en resurs i ett informationssystem kan åtkomstkontroll också användas för att begränsa när och hur användarens åtkomst är tillåten. Exempelvis kan en organisation begränsa vissa eller alla användares åtkomst till vissa resurser att endast gälla under kontorstid, eller kräva att högriskoperationer måste utföras av två användare tillsammans. (Ferraiolo, Kuhn, & Chandramouli, Role-Based Access Control, 2007)

Som en följd av fleranvändarsystemens framväxt och det ökade militära beroendet av sådana började U.S. Defense Science Board i slutet av 1960-talet att undersöka systemens sårbarhet. Åtkomstkontrollens utveckling tog fart när det amerikanska försvarsdepartementet 1983 publicerade standarden *Trusted Computer System Evaluation Criteria*, i vilken två åtkomstkontrollmodeller definierades; diskretionär åtkomstkontroll och obligatorisk åtkomstkontroll. I den diskretionära åtkomstkontrollen fördelas åtkomsträttigheter av respektive fils skapare, medan de i den obligatoriska åtkomstkontrollen avgörs av användarens och filens säkerhetsgrad. (Ferraiolo, Kuhn, & Chandramouli, Role-Based Access Control, 2007)

Rollbaserad åtkomstkontroll introducerades i början av 1990-talet och har sedan dess växt till att bli en av de åtkomstkontrollmodeller som diskuterats flitigast i den akademiska världen, och American National Standards Institute godkände 2004 modellen som en standard i och med ANSI 359-2004 (Franqueira & Wieringa, 2012). Modellen för rollbaserad åtkomstkontroll bygger på att tjänstebefattningar eller arbetsområden i en organisation representeras av roller, vilka tilldelas behörigheter istället för enstaka användare. De behörigheter som tilldelas en roll ska direkt baseras på det behov som finns för att utföra de arbetsuppgifter som hör till rollen. Genom att använda roller förenklas arbetet med att hantera åtkomstbehörigheter och den administrativa kostnaden minskas (Bertino, RBAC models - concepts and trends, 2003). I en ekonomisk analys förutspås att ”*just over 50 % of users at organizations with more than 500 employees are expected to have at least some of their permissions managed via roles”* (O'Connor & Loomis, 2010, s. 77).

Geografiska data har en strategisk relevans på många områden (Belussi, Bertino, Catania, Daminani, & Nucita, 2004), och geografiska informationssystem som baseras på att sådan information som sedvanligt finns i kartor istället lagras i digitala databaser med hjälp av koordinater har utvecklats sedan 1980-talet. Sådana system möjliggör inmatning, lagring, bearbetning och presentation av geografiska data med hjälp av datorer. Geografiska informationssystem ombesörjs i Sverige av bland

annat myndigheter, kommuner, Lantmäteriet och SMHI (Wennström, 2015). Som ett exempel på ett sådant system kan nämnas NVDB (Nationell vägdatabas), som administreras av Trafikverket i samarbete med Sveriges Kommuner och Landsting, skogsnäringen, Transportstyrelsen och Lantmäteriet. NVDB tillhandahåller samlade digitala uppgifter för Sveriges vägar, som exempelvis väghållare och högsta tillåtna hastighet (NVDB, u.d.). I ett förstadium till arbetet har den åtkomstkontroll med geografisk avgränsning som finns kring NVDB och de egenheter som en sådan avgränsning kan medföra studerats. Vid de leveranser av data som sker till NVDB har det uppenbarat sig vissa teoretiska problem som kan uppstå kring rollbaserad åtkomstkontroll med geografisk avgränsning, vilket kan exemplifieras med den områdesavgränsning som föreligger i följande typfall:

Användare A med behörighet för Borlänge kommun checkar ut en liten delmängd av vägnätet. Användare A gör förändringar som innebär att en del av vägnätet hamnar i angränsande Falu kommun, där användare A saknar skrivrättigheter.
Användare A bör (med geografiskt avgränsad åtkomstkontroll) inte få checka in resultatet.

1.2 Problemformulering

Rollbaserad åtkomstkontroll är idag en (både akademiskt och kommersiellt) välkänd och frekvent diskuterad modell för att hantera åtkomstbehörigheter i informationssystem, och sedan modellen 2004 godkänts som en ANSI-standard har dess tillämpning ökat (Franqueira & Wieringa, 2012). Även om området kring rollbaserad åtkomstkontroll har behandlats grundligt de senaste årtiondena har dock inte de aspekter som kontrollen av åtkomst till geografiska data frambringar studerats lika ingående (Belussi, Bertino, Catania, Daminani, & Nucita, 2004). De senaste årens framväxt av mobila enheter har dock bidragit till ett ökat fokus på användarpositionsbaserad åtkomstkontroll (Kirkpatrick, Damiani, & Bertino, Prox-RBAC: A Proximity-based Spatially Aware RBAC, 2011). Dock saknas, mig veterligen, idag en överskådlig områdesöversikt som sammanställer och påvisar den kunskap som idag finns på området, liksom en strukturerad framställning över de av områdets delar som står i behov att vidare utvecklas och forskas kring.

1.3 Syfte

Arbetets syfte är att genom en systematisk litteraturgenomgång med internationellt fokus beskriva det kunskapstillstånd i vilket ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning idag befinner sig i, och genom detta identifiera och beskriva beaktansvärda forsknings- och utvecklingsbehov som finns inom området.

Med detta som bakgrund har följande frågor formulerats:

> *Vad är idag ”state-of-the-art” inom ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning?*
>
> *Vilka forsknings- och utvecklingsbehov finns idag inom ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning?*

1.4 Avgränsning

Då en systematisk litteraturgenomgång är beroende av tillgång till relevant material behandlas i studien enbart sådana verk som funnits tillgängliga via Internet under den avgränsade tidsperiod då arbetet utförts. Arbetet ämnar beskriva det nuvarande kunskapstillståndet kring ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning, varför en tidsmässig avgränsning för det material som granskats varit nödvändig. Under arbetets gång har beslutet fattats att under den systematiska litteraturgenomgången endast studera sådana verk som publicerats under de senaste 25 åren, sedan 1990. Samtliga verk som inkluderats i studien måste också ha genomgått en kollegial granskning.

1.5 Disposition

Nedan följer en beskrivning av arbetets disposition, där varje kapitel ges en kortfattad förklaring.

Kapitel 1 – Inledning	Det inledande kapitlet redogör kort för ämnets bakgrund, och genom resonemang kring problematisering av ämnet presenteras den frågeställning som arbetet har för avsikt att besvara, liksom det syfte i vilket arbetet genomförs.
Kapitel 2 – Teori	I arbetets andra kapitel ges en litteraturgenomgång, där sådana teoretiska begrepp som är av vikt för en vidare förståelse i den fortsatta läsningen av arbetet förklaras.
Kapitel 3 – Metod	Det tredje kapitlet beskriver det strukturerade tillvägagångssätt vilket arbetets framtagande följt, liksom hur datainsamlingen och dataanalysen genomförts.
Kapitel 4 – Empiri	De empiriska data som utgör datainsamlingens resultat, i studien inkluderat vetenskapligt material, presenteras i det fjärde kapitlet.
Kapitel 5 – Analys	Den teoretiska referensram som bildats under litteraturgenomgången ställs i förhållande till arbetets empiriska data under en kvalitativ dataanalys som framställs i det femte kapitlet.
Kapitel 6 – Slutsatser	Arbetets egentliga avslutning finns i det sjätte kapitlet, i och med de resultat som arbetet i sin helhet landat i. Resultatet står i begrepp att besvara arbetets frågeställning, som presenterats i det första kapitlet. Uppsatsen avslutas med en diskussion kring slutsatserna och en kritisk utvärdering av det tillvägagångssätt som använts.
Referenser	Samtliga källor som refererats till i arbetet presenteras.
Bilagor	Sist i arbetet bifogas de bilagor som en läsare kan behöva, men vilka inte lämpar sig att placeras i själva arbetet.

2. Teori

I teorikapitlet sker en litteraturgenomgång på ämnesområdet åtkomstkontroll och rollbaserad åtkomstkontroll. Kapitlet presenterar också en introduktion till geografiska data.

2.1 Introduktion till åtkomstkontroll

För att underlätta förståelsen för det vidare arbetet finns i detta avsnitt en genomgång av hur litteraturen beskriver ämnet åtkomstkontroll.

2.1.1 Åtkomstkontrollens terminologi

Under de senaste decennierna har en tämligen homogen terminologi för att beskriva åtkomstkontroll utvecklats, och nästan alla åtkomstkontrollmodeller kan idag förklaras med begreppen *användare*, *subjekt*, *objekt*, *operation*, och *behörighet*. För en vidare förståelse för åtkomstkontrollen krävs en uppfattning av dessa begrepp, eftersom de är vanligt förekommande i den mesta litteraturen inom åtkomstkontroll. (Ferraiolo, Kuhn, & Chandramouli, Role-Based Access Control, 2007)

Användare Refererar till en människa som interagerar med informationssystemet. En enda användare kan ha flera olika användarkonton, även om autentisering kan göra det möjligt att härleda dessa till samma person. En instans av en användares dialog med systemet kallas *session*. (Ferraiolo, Kuhn, & Chandramouli, Role-Based Access Control, 2007)

Subjekt En datorprocess som agerar på begäran av en användare. I verkligheten genomförs dock samtliga av en användares handlingar genom mjukvaruprogram som körs på datorn. En användare kan ha flera olika subjekt verksamma på samma användarkonto vid samma tidpunkt och session. Till exempel kan ett e-postprogram arbeta i bakgrunden genom att med jämna mellanrum hämta e-post från en server, samtidigt som användaren arbetar i en webbläsare. Varje program som användaren nyttjar är ett subjekt, och varje programs åtkomster kontrolleras för att säkerställa att användaren som kör programmet har tillstånd att utföra handlingen. (Ferraiolo, Kuhn, & Chandramouli, Role-Based Access Control, 2007)

Objekt Samtliga resurser som finns åtkomliga i ett informationssystem. Det kan handla om filer, skrivare, databaser, eller till och med enskilda fält i en databas. Objekt brukar anses vara passiva enheter, som antingen innehåller eller tar emot information. (Ferraiolo, Kuhn, & Chandramouli, Role-Based Access Control, 2007)

Operation En aktiv process som anropas på begäran av ett subjekt. Tidiga åtkomstkontroll-modeller som endast behandlade informationsflöde (läs- och skrivrättigheter) benämnde alla aktiva processer *subjekt*, men rollbaserad åtkomstkontroll kräver att begreppen subjekt och operation skiljs åt. Ett exempel är när en bankkund matar in sitt bankomatkort och en korrekt pinkod i en bankomat. Subjektet är då kontrollprogrammet som agerar på användarens begäran, som i sin tur kan initiera operationer – uttag, insättning, saldo. (Ferraiolo, Kuhn, & Chandramouli, Role-Based Access Control, 2007)

Behörighet Befogenhet att utföra en viss handling i systemet, och med *behörighet* menas vanligtvis en kombination av objekt och operation. En viss operation som utförs på två olika objekt representerar två olika behörigheter, på samma sätt representerar två operationer som utförs på samma objekt två olika behörigheter. Exempelvis kan en kassör i en bank ha behörighet att utföra operationerna kredit och debet på

kundkonton, medan en revisor kan ha behörighet att utföra kredit- och debetoperationer på den huvudbok som innehåller bankens redovisningsmässiga data. Behörigheter kan också kallas *privilegier*. (Ferraiolo, Kuhn, & Chandramouli, Role-Based Access Control, 2007)

2.1.2 Autentisering och auktorisering

För att förstå åtkomstkontroll är det av stor vikt att känna till, och kunna skilja på, begreppen *autentisering* och *auktorisering*. Autentisering är den process som fastställer om en användare egentligen är den som denne påstår sig vara. I informationsteknologiska sammanhang sker autentisering vanligtvis genom att logga in med hjälp av ett lösenord, och användarens kännedom om lösenordet förutsätts vara en försäkran att användaren i själva verket är autentisk. Denna autentiseringsmetod medför dock svagheten att ett lösenord kan bli stulet, avslöjat eller glömt. (Mutch & Anderson, 2011)

Autentiseringens skydd kan förstärkas vid användandet av två eller fler faktorer vid autentiseringsprocessen, exempelvis kräver ett besök vid en bankomat vanligtvis att bankkunden matar in både ett bankomatkort och ett personligt identifieringsnummer, PIN-kod. (Ferraiolo, Kuhn, & Chandramouli, Role-Based Access Control, 2007)

Auktorisering är den process där en autentiserad användare ges behörighet att komma åt viss information eller funktionalitet, baserat på redan fördefinierade behörighetsprinciper. Till exempel kan en användare som arbetar vid en viss avdelning hos ett företag endast vara auktoriserad åtkomst till den funktionalitet och information som denne behöver för att utföra sitt arbete på avdelningen. När den autentiserade användaren begär att få utföra en operation kontrollerar systemet att användaren är auktoriserad innan operationen antingen accepteras eller avslås. (Mutch & Anderson, 2011)

2.1.3 Least privilege

I syfte att bevara ett informationssystems dataintegritet anses principen om *Least Privilege* vara en viktig del. Principen innebär att en användare inte ska tilldelas fler privilegier än vad som är nödvändigt för att kunna utföra sitt arbete, det vill säga att användaren endast auktoriseras åtkomst till den information och den funktionalitet som behövs för att utföra dennes arbetsuppgifter. För att kunna upprätthålla Least Privilege-principen krävs att respektive användares arbetsuppgifter identifieras, för att sedan ligga till grund för en samling privilegier som arbetsuppgifternas utförande kräver. Genom att använda rollbaserad åtkomstkontroll underlättas upprätthållandet av Least Privilege-principen. (Ferraiolo & Kuhn, 1992)

2.1.4 Diskretionär åtkomstkontroll

Åtkomstkontroll är inte ett enhetligt fenomen, utan kan snarare utformas på olika vis. Den *diskretionära åtkomstkontrollen* (Discretionary Access Control, DAC) begränsar åtkomsten till objekt baserat på en användares identitet eller grupptillhörighet. Diskretionär åtkomstkontroll tillåter användare med åtkomstbehörighet till ett visst objekt att föra denna åtkomstbehörighet vidare (också indirekt) till en annan användare. (DoD, 1985)

Den användare som skapar ett objekt är också ägare av objektet med behörighet att läsa och förändra objektet och dess innehåll, samt med beslutsrätt att delegera rättigheter till andra användare, användargrupper, eller att göra objektet åtkomligt för samtliga användare. (Lehtinen, Russell, & Gangemi Sr., 2011)

2.1.5 Obligatorisk åtkomstkontroll

Den *obligatoriska åtkomstkontrollen* (Mandatory Access Control, MAC) begränsar åtkomsten till objekt baserat på känslighetsgrad hos den information som det specifika objektet innehåller, och den formella befogenheten hos användaren som utför en åtkomstbegäran. (DoD, 1985)

Samtliga både objekt och användare i systemet måste märkas med känslighetsgrad, vilken för en användare är att betrakta som graden av behörighet. Ett objekts känslighetsgrad anger vilken känslighetsgrad en användare måste inneha för att beredas åtkomst till objektet. Obligatorisk åtkomstkontroll är på grund av sin strikta natur lämplig för informationssystem som behandlar särskilt känsliga data, till exempel sekretessbelagd information eller företagshemligheter. (Lehtinen, Russell, & Gangemi Sr., 2011)

2.2 Rollbaserad åtkomstkontroll

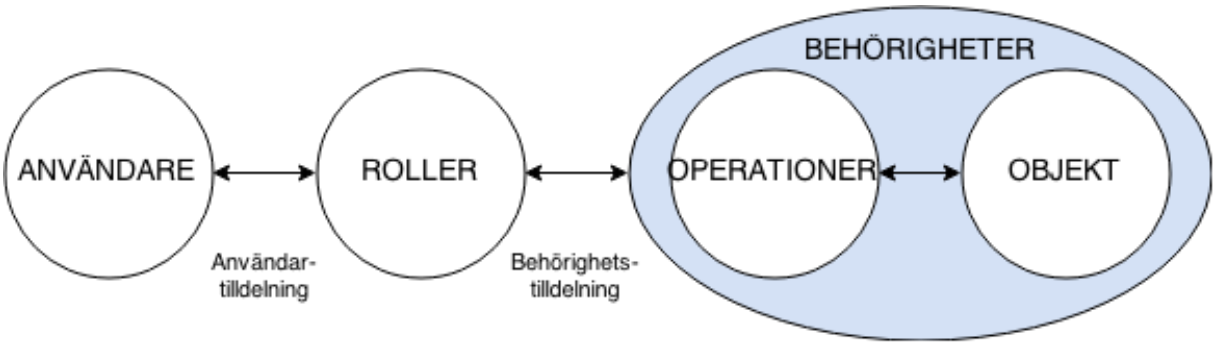
I nittiotalets början uppdagades att befintliga åtkomstkontrollmodeller inte tillfredsställde de behov som fanns, varken i kommersiella eller statliga organisationer. I många av organisationerna var slutanvändare inte alls ägare till den information som de bereddes åtkomst till enligt diskretionär åtkomstkontroll, och obligatorisk åtkomstkontroll ansågs ha ett för starkt fokus på att upprätthålla sekretess. (Ferraiolo, Kuhn, & Chandramouli, Role-Based Access Control, 2007)

De traditionella modellerna för åtkomstkontroll kunde också vara svåra att administrera, och i system som tillämpar dessa ökar antalet befogenhetskonfigureringar i takt med att antalet objekt och subjekt i systemet ökar. Är subjektbeståndet dessutom föränderligt krävs många operationer för att bevilja eller återkalla auktoriseringar. (Bertino, RBAC models - concepts and trends, 2003)

För att åtgärda de upplevda problemen introducerades modellen för rollbaserad åtkomstkontroll 1992 under benämningen *Role-Based Access Control*, eller *RBAC* (Ferraiolo & Kuhn, Role-Based Access Controls, 1992). Efter vidare arbete av Sandhu et al. (1996) resulterade modellen i sammanställningen av en officiell standard, ANSI/INCITS 359-2004 (Franqueira & Wieringa, 2012). Begreppet *roll* fyller en central funktion i rollbaserad åtkomstkontroll, och definieras i standarden som:

> *"A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned the role."* – ANSI 359-2004 (2004, s. 2)

Den rollbaserade åtkomstkontrollmodellen innehåller fem grundläggande dataelement; *användare*, *roller*, *objekt*, *operationer*, och *behörigheter*. Användare tilldelas roller och roller tilldelas behörigheter, varför roller kan anses utgöra ett medel för att benämna *många till många*-förhållanden mellan enskilda användare och behörigheter, vilket illustreras av de dubbelsidiga pilarna i figur 1 nedan. (ANSI, 2004)



Figur 1: Kärnan i rollbaserad åtkomstkontroll. Översatt från ANSI 359-2004 (2004)

I standarden definieras även ett tillägg vilket gör det möjligt för den rollbaserade åtkomstmodellen att stödja rollhierarkier där roller kan struktureras hierarkiskt för att spegla en organisations reella befattningshierarki. Rollhierarki bidrar till att undvika duplicering av behörigheter, då en roll kan ärva de behörigheter som en roll på lägre nivå i hierarkin innehar. Arvskedjan utgår från botten av hierarkin. (ANSI, 2004)

Franquiera och Wieringa (2012) beskriver att standarden för rollbaserad åtkomstkontroll kan brytas ned i åtta grundläggande särdrag, fördelat på tre kategorier:

Obligatoriska särdrag hos grundläggande rollbaserad åtkomstkontroll

1. Enbart roller tilldelas behörigheter. En behörighet kan aldrig tilldelas en användare direkt.
2. Det råder ett många till många-förhållande mellan användare och roller.
3. Det råder ett många till många-förhållande mellan roller och behörigheter.
4. Alla roller behöver inte alltid vara aktiverade hos en användare.
5. Användare kan ha fler än en roll aktiverad vid samma tidpunkt.

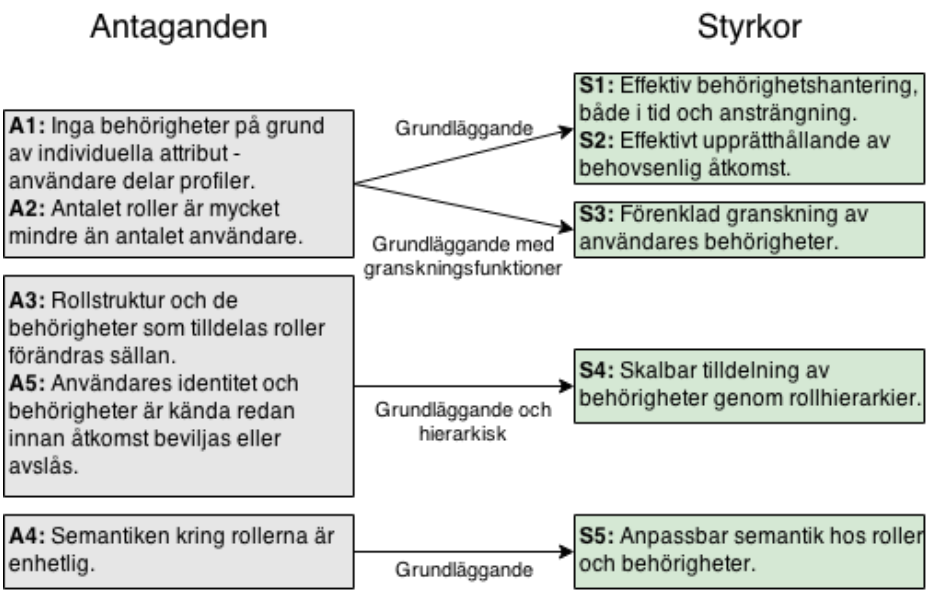
Obligatoriska översiktsfunktioner hos grundläggande rollbaserad åtkomstkontroll

6. Det är möjligt att få en översikt över samtliga användare som tilldelats en viss roll.
7. Det är möjligt att få en översikt över samtliga roller som en viss användare tilldelats.

Icke obligatoriska särdrag hos hierarkisk rollbaserad åtkomstkontroll

8. Roller kan organiseras i hierarkier, i vilka behörigheter kan ärvas från andra roller.

Franquiera och Wieringa (2012) beskriver hur rollbaserad åtkomstkontroll vilar på en samling antaganden. Användare ska inte tilldelas behörigheter på grund av dennes individuella egenskaper, en användare delar behörigheter med andra användare genom roller som bygger på ansvarsområden, arbetsuppgifter, kompetens, eller befogenhet i organisationen (A1). Antalet roller ska vara betydligt lägre än det antalet användare som ska tilldelas behörigheter (A2). Organisationens rollstruktur bör vara stabil och det största administreringsarbetet bör ske genom att hantera rolltillhörighet hos användarna vid personalomsättning och förändringar i arbetsuppgifter (A3). De personer som är inblandade i att planera och arrangera roller bör vara eniga i vilken semantik som används (A4). Rollbaserad åtkomstkontroll förutsätter att en användares identitet är känd redan före systemet beviljar eller avslår dennes åtkomst, även om detta inte alltid är fallet i till exempel webbaserade applikationer (A5). (Franqueira & Wieringa, 2012)



Figur 2: Antaganden hos rollbaserad åtkomstkontroll, och de styrkor de leder till. Egen översättning från Franquiera och Wieringa (2012)

Givet att ovanstående dessa antaganden stämmer uppmäter rollbaserad åtkomstkontroll enligt Franqueira och Wieringa (2012) en rad styrkor, vilket illustreras i figur 2 ovan.

2.3 Geografiska data

I följande avsnitt ges en introduktion till geografiska data.

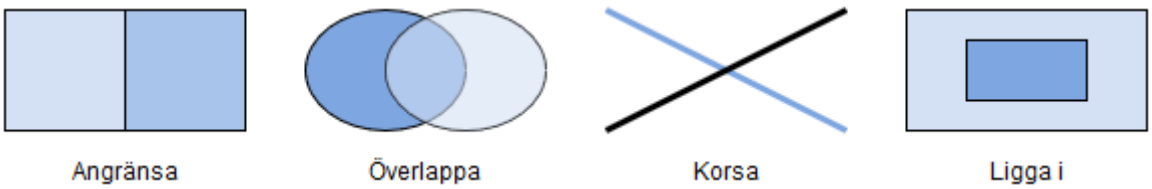
Den allt mer utbredda användningen av mobila enheter och positionsbaserade tjänster har tillsammans med ett växande intresse för hanteringen av geografisk information resulterat i en ökad efterfrågan på en förfinad rollbaserad åtkomstkontroll där geografiska faktorer beaktas (Bertino, Catania, Damiani, & Perlasca, 2005). I ett informationssystem representeras geografisk information av geografiska data (Huisman & de By, 2009).

Även om den verkliga världens komplexitet är gränslös ämnar man med geografiska data återge en bild av verkligheten, vilket endast är rimligen genomförbart om man förenklar denna (Harrie, 2012). Om man exempelvis skulle vilja ta reda på den kortaste möjliga resvägen för en pizzautkörning kanske vägens typ, hastighet och platser med trafikstockning kan vara av intresse. Vägens lutning, markeringar och skyltar kanske däremot kan anses vara överflödig information i sammanhanget. (Heywood, Cornelius, & Carver, 2011)

För att beskriva av mänskligheten skapade fenomen (till exempel byggnader eller vägar) kan man använda objektmodellen, där objekt av samma kategori tillhör samma objekttyp. En sjö kan till exempel tillhöra objekttypen sjö, och en väg kan tillhöra objekttypen väg. Varje objekt har geometriska egenskaper, vilka kan utgöras av en punkt, en linje, eller en yta (polygon). (Harrie, 2012)

En *punkt* består av koordinater, och kan beskriva objektets läge där dess egentliga utformning är ointressant. På en karta som framställer förekomsten av brevlådor eller träd i ett område kanske dessa endast behöver avbildas geometriskt med punkter. *Linjer* används för att avbilda linjära objekt som vägar, elledningar eller floder. En linje består av en samling punkter, sorterade i en ordning som motsvarar linjens utsträckning. En *yta* definieras av en eller flera stängda linjer där dess innanmäte utgör objektets geografiska utbredning. Ytor kan exempelvis användas för att avbilda administrativa områden eller upptagningsområden hos skolor. (Heywood, Cornelius, & Carver, 2011)

Förhållandet mellan två objekt kan vara antingen geometriskt eller topologiskt. En geometrisk relation beskriver exempelvis avstånd mellan objekten, medan en topologisk relation bland annat beskrivs i termer om att *överlappa*, *angränsa*, *korsa*, och *ligga i*, vilket illustreras i efterföljande figur 3. Exempelvis kan två kommuner angränsa till varandra, ett naturreservat kan överlappa en kommun, två vägar kan korsa varandra, och en byggnad kan ligga i en kommun. (Harrie, 2012)



Figur 3: Topologiska relationer mellan objekt, efter Harrie (2012, s. 20).

Vanligtvis har geografiska data också andra icke-rumsliga egenskaper, så kallade attribut. En kommun som geometriskt avbildas av en yta kan ha attributet befolkningsmängd, och en väg som geometriskt representeras av en linje kan ha attribut som högsta tillåtna hastighet och vägnummer. (Harrie, 2012)

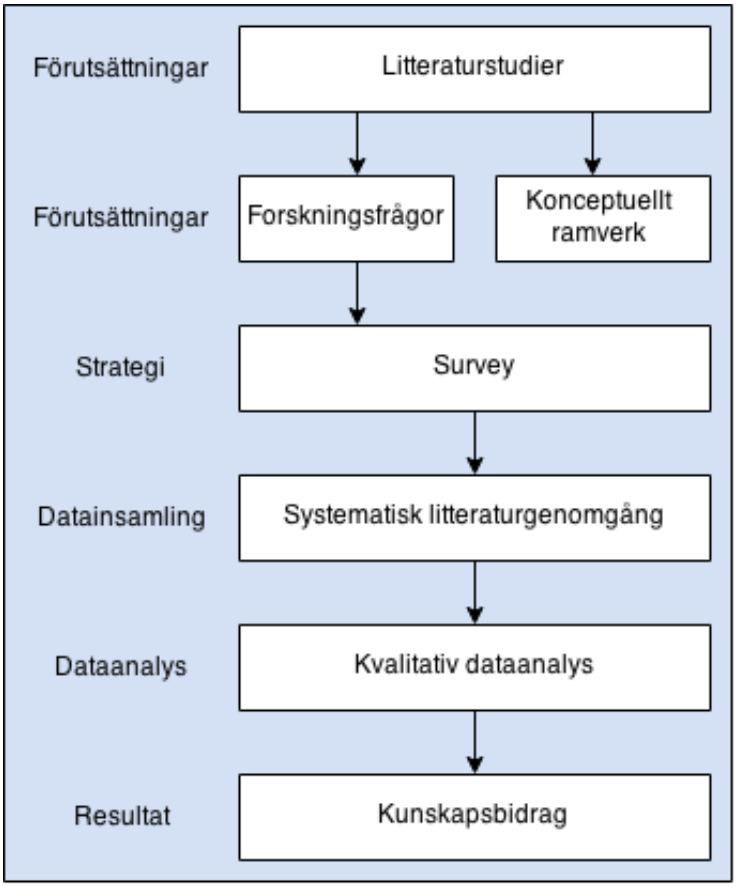
3. Metod

I metodkapitlet beskrivs arbetets upplägg och tillvägagångssätt, samt de processer som driver arbetet framåt från förutsättningar till resultat.

3.1 Forskningsetiska överväganden

Högskolan Dalarnas forskningsetiska anvisningar för examens- och uppsatsarbeten har beaktats vid arbetets genomförande (Högskolan Dalarna, 2013). Då arbetet utöver handledare och examinator inte involverat andra människor har inte några särskilda etiska frågor väckts, förutom axiomet att upprätthålla akademisk hederlighet. De riktlinjer kring plagiat och upphovsrätt som Högskolan Dalarna (2014) anger har tillsammans med sunt förnuft utgjort grunden för akademisk hederlighet i arbetet.

3.2 Arbetets metodupplägg



Figur 4: Arbetets metodupplägg, fritt illustrerat efter Oates (2006)

Utifrån en initial litteraturstudie har ämnesområdet problematiserats och lett till valet av forskningsstrategi och datainsamlingsmetod. Analys av datainsamlingens resultat har därefter genomförts för att sedermera leda till arbetets resultat. Litteraturstudier har förutom att utgöra förutsättningarna för arbetet och ligga till grund för strategi- och metodval även varit en kontinuerligt pågående process i syfte att förhöja graden av förståelse för ämnesområdet. Processen illustreras i figur 4 ovan.

3.3 Inledande litteraturstudier

Enligt Oates (2006) bedrivs en litteraturstudie vanligtvis till en början i syfte att få kännedom kring ämnesområdet och för att hitta uppslag till problemfrågor, för att sedan övergå i en mer långvarig process som pågår under hela den resterande tid då arbetet skrivs. För att få en överblick över de koncept som finns på ämnesområdet har det konceptuella ramverket i tabell 1 nedan utarbetats vid den inledande litteraturstudien.

Tabell 1: De koncept och söktermer som utgjort grunden för sökning under de inledande litteraturstudierna

Konceptuellt ramverk för sökning i inledande litteraturstudier

Koncept 1	*Koncept 2*	*Koncept 3*	*Koncept 4*
Role-based	Access Control	Model	Geographical
Roles	Security	Framework	Spatial
	RBAC	Standard	Geo
			GIS

Vetenskaplig litteratur på ämnesområdet har i den inledande fasen främst hittats genom att kombinera och söka på de termer som ingår i det konceptuella ramverket i tabell 1 ovan i databaserna Summon och Google Scholar. I Summon har sökningarna avgränsats till att endast innefatta sådant material som genomgått en *peer review*, medan Google Scholar saknar en sådan funktion. Resultatfrekvenser för sökningar visas i tabell 2 nedan.

Tabell 2: Resultatfrekvens vid sökning av vetenskaplig litteratur baserat på det konceptuella ramverket

	Antal sökresultat	
Söktermer	Google Scholar	Summon (Peer reviewed)
Role-based + Security	55 000	44 480
Role-based + Access Control	62 600	21 443
RBAC	30 200	889
Role-based + Access Control + Model	51 600	6 498
Role-based + Security + Model	53 400	10 220
Role-based + Access Control + Standard	39 400	4 310
Role-based + Access Control + Model + Geographical	14 000	346
Role-based + Access Control + Model + Spatial	7 110	370
Role-based + Access Control + Model + Geo	3 090	76
Role-based + Access Control + Model + GIS	2 180	76

Även om databassökningarna kan tyckas ha en hög resultatfrekvens har sökmotorerna själva sorterat resultaten baserat på relevans, och det har i de flesta fall visat sig vara endast det första trettiotalet resultat som haft tillräcklig relevans att studera närmre. Det allt snävare antalet relevanta sökresultat i de inledande litteratursökningarna (se tabell 2 ovan) tydde dock på att området kring rollbaserade åtkomstkontrollmodeller i en geografisk kontext inte var särskilt utforskat. Vidare urval och avgränsning har skett genom en kombination av att kontrollera hur frekvent respektive verk citerats av andra, att begränsa databassökningen till vetenskapligt granskade och publicerade verk, samt att bedöma huruvida respektive verks upphovsmans litterära bakgrund förhöjer dess trovärdighet (Oates, 2006).

De relevanta verk som hittats har sedan utgjort en grund för vidare litteraturstudier genom att som Oates (2006) beskriver följa upp dessa verks källhänvisningar, samt att genom Google Scholar följa upp vilka efterkommande verk som citerat dessa. Referenslistor från Wikipedia har också gåtts igenom.

3.4 Strategi: Survey

Den bakomliggande tanken med användandet av forskningsstrategin survey är enligt Oates (2006) att samla in likartad data från en större grupp datakällor. Då arbetets ambition varit att beskriva det befintliga kunskapstillståndet inom ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning har valet av forskningsstrategi naturligt fallit på en survey.

Även om en forskningsstrategin survey för det mesta kopplas samman med enkätundersökningar förklarar Oates (2006) att också andra metoder för att insamla data kan användas tillsammans med strategin. Oates (2006) menar vidare att en survey vanligtvis använder en enstaka datainsamlingsmetod. I arbetet har valet av datainsamlingsmetod fallit på en systematisk litteraturgenomgång.

Den delmängd av den totala mängden existerande material som har tillåtits inkluderas i arbetet har inte bestämts i förväg, och arbetet har istället tagit sin grund i en process kretsande kring ett sekventiellt upptäckande där en funnen datakälla i sin tur har kunnat leda till ytterligare en datakälla. Oates (2006) beskriver hur ett dylikt förhållningssätt anses tillhöra så kallad *grounded theory*.

Det är enligt Oates (2006) viktigt att redan i planeringsfasen av en survey fatta beslut kring vilka data som bör genereras och hur sådana data ska behandlas för att kunna besvara ett arbetes problemställning, och i arbetet har strategin survey därför varit tätt sammankopplad till metoden för datainsamling, den systematiska litteraturgenomgången.

3.5 Datainsamling: Systematisk litteraturgenomgång

I följande avsnitt beskrivs hur den systematiska litteraturgenomgångens förfarande utarbetats. I avsnittet behandlas strategi för sökningar, inklusions- och exklusionskriterier vid urval av material, liksom studiens dataextrahering och hur materialet sammanställts.

Oates (2006) menar att en utforskning av ett ämne, med grund i en litteraturbaserad undersökning av det befintliga kunskapstillståndet inom det specifika ämnesområdet, kan vara ett forskningsresultat. Enbart en rättfram beskrivning av ämnesområdet är dock inte tillräckligt för att utgöra ett fullgott kunskapsbidrag, och som Oates (2006) beskriver skjuts i detta arbete också till ytterligare tillskott i form av identifierandet av områden som står i behov av vidare utveckling och forskning.

En systematisk litteraturgenomgång är ett tillvägagångssätt för att identifiera, utvärdera och tolka allt vetenskapligt material som finns tillgängligt kring ett ämnesområde, en forskningsfråga, eller ett fenomen (Kitchenham & Charters, 2007). Systematiska litteraturgenomgångar är ett väletablerat tillvägagångssätt inom medicin och andra vetenskapsgrenar, även om informatiken inte ännu har omfamnat metoden i samma utsträckning (Staples & Niazi, 2007). De enskilda studier och verk som ingår i den systematiska litteraturgenomgången och bidrar till dess resultat är *primära verk*, medan den studie i vilket den systematiska litteraturgenomgången ingår är *sekundärt*. (Kitchenham & Charters, 2007)

> *"A systematic review is a defined and methodical way of identifying, assessing, and analyzing published primary studies in order to investigate a specific research question." – Staples & Niazi (2007, s. 1)*

Enligt Webster och Watson (2002) ska en systematisk litteraturgenomgång på ett heltäckande vis omfatta relevant litteratur inom ämnesområdet för att uppnå hög kvalitet, och det studerade materialet bör inte avgränsas till exempelvis en geografisk region eller en viss forskningsmetodik. I

sådana fall där en systematisk litteraturgenomgång inte är grundlig och genomgripande saknas det vetenskapliga värdet hos denna (Kitchenham & Charters, 2007).

Det underliggande motivet till genomförandet av den systematiska litteraturgenomgången är att besvara arbetets frågeställningar genom att identifiera kunskapsluckor i befintligt vetenskapligt material och därigenom föreslå områden eller ämnen vilka kan vara relevanta för vidare undersökningar. Kitchenham och Charters (2007) menar att detta är en av de vanligaste anledningarna till användning av metoden, tillsammans med framtagandet av en sammanställning av befintlig kunskap inom ett visst ämnesområde.

> *"Systematic literature reviews in all disciplines allow us to stand on the shoulders of giants and in computing, allow us to get off each other's feet."* – Kitchenham & Charters (2007, s. 4)

Kitchenham och Charters (2007) framhåller fyra frågor, vilka kan utgöra en bas för att bedöma kvaliteten hos en systematisk litteraturgenomgång:

- Är inklusions- och exklusionskriterier beskrivna och lämpliga?
- Är det rimligt att anta att litteratursökningen omfattar allt relevant material?
- Har kvaliteten hos det material som ingår i studien utvärderats?
- Har det material som ingår i studien beskrivits på ett rättvisande sätt?

Vid den systematiska litteraturgenomgångens utförande har dessa frågor utgjort en bas för att säkerställa att arbetets kvalitet håller en hög nivå. I syfte att förhöja arbetets transparens bifogas relevanta dokument kring genomförandet som bilagor. De riktlinjer som presenteras av Kitchenham och Charters (2007) har utvärderats och rekommenderats för användning inom informatik och datavetenskap av Staples och Niazi (2007) och Brereton et al. (2007).

3.5.1 Sökstrategi

En systematisk litteraturgenomgång måste utföras i enlighet med en fördefinierad sökstrategi som gör det möjligt att bedöma dess tillförlitlighet (Kitchenham & Charters, 2007). Vid genomförandet av sökningarna för studien användes de båda söktjänsterna Google Scholar och Summon, vilka indexerar vetenskapligt material från en mängd olika källor. Summon indexerar 587 journaler under ämneskategorin *Computer Science* (Högskolan Dalarna, 2015). Såvitt kan utläsas från Google Scholar's webbplats redovisas inte fullständigt vilka journaler som ingår, även om vissa högt rankade journaler listas (Google, u.d.). Valet av de söktjänster som använts för arbetet har baserats på Kitchenham och Charters (2007) andra kvalitetskriterium, i syfte att i så hög grad som rimligen är möjligt inkludera allt relevant material.

Ett konceptuellt ramverk har likt Oates (2006) förordar utarbetats för att ligga till grund för de praktiska sökningarna. Det konceptuella ramverket har utarbetats baserat på de insikter som den inledande litteraturstudien medfört. Vid sökningarna har de olika söktermerna i varje respektive konceptkategori kombinerats för att resultera i ett så brett materialunderlag som möjligt. Det konceptuella ramverket beskrivs i tabell 3 nedan.

Tabell 3: De koncept och söktermer som utgjort grunden för sökning under den systematiska litteraturgenomgången

Konceptuellt ramverk för sökning i systematisk litteraturgenomgång

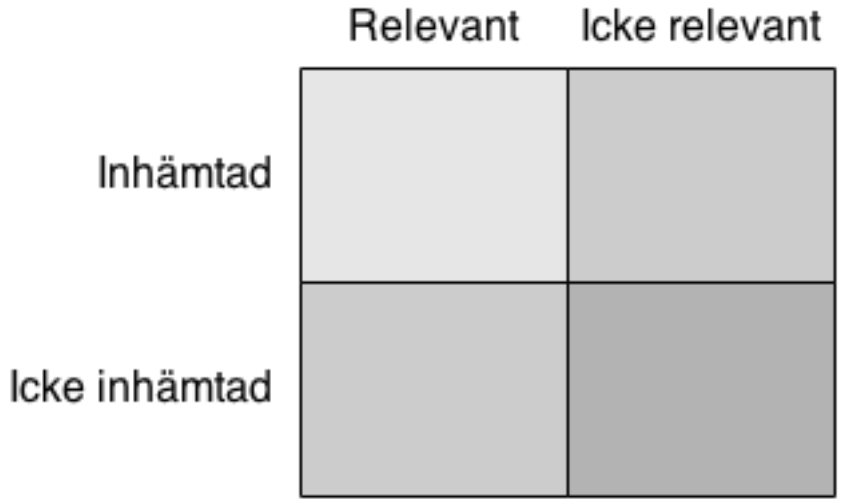
Koncept A	*Koncept B*	*Koncept C*	*Koncept D*	*Koncept E*
Roles	Access Control	Model	Geographical	Location
Role-Based	Security	Framework	Spatial	Position
RBAC	Authorization	Standard	Geo	
			GIS	

I sådana fall där ett verk som bedöms vara intressant för arbetets frågeställning listats bland sökresultatet, men inte funnits direkt tillgängligt via en länk, har den traditionella sökmotorn Google använts för att om möjligt finna en läsbar och fullständig version av materialet på annat håll. Sökningen har då innefattat verkets fullständiga titel i kombination med författarens efternamn. Har det eftersökta verket inte återfunnits i sin helhet genom detta har det utelämnats från det fortsatta arbetet. Det material i vilket sökningarna resulterat i har sedermera inkluderats för vidare urval.

För att kunna tillhandahålla en så fullständig bild av det aktuella kunskapstillståndet som möjligt har sökningarna i söktjänsterna Google Scholar och Summon även kompletterats med framåt- och bakåtsökningar, likt Webster och Watson (2002) förespråkar. Bakåtsökning har baserats på att under genomgången av respektive verk studera de referenser som angetts av verkets författare. De titlar som tyckts vara av relevans för arbetets ämne har sedan i möjlig mån inkluderats för den fortsatta studien. Framåtsökning har utförts genom att under genomgången av respektive verk genom söktjänsten Google Scholar granska vilka efterföljande verk som citerat det aktuella verket. De verk som framåt- och bakåtsökning resulterat i har på samma villkor som övriga verk fått genomgå en efterföljande urvalsprocess. En logg för sökningarna finns i bilaga 1.

3.5.2 Precision och Recall

Precision och Recall är två sätt att mäta effektiviteten hos en informationssökning eller söktjänst (Fransson, 2007). Precision anger informationsinhämtningens exakthet, vilket kan uttryckas i tal om hur stor andel av inhämtade verk som är relevanta i relation till totalt antal inhämtade verk. Recall är den grad av fullständighet som inhämtandet av information uppnår och kan uttryckas i tal om antalet relevanta inhämtade verk i relation till det totala antalet relevanta verk. För att kunna göra en bedömning krävs att ett binärt omdöme ges varje verk; det kan antingen vara relevant eller icke relevant. Varje respektive verk som en sökning resulterar i kan således kategoriseras in i *en* av rutorna i figur 5 nedan. (Buckland & Gey, 1994)



Figur 5: Matris för bedömning av precision och recall. Egen modell efter Buckland och Gey (1994).

Även om det naturligtvis vore önskvärt att samtidigt åstadkomma höga värden både för precision och recall är detta enligt Buckland och Gey (1994) ouppnåeligt, och en avvägning måste göras för att sätta den faktor som är lämpligast för varje respektive studie i fokus. Då detta arbete ämnar ge en översiktlig bild av det tillstånd i vilket kunskapen i skrivande stund befinner sig i är måttet recall i störst fokus, eftersom fullständigheten och att inte gå miste om viktiga relevanta artiklar inom området är av stor vikt. Det bästa tänkbara recall-värdet hos den systematiska litteraturgenomgången i detta arbete är således 1.

3.5.3 Urvalskriterier

En systematisk litteraturstudie kräver enligt Kitchenham och Charters (2007) att uttryckliga inklusions- och exklusionskriterier utformas i syfte att bedöma huruvida det är lämpligt att inkludera de respektive verk som sökningarna resulterar i. De primära verk som tillåtits ingå i den systematiska litteraturgenomgången har godkänts enligt de inklusions- och exklusionskriterier som beskrivs i tabell 4 nedan.

Tabell 4: Den systematiska litteraturgenomgångens inklusions- och exklusionskriterier

	Inklusionskriterier	**Exklusionskriterier**
Urvalsnivå 1	Publicerat tidigast 1 januari 1990 Engelskspråkig titel	Saknar enligt titel relevans för studien
Urvalsnivå 2	Genomgått peer review	Saknar engelskspråkigt abstract Abstract tyder inte på relevans för studien
Urvalsnivå 3	Tillgängligt i sin helhet på Internet	Saknar i innehåll relevans för studien

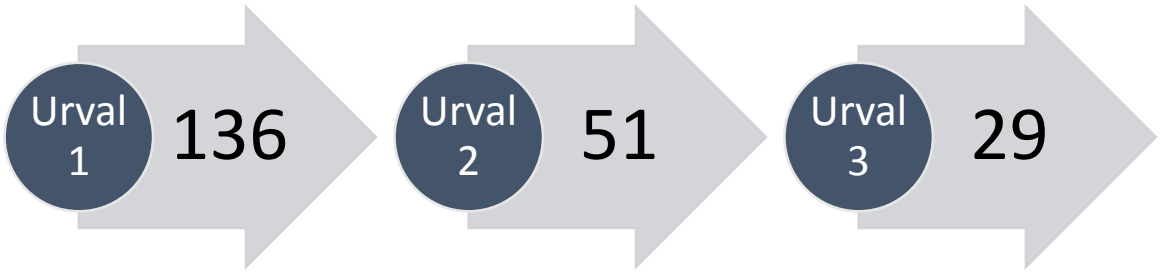
Urval har skett på tre nivåer. Den första nivån av urval har utförts redan vid sökningen i de båda söktjänsterna Google Scholar och Summon. Söktjänsterna har konfigurerats för att i sökningarna enbart inkludera sådant material med en angiven tidpunkt för publicering från och med den första januari 1990. Booth et al. (2012) menar att det enskilt mest effektiva sättet att avgöra huruvida funnet material är av betydelse för en studie är att granska dess titlar. Endast sådant material som tillhandahåller en titel skriven på engelska, som inte uppenbart visar att det aktuella verket saknar relevans för litteraturgenomgångens syfte har passerat den första urvalsnivån. I urval ett har 136 verk inkluderats för att passera till urval två.

Enbart sådana vetenskapliga verk, som genomgått en peer review, och som Booth et al. (2012) beskriver har ett befintligt abstractavsnitt eller motsvarande sammanfattande text (författad på engelska) som uppvisar relevans för arbetets frågeställning har tillåtits passera urvalsnivå två. Söktjänsten Summon har inbyggt stöd för att filtrera ut endast sådant material som genomgått peer review-granskning, medan Google Scholar inte innehåller någon dylik funktion. Kontrollen av huruvida ett verk genomgått en peer review-granskning har istället i första hand skett genom publikationsdatabasen Ulrichsweb. I sådana fall där den aktuella publikationen inte hittats på Ulrichsweb har istället dess utgivares webbsida kontrollerats. Om ingen information av värde framkommit efter dessa steg har antagandet att verket inte genomgått en peer review gjorts. Sådana verk som inte uppfyller kraven har exkluderats ur den vidare studien. I urval två har 51 verk inkluderats för att tillåtas vidare passage till urval tre.

Vid urvalet på den tredje nivån har sådant material som godtagits i urvalsnivå två hämtats hem i sin helhet och studerats i syfte att avgöra om dess innehåll varit av relevans för studien. För att detta skulle vara möjligt har endast sådant material som under studiens genomförande i sin helhet funnits tillgängligt på Internet inkluderats. För material som exkluderas ur den fortsatta studien baserat på innehållskriteriet dokumenteras och beskrivs anledningen till detta (Booth, Papaioannou, & Sutton, 2012). Dokumentation över verk som exkluderats med grund i bristande innehållsrelevans och som inte varit möjliga att nå via internet finns i bilaga 2 och 3.

Då Kitchenham och Charters (2007) betonar att det är av stor vikt för trovärdigheten hos en systematisk litteraturgenomgång att dess utförare utvärderar kvaliteten hos det material som tillåts ingå i studien var tanken från början att en kvalitetsutvärdering skulle ingå i urvalsnivå tre. På grund av den subjektivitet som uppstår hos en kvalitetsutvärderings samt risken för att med grund i

utvärderingen exkludera relevant material har kvalitetsutvärderingen dock inte låtits utgöra ett inklusions- eller exklusionskriterium. Samtligt inkluderat material har trots det utvärderats, och resultatet kan ses i bilaga 4. I urvalsnivå tre har 29 verk godkänts för att inkluderas i den fortsatta litteraturgenomgången. Den totala urvalsprocessens utgång beskrivs i figur 6 nedan.



Figur 6: Urvalsprocessen i den systematiska litteraturgenomgången

De genomförda sökningarna har i många fall resulterat i en stor andel material som redan exkluderats eller inkluderats vid en tidigare sökning, och sådana verk har uteslutits ur det vidare urvalet när det upptäckts att så varit fallet.

3.5.4 Extrahering av data

I syfte att möjliggöra insamling av all sådan information som är nödvändig för att besvara ett arbetes problemfrågor krävs enligt Kitchenham och Charters (2007) att ett dataextraheringsformulär utformas. För att på ett systematiskt vis kunna utvinna data ur det material som inkluderats i studien har en samling punkter som definierar vilken data som ska extraheras framtagits och sammanställts i ett formulär, vilket beskrivs ytterligare i efterföljande tabell 5. En kopia av det formulär som använts bifogas i bilaga 5.

Tabell 5: Beskrivning av det formulär som använts för att extrahera data från inkluderade verk

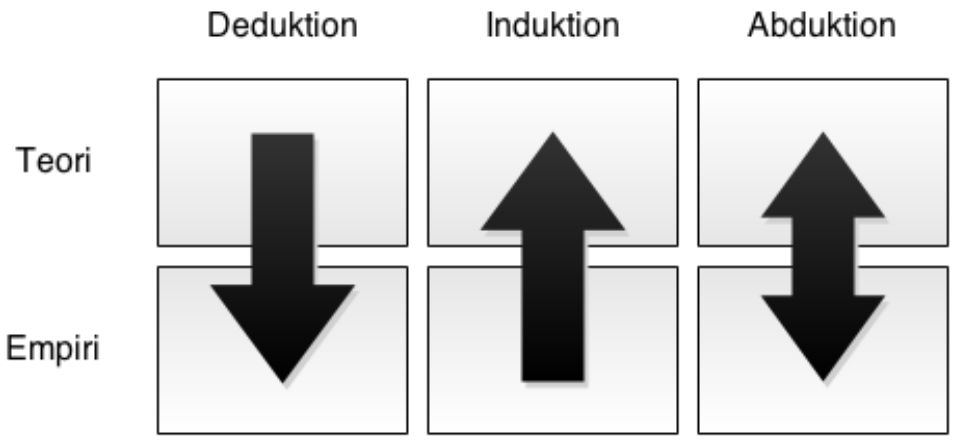
Data	Förklaring
Titel	Den fullständiga titel under vilken verket publicerats.
Källa	Den konferenshandling eller journal i vilken verket publicerats.
Årtal	Det år då verket publicerats. I sådana fall där det aktuella verket publicerats flera gånger under olika år noteras båda årtalen, men endast det första årtalet används i den efterkommande dataanalysen.
Författare	Den eller de författare som står som upphovsman till verket, samt organisationstillhörighet och verkets ursprungsland.
Typ	Den typ som verket utgör. Ett verk kan exempelvis vara en journalartikel eller en konferenshandling.
Angivna nyckelord	De nyckelord som angetts av verkets författare.
Sammanfattning	Den sammanfattning eller det abstraktavsnitt som verket innehåller.
Slutsatser	De slutsatser som i verket anges ha dragits.
Vidare studieförslag	De eventuella förslag på vidare studier som anges i verket.
Antal citeringar	Det antal gånger som verket enligt Publish or Perish citerats.
Ytterligare noteringar	Plats för eventuella ytterligare noteringar som inte faller under någon av de ovanstående kategorierna.
Extraheringsdatum	Det datum som dataextraheringen ägt rum.

3.5.5 Sammanställning och analys

Alla icke-numeriska data är kvalitativa, och de data som inhämtats från den systematiska litteraturgenomgången är inget undantag. För att kunna analysera sådana data krävs enligt Oates (2006) att den i ett första steg prepareras genom att överföras till ett likartat format, vilket uppnås genom att använda formuläret för dataextrahering. Analysen av insamlade data sker med hjälp av den referensram som skapats vid litteraturstudier och teorigenomgång (Björklund & Paulsson, 2003).

När data extraherats från de inhämtade primära verken måste dessa enligt de riktlinjer som presenterats av Kitchenham och Charters (2007) sammanställas och sammanfattas, vilket kan ske i beskrivande kvalitativ form. Då arbetets frågeställningar lämpligen besvaras med ord och satser snarare än med reella tal antar arbetet en kvalitativ ansats (Nyberg, 2000). Kitchenham och Charters (2007) menar vidare att en deskriptiv sammanställning vid behov kan kompletteras med en kvantitativ sammanfattning genom statistiska tekniker, en så kallad metaanalys.

Sammanställningen av en systematisk litteraturgenomgång är konceptfokuserad istället för författarfokuserad, då ett för starkt fokus på författare kan leda till att sammanställningens egentliga inriktning istället centrerar kring vilka författare som ligger bakom de olika verken (Webster & Watson, 2002; Oates, 2006). Enligt Webster och Watson (2002) rekommendationer används i detta syfte en konceptmatris där respektive analysenhet, vetenskapligt verk, sammanlänkas med de koncept som redan definierats med grund i den inledande litteraturstudien. Booth et al. (2012) menar att en sådan innehållsanalys där data organiseras och analyseras med grund i en redan skapad konceptkonstruktion är en ramverkssammanställning. Att i en analys kategorisera insamlad data efter redan fördefinierade koncept kan enligt Oates (2006) anses utgöra en deduktiv approach. Den deduktiva approachen medför aspekten att det är av stor vikt att inte för strängt fokusera på de givna koncepten och därigenom förbise andra relevanta koncept (Oates, 2006). Under läsningen av de insamlade verken tilläts därför dessutom också att nya koncept kunde uppstå, vilka efter att de identifierats och definierats införts i konceptmappningsmatrisen. Befintliga koncept har också modifierats allt eftersom förståelsen för de olika företeelserna förbättrats allt efter arbetets gång. Oates (2006) menar att det när nya kategorier uppstår under observation och granskning av insamlad data föreligger en induktiv approach. När man som i detta fall under arbetets gång växlar mellan induktion och deduktion kan man enligt Björklund och Paulsson (2003) istället tala om att abduktion föreligger. I figur 7 nedan illustreras de olika approacherna som anger hur fakta skapas enligt Björklund och Paulsson (2003).



Figur 7: Hur deduktion, induktion och abduktion förhåller sig till teori och empiri, efter Björklund och Paulsson (2003)

3.6 Metodkritik

Kitchenham och Charters (2007) menar att den största nackdelen hos en systematisk litteraturstudie är den bemödande arbetsinsats som metoden kräver av dess utförare. Sammanställningen av detta arbete har endast pågått under en begränsad tidsperiod, men då en eventuellt hög tidsåtgång tagits i beaktning har det varit möjligt att på ett, i så stor utsträckning som möjligt, lämpligt sätt planera genomförandet av arbetet. Det är emellertid uppenbart att en studie som utförs under en längre tidsperiod skulle kunna genomföras med högre noggrannhet. För att på ett effektivt vis kunna utföra en litteraturstudie krävs enligt Marelli (2005) en god förmåga att söka och identifiera relevant information, liksom färdigheter i att analysera och meningsfullt sammanfatta denna. Tillvägagångssättet för litteraturgenomgången har baserats på redan existerande riktlinjer för att i så hög grad som är möjligt bemöta detta.

Marelli (2005) menar vidare att litteraturstudier är begränsade i det avseende att det endast är möjligt att samla in data kring sådant som redan skett i det förflutna, och att aktualiteten hos en litteraturstudie därmed riskerar att vara låg. Oates (2006) beskriver också hur sådana ögonblicksbilder utgör en negativ aspekt under användandet av forskningsstrategin survey. Vid genomförandet av detta arbete har naturligtvis endast sådant material som i skrivande stund varit publicerat kunnat granskas, vilket dock bör anses vara fullt tillräckligt för att kunna besvara arbetets problemfrågor.

Enligt Brereton et al. (2007) är det viktigt att den systematiska litteraturgenomgångens utförare för spårbarhetens skull noggrant dokumenterar eventuella förändringar eller nya beslut som tas under dess genomförande. Så har skett i förekommande fall.

Det är i en systematisk litteraturgenomgång oundvikligt att inte av misstag förbise visst sådant material som eventuellt hade varit relevant för arbetet. Om sådant material har en sådan karaktär att de skulle ha varit kritiska eller avgörande för arbetet är det dock troligt att sådana dokument identifieras vid granskning före eller efter arbetets inlämning. (Webster & Watson, 2002)

Oates (2006) förklarar att forskningsstrategin survey fokuserar på en bred snarare än djup täckning av ämnesområdet, vilket medför att detaljnivån hos ett sådant arbete blir låg. Det är naturligtvis viktigt att vara medveten om detta i den fortsatta läsningen av detta arbete.

4. Empiri

I följande kapitel sammanställs resultatet av arbetets datainsamling, den systematiska litteraturgenomgång som utförts.

4.1 Inkluderat material

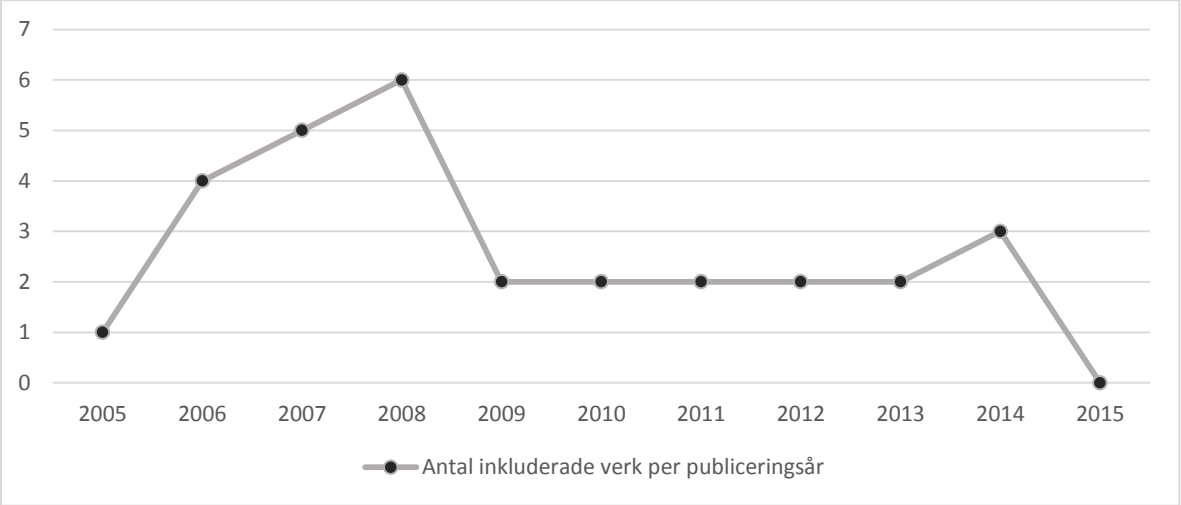
Det material som tillåtits passera de tre urvalsnivåerna presenteras i tabell 6 nedan, där de inkluderade verken för överskådlighetens skull sorterats efter år för publicering. Respektive verk tilldelas ett nummer som används i efterföljande konceptmappning.

Tabell 6: De verk som passerat de tre urvalsnivåerna i den systematiska litteraturgenomgången

#	Titel	Årtal	Författare
1	GEO-RBAC: A Spatially Aware RBAC	2005	E Bertino, B Catania, ML Damiani, P Perlasca
2	Application of temporal and spatial rbac in 802.11 wireless …	2006	E Tomur, YM Erten
3	LRBAC: A Location-Aware RoleBased Access Control Model	2006	I Ray, M Kumar, L Yu
4	Proximity Based Access Control in Smart-Emergency …	2006	SKS Gupta, T Mukherjee, K Venkatasubramanian
5	STRBAC An approach towards spatio-temporal role-based …	2006	M Kumar, R Newman
6	A geotemporal role-based authorization system	2007	V Atluri, SA Chun
7	A Spatio-Temporal Role-Based Access Control Model	2007	I Ray, M Toahchoodee
8	Coordinated access control with temporal and spatial …	2007	S Fu, CZ Xu
9	C-RBAC: Contextual Role-Based Access Control Model	2007	MN Tahir
10	STARBAC: Spatiotemporal Role Based Access Control	2007	S Aich, S Sural, AK Majumdar
11	Context-Aware Adaptation of Access-Control Policies	2008	A Samuel, A Ghafoor, E Bertino
12	Context-Aware Role-based Access Control in Pervasive …	2008	D Kulkarni, A Tripathi
13	Hierarchies in Contextual Role-Based Access Control Model …	2008	MN Tahir
14	Policy Mapper: Administering Location-Based Access …	2008	R Bhatti, ML Damiani, DW Bettis, E Bertino
15	Role-based access control for boxed ambients	2008	A Compagnoni, E Gunter, P Bidinger
16	Spatial Domains for the Administration of Location-based …	2008	ML Damiani, E Bertino, C Silvestri
17	Role Based Access Control with Spatiotemporal Context for …	2009	S Aich, S Mondal, S Sural, AK Majumdar
18	Spatiotemporal Access Control Enforcement under …	2009	H Shin, V Atluri
19	A Generalized Temporal and Spatial Role-Based Access …	2010	HC Chen
20	Enforcing Spatial Constraints for Mobile RBAC Systems	2010	MS Kirkpatrick, E Bertino
21	Location-Based Access Controls for Mobile Users …	2011	E Bertino, MS Kirkpatrick
22	Prox-RBAC: A Proximity-based Spatially Aware RBAC	2011	MS Kirkpatrick, ML Damiani, E Bertino
23	Mobile Security with Location-Aware Role-Based Access …	2012	N Ulltveit-Moe, V Oleshchuk
24	STRoBAC - Spatial Temporal Role Based Access Control	2012	KTL Thi, TK Dang, P Kuonen, HC Drissi
25	A formal role-based access control model for security …	2013	D Unal, MU Caglayan
26	A Location-based Secure Access Control Mechanism for …	2013	MS Rajpoot
27	A Formal Proximity Model for RBAC Systems	2014	A Gupta, MS Kirkpatrick, E Bertino
28	Contextual View-based Access Control Model for Spatial …	2014	M Ibrahim, H Hefny, N Hamza
29	Multi-granularity spatial-temporal access control model for …	2014	A Zhang, J Gao, C Ji, J Sun, Y Bao

Som det kan utläsas av tabell 6 ovan är vissa författare återkommande i det inkluderade materialet. Bertino har medverkat i åtta av de totalt 29 inkluderade verken. Kirkpatrick och Damiani har vardera medverkat i fyra inkluderade verk. Det tidsmässigt först publicerade inkluderade verket där Bertino et al. (2005) presenterar modellen GEO-RBAC har enligt Publish or Perish refererats 243 gånger i andra verk. Många av de övriga inkluderade verken refererar också till GEO-RBAC, som behandlar användarpositionsbaserad åtkomstkontroll.

4.2 Inkluderat material fördelat på år för publicering



Figur 8: Totalt antal inkluderade verk per fördelat på år för publicering

Fördelningen per år för publicering hos de totalt 29 verk som inkluderats i den systematiska litteraturgenomgången illustreras i figur 8 ovan. Störst andel av det inkluderade materialet har publicerats 2007 och 2008, med 5 respektive 6 publicerade verk. Antalet verk per år som passerat urvalet och därmed inkluderats har därefter sjunkit, och från och med 2009 har endast två eller tre verk per år inkluderats.

4.3 Kvalitet hos inkluderat material

Då det material som passerat de tre urvalsnivåerna och därmed inkluderats i den systematiska litteraturgenomgången utgjorts av vetenskapliga publikationer som refereegranskats har en viss miniminivå för kvaliteten hos det inkluderade materialet upprätthållits. Förutom enstaka språkliga fel är samtliga verk välskrivna, och de källor som använts i verken redovisas öppet. En del av de inkluderade verken har en aning svävande problemställning, vilket kan härröras från det komprimerade format som journalartiklar och konferensbidrag kan ha. Den tid som förflutit sedan ett verk publicerats inverkar på hur frekvent det refereras av andra verk, och sådana verk som relativt nyligen publicerats har som en naturlig följd ofta inte refererats i lika stor utsträckning som äldre verk. Två av de verk som inkluderats har vid tidpunkten för den systematiska litteratur genomgången enligt Publish or Perish inte alls refererats från andra verk, vilket kan härledas till att de publicerats först föregående år. Inkluderat material har generellt hållit en hög kvalitetsnivå, och samtliga inkluderade verk har genomgått en kvalitetsutvärdering som kan ses i bilaga 4.

5. Analys

I följande kapitel analyseras och sammanställs de data som framkommit under den systematiska litteraturgenomgången. Kapitlet börjar med att definiera ett antal koncept som sedan sammankopplas med de verk som inkluderats i studien. Därefter återges hur respektive koncept behandlas i det inkluderade materialet.

5.1 Konceptdefinitioner

De koncept som används i analysen har uppkommit genom abduktion. Från de inledande litteraturstudierna har ett antal preliminära koncept uppstått som under den systematiska litteraturgenomgångens genomförande förändrats. Nya koncept har tillkommit och andra har tagits bort. Nedan definieras och förklaras de koncept som slutligen utformats och använts i analysen.

Koncept A: Datapositionsavgränsning
Åtkomstkontrollen hanterar användares begäran om att nå rumsliga data i ett geografiskt informationssystem. Datapositionsavgränsning baseras likt Ibrahim et al. (2014) beskriver på att en användare endast tillåts åtkomst till de objekt som geografiskt befinner sig inom en sådan yta där denne har behörighet.

Koncept B: Geografisk användarpositionering
Den geografiska position på vilken användaren befinner sig. En geografisk användarposition utgörs av en geometrisk form (Bertino, Catania, Damiani, & Perlasca, 2005), där dess koordinater bestämmer läget i minst två dimensioner.

Koncept C: Annan användarpositionering
En användares position behandlas på annat sätt än geografiskt. Sådan användarpositionering innefattar exempelvis logisk positionering, där användarens topologiska position står i fokus snarare än användarens exakta koordinater (Bertino, Catania, Damiani, & Perlasca, 2005).

Koncept D: Rörlighet
Den föränderlighet som en användares geografiska position uppbär behandlas, och aspekter som rörligheten medför diskuteras. Det kan handla om att likt Thi et al. (2012) beskriver förändra en användares åtkomstmöjligheter när denne förflyttar sig.

Koncept E: Närhet
Förhållandet mellan olika användares geografiska läge (Bertino, RBAC models - concepts and trends, 2003) eller användares geografiska läge och de objekt som åtkomstkontrollen syftar begränsa åtkomsten till (Gupta, Mukherjee, & Venkatasubramanian, 2006). Avståndet däremellan är relevant för konceptet närhet.

Koncept F: Integritet
Diskussioner förs kring integritetsmässiga aspekter hos geografiska data. Det kan exempelvis handla om hur användarpositioner hanteras och lagras (Ray, Kumar, & Yu, LRBAC: A Location-Aware Role-Based Access Control Model, 2006).

Koncept G: Hierarkiska relationer
Koncept i åtkomstkontrollen kan organiseras i hierarkiska strukturer. Det kan handla om att de roller som åtkomstkontrollen kretsar kring organiseras i strukturerade hierarkier där roller ärver behörigheter från andra roller som befinner sig på en överordnad position i arvskedjan (ANSI, 2004), men också andra företeelser kan ingå i en hierarkisk relation.

Koncept H: Tidsmässiga restriktioner
Tid ingår, likt Aich et al. (2007) beskriver, i åtkomstkontrollen i form av en faktor som bestämmer när åtkomsten till data är möjlig.

Koncept I: Nätverk
Den rollbaserade åtkomstkontrollen hanterar åtkomlighet till ett nätverk (Unal & Caglayan, 2013).

Koncept J: Ändamål
De ändamål med vilka en användare i ett system med rollbaserad åtkomstkontroll ämnar använda resurser i ett informationssystem behandlas (Tahir, C-RBAC: Contextual Role-Based Access Control Model, 2007).

Koncept K: Policyhantering
Hur administrering och hantering av policys för rollbaserad åtkomstkontroll behandlas (Damiani, Bertino, & Silvestri, 2008).

Koncept L: Automatisering
Automatisering av arbetsflöden behandlas. Ett exempel är som Gupta et al. (2006) beskriver hur automatisering kan medföra att användare automatiskt loggas in i ett system utan att behöva manuell autentisering genom att mata in användarnamn och lösenord.

5.2 Sammanlänkning av inkluderat material och koncept

Den systematiska litteraturgenomgångens inkluderade material har i en konceptmappningsmatris sammanlänkats med de koncept som tidigare definierats. Som Booth et al. (2012) beskriver används färgkodning för att göra matrisen tydligare. I tabell 7 nedan återfinns konceptmappningsmatrisen.

Tabell 7: Konceptmappningsmatris för sammanlänkning av inkluderat material till koncept

1 Behandlar konceptet utförligt
Hur konceptet hanteras beskrivs utförligt och utgör en av verkets centrala byggstenar.

2 Behandlar delvis konceptet
Hur konceptet hanteras beskrivs till viss del, men är inte en av verkets centrala delar.

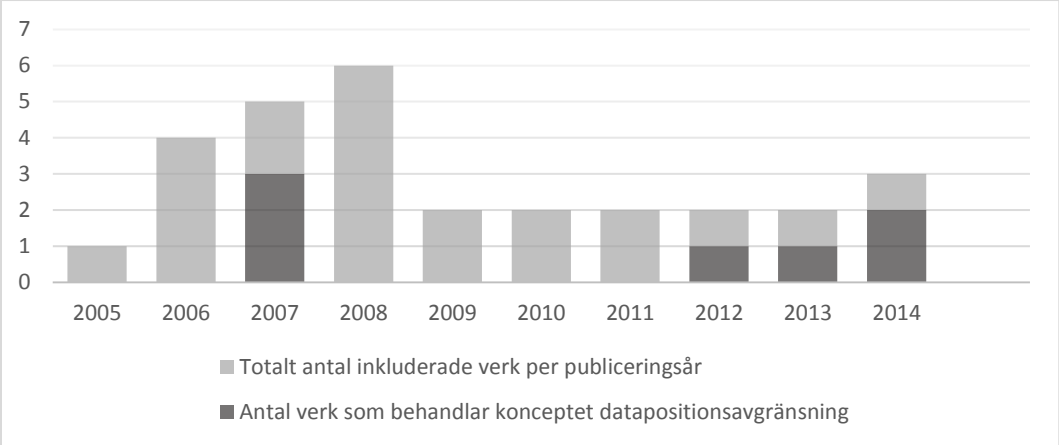
3 Behandlar konceptet flyktigt
Konceptet nämns på ett lättvindigt vis, utan att ges vidare behandling.

	Koncept											
Artikel	A	B	C	D	E	F	G	H	I	J	K	L
1		1	1	3			1					
2			2					2	1			
3		1	2			2						
4			2	2	1							1
5		1	1			2		1				
6	1	2				1	2	2				
7		1	2				1	1				
8			2	2				2	1			
9	1									1		
10	3	1	2					1				
11		2						2			1	
12			2	1				3				
13			1				1			1		
14											1	
15			1	2					1			
16											1	
17		1	1	2				2				
18			1	1								
19		2					2	2				
20				1	1	2						
21		2			2	2						
22					1		2					
23		1										
24	1											
25			2	1			3		1			
26	1											
27					1							
28	1											
29	1							2				

5.3 Konceptanalys

I följande avsnitt återges hur de verk som inkluderats i den systematiska litteraturgenomgången behandlar de koncept som definierats.

5.3.1 Koncept A: Datapositionsavgränsning



Figur 9: Antal inkluderade verk som per år behandlar konceptet datapositionsavgränsning

I figur 9 ovan illustreras hur konceptet datapositionsavgränsning representeras fördelat på årtal i det inkluderade materialet. 2007 behandlades konceptet i tre verk, för att sedan inte behandlas igen förrän 2012.

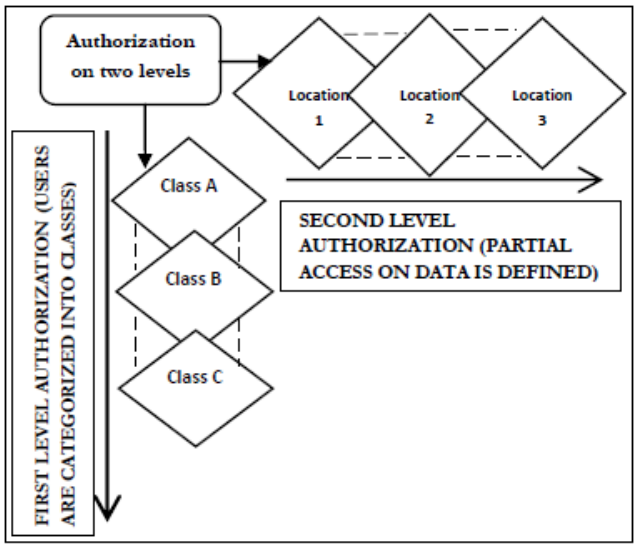
Atluri och Chun (2007) beskriver i sin modell GSAS hur de rumsliga attribut som finns hos data kan användas för att endast låta användare få behörighet att nå data som befinner sig på vissa platser. I GSAS-modellen används åtkomstkontrollen främst för att skydda satellitbilder, och det kan då vara av stor vikt att inte vem som helst kan tillåtas se vilken plats som helst på en högupplöst och detaljrik nivå. (Atluri & Chun, 2007)

Tahir (2007) menar att data kan grupperas i spatiala domäner som utgörs av en avgränsning kring ett eller flera objekt. Sådana spatiala domäner kan också överlappa varandra, vilket exemplifieras med att olika avdelningar på ett sjukhus. En operationsavdelning kan exempelvis också delvis ingå i en akutavdelning. (Tahir, 2007)

I STARBAC förutsätts att både användare och data innehar en position, även om datapositionsavgränsningen inte behandlas djupare. (Aich, Sural, & Majumdar, 2007)

STRoBAC, en åtkomstkontrollmodell som baseras på den tidigare presenterade modellen STRBAC, hanterar åtkomsten till geospatial data i geografiska informationssystem baserat på roller med rumsliga och tidsmässiga avgränsningar. (Thi, Dang, Kuonen, & Drissi, 2012)

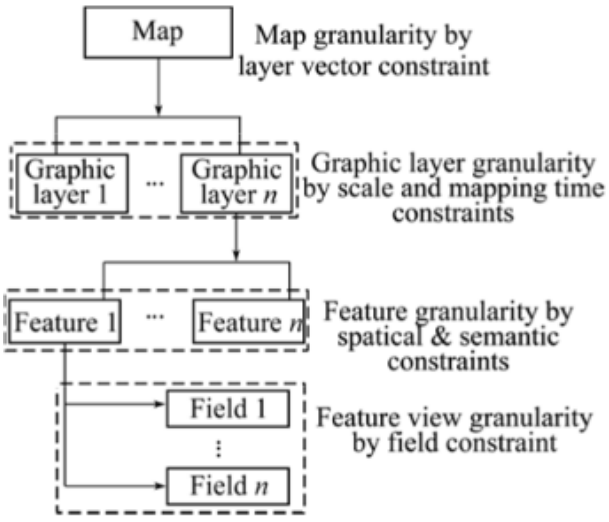
Rajpoot (2013) introducerar en liknande modell för att hantera kontrollen av åtkomst till geospatial data. I den presenterade modellen fördelas åtkomstkontrollen på två nivåer. På den första nivån hanteras användarauktoriseringen, det genomförs en kontroll av att användaren faktiskt innehar rättigheter att nå den del av den geografiska databasen som denne försöker nå. För att kunna avgöra huruvida en användare har rättighet att nå efterfrågad del av databasen fördelas dessa på olika klasser. På den andra nivån behandlas användarens rättighet att nå geografiska bilder, exempelvis satellitbilder, och att användaren endast tillåts hämta de delar av bilderna som denne har rättighet och behov för med en sådan upplösning som behörigheten tillåter. De två nivåerna av åtkomstkontroll enligt Rajpoot (2013) presenteras i figur 10 nedan.



Figur 10: Auktoriseringens två nivåer (Rajpoot, 2013, s. 29)

Ibrahim et al. (2014) behandlar åtkomsten till geografiska data genom att introducera konceptet *vy*. En vy är en virtuell tabell, där sådana värden från den geografiska databasen som en användare tillåts komma åt hålls i syfte att utgöra ett avgränsat fönster till den egentliga databasen. Det föreligger ingen direkt kontakt mellan användaren och den bakomliggande databasen, all data som en användare tillåts nå extraheras istället till en vy. Ibrahim et al. (2014) visar upp sin modell i en prototyp där ett lagerföretag med rollerna *Administratör* och *MellanAmerikaChef* utgör ett exempel. Administratör har behörighet att se samtliga lagerlokaler i USA, och MellanAmerikaChef har endast behörighet att se lagerlokaler som geografiskt befinner sig i Mellanamerika. När Administratör använder systemet för att se lagerlokaler på en karta över USA används vyn AllaLagerlokaler som hämtar och visar alla lagerlokaler. När MellanAmerikaChef använder systemet för att titta på alla lagerlokaler används istället vyn LagerlokalerMellanamerika som hämtar och visar endast sådana lagerlokaler som geografiskt befinner sig i det fördefinierade området MellanAmerika på USA-kartan. (Ibrahim, Hefny, & Hamza, 2014)

Zhang et al. (2014) presenterar i sin åtkomstkontrollmodell MSTAC (Multi-granularity Spatial-temporal Access Control Model) ett tillvägagångssätt för att tillhandahålla flerlagerbaserad åtkomstkontroll till spatial data, vilket illustreras i figur 11 nedan.

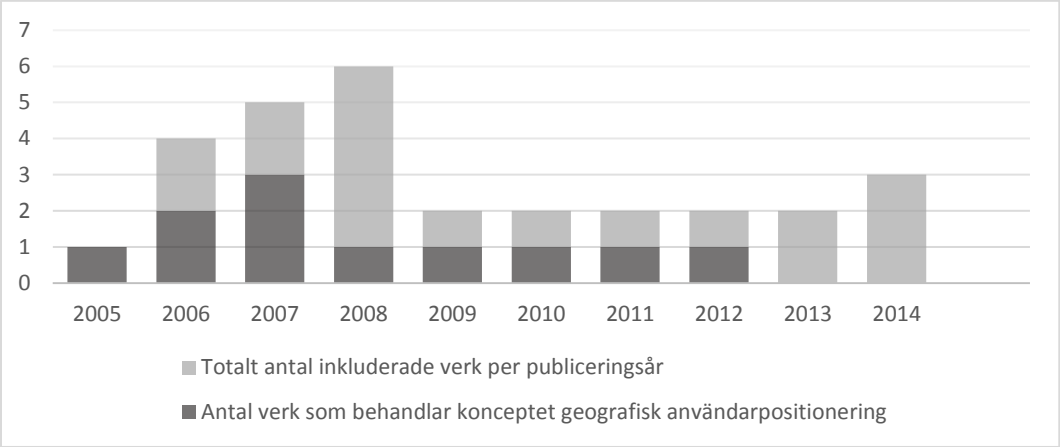


Figur 11: Åtkomstkontroll på flera nivåer hos spatial data i MSTAC (Zhang, Gao, Ji, Sun, & Bao, 2014, s. 2948)

På kartlagernivå specificeras vilka grafiska lager i kartan som en roll ska kunna inhämta, och på grafiklagernivån definieras restriktioner för tid och för vilken skala som en viss klass ska kunna hämtas och visas. Featurenivån hanterar rumsliga och semantiska restriktioner, och featurefältnivån hanterar vilka fält hos de spatiala objekten som hämtas och visas. (Zhang, Gao, Ji, Sun, & Bao, 2014)

I det inkluderade materialet beskrivs hur spatiala data i geografiska informationssystem kan skyddas genom rollbaserad åtkomstkontroll med datapositionsavgränsning.

5.3.2 Koncept B: Geografisk användarpositionering



Figur 12: Antal inkluderade verk som per år behandlar konceptet geografisk användarpositionering

I figur 12 ovan illustreras behandlingen av konceptet geografisk användarpositionering i det inkluderade materialet, fördelat på år för publicering. Konceptet har fram till och med 2012 berörts av kring hälften av de inkluderade verken varje år.

I GEO-RBAC finns två typer av användarposition, en geografisk position och en logisk position (se under *Annan användarpositionering*). Den geografiska positionen inhämtas från en mobil enhet med stöd för GPS-positionering och representeras av en icke typbestämd geometrisk figur, exempelvis en punkt eller en polygon. (Bertino, Catania, Damiani, & Perlasca, 2005)

Även LRBAC möjliggör en varierande detaljnivå för en position, vilket baseras på att en position definieras som en icke tom samling punkter och då på lägsta möjliga detaljnivå utgörs av endast en punkt. LRBAC sammankopplar till skillnad från GEO-RBAC också platser till rolltilldelningar och behörigheter, och roller kan definieras att endast kunna tilldelas till användare som befinner sig på en viss plats (Ray, Kumar, & Yu, LRBAC: A Location-Aware Role-Based Access Control Model, 2006).

I modellen STRBAC definieras i samma anda som i GEO-RBAC två typer av positioner, primitiv position och logisk position. En primitiv position definieras av en tredimensionell geometri med koordinater, vilken sedan kan ha relationer till andra primitiva positioner för att utgöra en logisk position (se under Annan användarpositionering). (Kumar & Newman, 2006)

Atluri och Chun (2007) beskriver att både användare och resurser har positionsattribut i deras modell GSAS. Genom detta kan användare exempelvis beredas åtkomst till data när de befinner sig på samma geografiska plats som de data denne vill nå. (Atluri & Chun, 2007)

Ray och Toahchoodee (2007) baserar i en efterföljande modell definitionerna för hur positioner representeras på hur det förklarats i LRBAC. (Ray & Toahchoodee, A Spatio-Temporal Role-Based Access Control Model, 2007)

I modellen STARBAC finns liksom i flera andra modeller både geografiska och logiska positioner. I STARBAC väljer författarna att anta att geografiska positioner inhämtas på ett korrekt vis, men vilka tekniker som skulle vara lämpliga för att inhämta sådana data diskuteras inte. En geografisk position består av en eller flera koordinatbaserade punkter. (Aich, Sural, & Majumdar, 2007)

Samuel et al. (2008) framhåller vikten av att under krisomständigheter hastigt kunna förändra rumsliga restriktioner. En användare som under krisförhållande befinner sig på en olycksplats behöver snabbt tilldelas åtkomsträttigheter trots att olycksplatsen inte ligger i användarens normala miljö. (Samuel, Ghafoor, & Bertino, 2008)

Aich et al. (2009) beskriver i sin modell ESTARBAC på samma sätt som flera tidigare presenterade modeller hur positioner kan fördelas på fysiska geografiska positioner, bestående av en samling koordinatbaserad punkter, och logiska positioner som identifierar platser som är av intresse för systemet. (Aich, Mondal, Sural, & Majumdar, 2009)

Shin och Atluri (2009) framhåller att en användares geografiska position vanligtvis inte behandlas med tillräckligt hög uppdateringsfrekvens för att kunna säkerställa att användarens position faktiskt är korrekt, och föreslår en lösning av problemet, se koncept *Rörlighet*. (Shin & Atluri, 2009)

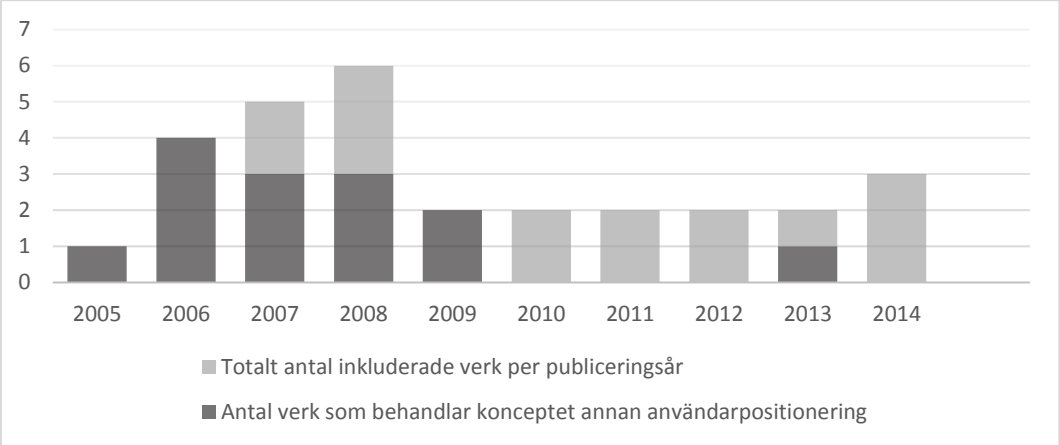
Chen et al. (2010) beskriver i sin föreslagna åtkomstkontrollmodell med stöd för rumsliga och tidsmässiga restriktioner att användares geografiska position kan användas för att bevilja eller avslå åtkomst beroende på om användaren befinner sig inom ett geografiskt område där denne har rättighet att nå den efterfrågade informationen. (Chen, Wang, Wen, Huang, & Chen, 2010)

Bertino och Kirkpatrick (2011) menar att en mobil enhets geografiska position dock inte ska förlitas på allt för mycket för att begränsa åtkomst. En sådan enhet kan tappas, lånas ut eller på annat sätt användas av någon som inte är avsedd att använda enheten. Det är i sådana fall av stor vikt att även andra mekanismer än positionsbaserade används för att kontrollera att den person som använder enheten faktiskt är dess ägare. (Bertino & Kirkpatrick, Location-Based Access Control Systems for Mobile Users - Concepts and Research Directions, 2011)

Ulltveit-Moe och Oleshchuk (2012) understryker påståendet om osäkerhet hos mobila enheters positionering, och menar att GPS-data som kommer från en mobil enhet kan förfalskas eller på annat sätt modifieras på ett sätt som medför att den inte är korrekt. De väljer dock att förbise detta faktum och presenterar ett tillvägagångssätt för att upprätthålla rollbaserad åtkomstkontroll baserad på en fysisk geografisk användarpositionering. (Ulltveit-Moe & Oleshchuk, 2012)

I det inkluderade materialet beskrivs hur en användares fysiska position kan användas för att avgöra huruvida denna ska beredas åtkomst till data eller inte.

5.3.3 Koncept C: Annan användarpositionering



Figur 13: Antal inkluderade verk som per år behandlar konceptet annan användarpositionering

I figur 13 ovan återges hur konceptet annan användarpositionering behandlats i det inkluderade materialet, fördelat på år för publicering. De flesta verk som behandlat konceptet är publicerade 2009 och tidigare.

GEO-RBAC tillhandahåller utöver stöd för geografiska användarpositioner också stöd för logiska användarpositioner. Den geografiska positionen kan *ligga i* ett visst område som representeras av en polygon, exempelvis en stad, och den polygon som representerar staden utgör då användarens logiska position. Modellen tillåter att den logiska positionens detaljnivå bestäms av rollens funktion, och exempelvis en taxiförares logiska position kan istället vara en punkt längs en vägsträcka. (Bertino, Catania, Damiani, & Perlasca, 2005)

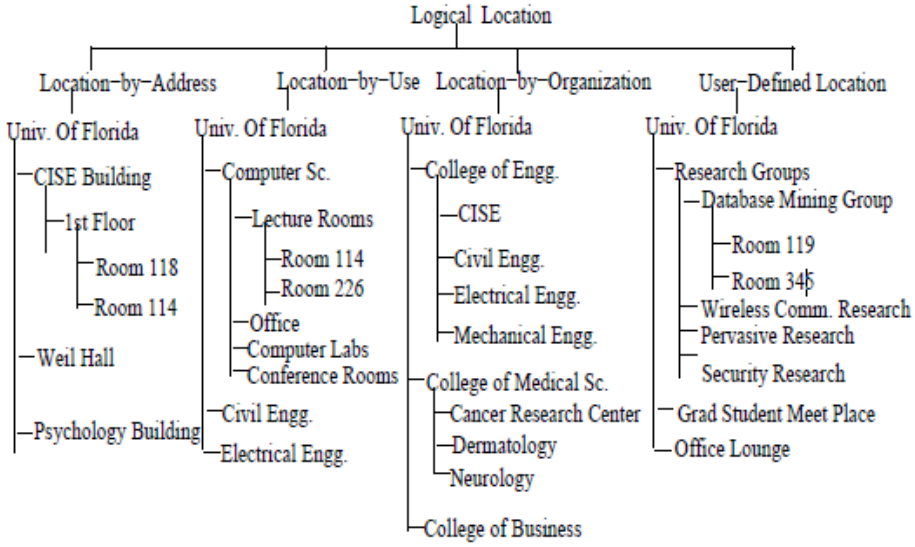
I den rollbaserade arkitektur för åtkomstkontroll av trådlösa nätverk som föreslås av Tomur och Erten (2006) förenklas användarpositionsbestämmandet till att lokalisera de anslutande klienterna baserat på den delmängd av nätverket som dess IP-adresser tillhör. Författarna uppger dock att GPS-positionering hade medfört mer stabilitet och en högre precisionsnivå. (Tomur & Erten, 2006)

LRBAC definierar tre topologiska relationer som kan uppstå mellan två positioner. En position kan antingen *ligga i* en annan position, *överlappa* en annan position eller *vara lika med* en annan position. En sådan relation mellan två geografiska positioner kan sedan utgöra en form av topologisk position. (Ray, Kumar, & Yu, LRBAC: A Location-Aware Role-Based Access Control Model, 2006)

I modellen PBAC används radioteknik för att avgöra huruvida en användare befinner sig inom någon av de fördefinierade zoner där åtkomst till en viss resurs är möjlig. PBAC använder inte geografisk positionering, utan baserar positioneringen snarare på närhet till den aktuella resursen och dess förbestämda åtkomstzon. Modellen är avsedd att användas i sjukhusmiljöer, och författarna menar att ett sådant tillvägagångssätt borgar för högre precision vid inomhuspositionering. (Gupta, Mukherjee, & Venkatasubramanian, 2006)

STRBAC tillhandhåller likt GEO-RBAC även logiska användarpositioner, vilka i modellen fördelas på fyra underkategorier. Den första, *position genom adress*, specificerar en position baserat på dess geografiska position. Den adress som en byggnad befinner sig på kan utgöra en samling positioner vilka den geografiska positionen kan befinna sig i. Den andra, *position genom användningsområde*, kopplar position till funktion, och exemplifieras med att vissa rum i en skola kan klassificeras som klassrum samtidigt som andra rum kan klassificeras som föreläsningssalar. *Position genom organisation* möjliggör att medlemmar av en organisation kan inneha andra behörigheter än icke-

medlemmar på den logiska positionen. Den sista underkategorin, *användardefinierad position*, används för att skapa skräddarsydda positioner som inte faller under någon av de andra kategorierna. De olika logiska underkategorierna illustreras i figur 14 nedan. (Kumar & Newman, 2006)



Figur 14: Hierarkin för de olika logiska positionstyperna (Kumar & Newman, 2006, s. 3)

Ray och Toahchoodee (2007) presenterade en modell, där logiska positioner baseras på den definition som presenterades i LRBAC-modellen. (Ray & Toahchoodee, A Spatio-Temporal Role-Based Access Control Model, 2007)

Fu och Xu (2007) beskriver hur användarens position i mobila miljöer kan bestämmas genom att lokalisera den nätverksnod, till vilken användaren är ansluten. Författarna menar att så är tillämpligt i miljöer där mobila enheter används, vilka allt efter att användaren förflyttar sig ansluter till nya nätverksnoder. (Fu & Xu, 2007)

I modellen STARBAC menar Aich et al. (2007) att en logisk position utgörs av en geometrisk form, uppbyggd av en samling punkter. En logisk position kan överlappa en annan logisk position, och en geografisk position kan befinna sig inom en logisk position. (Aich, Sural, & Majumdar, 2007)

Kulkarni & Tripathi (2008) beskriver i sin modell inte närmre hur positionering ska gå till, men modellen hanterar topologisk positionering där en användare kan befinna sig i ett visst rum eller på en viss avdelning på en arbetsplats. (Kulkarni & Tripathi, 2008)

Tahir (2008) inför i en förlängning av sin tidigare presenterade modell C-RBAC också topologiska positioner, och möjliggör en strukturering av dessa via hierarkiska relationer. Domäner används som en överstruktur för att samla topologiska positioner inom samma kategori för att tillåta att samma behörighet kan gälla också på flera positioner. (Tahir, 2008)

Compagnoni et al. (2008) använder i sin modell BACIR också logiska positioner, vilka de kallar omgivningar, för att möjliggöra kontrollerad nätverksåtkomst. Sådana omgivningar kan exempelvis vara ett klassrum eller en lounge på ett universitet, men också studenter som använder sin laptop befinner sig inom den logiska omgivningen laptop. (Compagnoni, Gunter, & Bidinger, 2008)

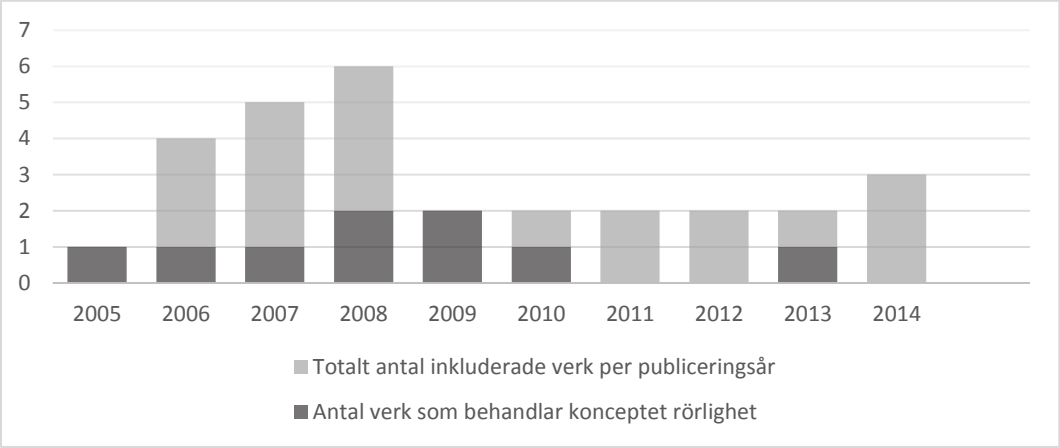
Aich et al. (2009) använder i sin modell ESTARBAC, på samma sätt som flera tidigare presenterade modeller, också logiska positioner. Sådana logiska positioner består av koordinatförsedda punkter,

vilka utgör platser som är av intresse för ett system. En användare kan topologisk befinna sig inom en logisk position. (Aich, Mondal, Sural, & Majumdar, 2009)

I modellen FPM-RBAC används inte användarens geografiska position, platsbestämmandet begränsas istället till att avgöras av den nätverksdomän till vilken användaren är uppkopplad. (Unal & Caglayan, 2013).

I det inkluderade materialet beskrivs hur annan användarpositionering än geografisk sådan kan användas för att avgöra huruvida en användare ska beredas åtkomst till data eller inte.

5.3.4 Koncept D: Rörlighet



Figur 15: Antal inkluderade verk som per år behandlar konceptet rörlighet

I figur 15 ovan illustreras behandlingen av konceptet rörlighet bland det inkluderade materialet fördelat på år för publicering. Konceptet har främst behandlats 2010 och tidigare.

Bertino et al. (2005) beskriver hur de i modellen GEO-RBAC förutsätter att användarpositioner kan förändras med tiden, men behandlar inte något särskilt tillvägagångssätt för att hantera detta. (Bertino, Catania, Damiani, & Perlasca, 2005)

I modellen PBAC, avsedd för sjukhusmiljöer, hanteras personalens rörlighet genom användandet av flerskiktiga närhetszoner. Gupta et. al (2006) beskriver detta i ett exempel, där åtkomst till en specifik resurs kräver att användaren befinner sig inom den innersta zonen. Den beviljade åtkomsten till resursen återkallas dock inte förrän användaren lämnat den omslutande yttre zonen. Att använda en yttre omslutande närhetszon medför också att till exempel en sjuksköterska som befinner sig i den inre zonen dessutom snabbt kan underrättas om att en läkare närmar sig när denne träder in i den yttre zonen. (Gupta, Mukherjee, & Venkatasubramanian, 2006)

Fu och Xu (2007) behandlar användares rörlighet genom att den nätverksnod till vilken användaren är ansluten förbyts när en annan nätverksnod är mer lämplig. (Fu & Xu, 2007)

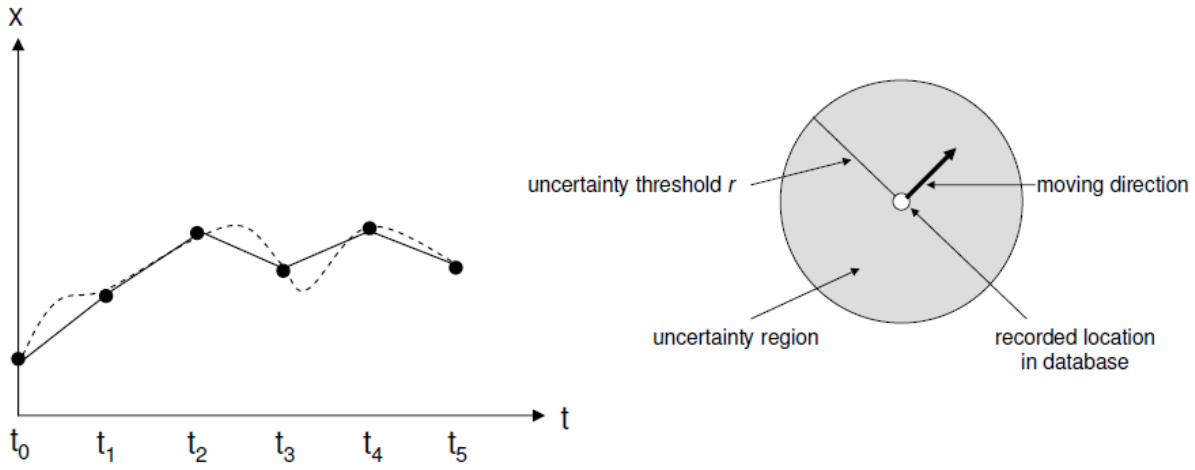
Kulkarni och Tripathi (2008) introducerar konceptet kontextskydd, vilket de beskriver som en mekanism som övervakar aktiva sessioner och avbryter dessa när de rumsliga och tidsmässiga villkor som ställs inte längre uppfylls. De exemplifierar detta genom att beskriva ett typfall där en sjuksköterska endast har åtkomst till en resurs när en läkare närvarar. Då läkaren sedan lämnar sjuksköterskan ensam i rummet utgör läkarens avlägsnande en kontextuell förändring som innebär att de kontextuella villkoren inte längre är uppfyllda. Kontextskyddsmekanismen identifierar att villkoren inte längre uppfylls, och avbryter sjuksköterskans aktiva session. Sjuksköterskan har därmed inte längre åtkomst till den aktuella resursen. (Kulkarni & Tripathi, 2008)

Kulkarni och Tripathi (2008) beskriver vidare hur rollvalideringsvillkor kan användas för att återkalla rollmedlemskap när en medlem inte längre bör inneha en roll. De illustrerar detta med ett exempel, där medlemskap i rollen NurseOnDuty möjliggör åtkomst till data i ett patientinformationssystem. När en sjuksköterska som är medlem av rollen lämnar avdelningen eller när en viss tidsperiod löpt ut uppfyller sjuksköterskan inte längre rollvalideringsvillkoren, och medlemskapet återkallas. (Kulkarni & Tripathi, 2008)

Compagnoni et al. (2008) definierar i sin modell BACIR två rörelser som är relevanta för logiska positioner (i modellen benämnt omgivningar); inträde och utträde. Genom inträde i en omgivning öppnas en ny kommunikationskanal till nätverket, medan ett utträde medför att kanalen stängs. (Compagnoni, Gunter, & Bidinger, 2008)

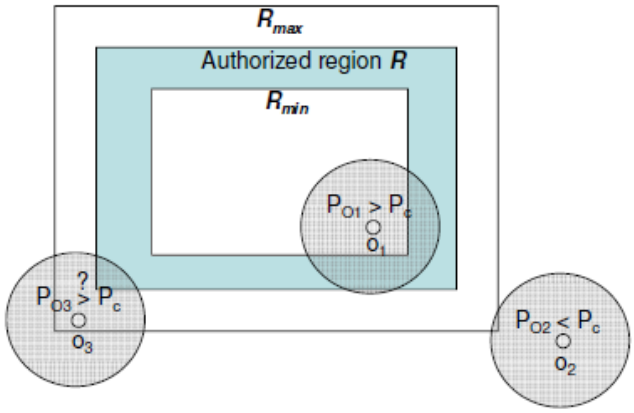
I modellen ESTARBAC hanteras användares rörlighet genom att lagra senast kända position, vilken åtföljer en skickad begäran om åtkomst till en resurs tillsammans med den tidpunkt då användarpositionen senast uppdaterats. Åtkomstkontrollmekanismen kan då utvärdera huruvida mottagen begäran ska beviljas eller inte. (Aich, Mondal, Sural, & Majumdar, 2009)

Shin och Atluri (2009) menar att position hos användare som rör sig inte lagras med tillräckligt stor precision. I syfte att minimera antalet positionsuppdateringar hålls istället en ungefärlig position, baserat på den senast kända positionen. Shin och Atluri (2009) framhåller att detta kan utgöra en säkerhetsrisk i system som innehåller känslig information. De menar att mellan positions-uppdateringarna är den egentliga positionen okänd och kan antas befinna sig var som helst inom ett visst intilliggande spann, vilket illustreras till vänster i figur 16 nedan. Det kan dock inte sägas med garanterad säkerhet att spannet är korrekt. Som illustreras till höger i figur 16 utgör spannet bara den troliga positionen, även om det är möjligt att den verkliga positionen egentligen befinner sig inom det osäkra området.



Figur 16: Positionshistorik och möjliga avvikelser mellan uppdateringar, samt hur dessa beräknas (Shin & Atluri, 2009, s. 5)

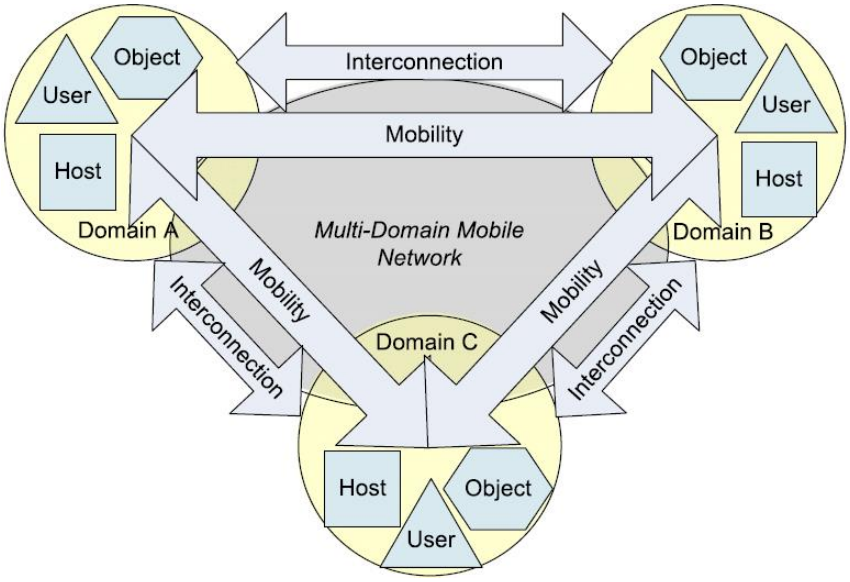
Shin och Atluri (2009) föreslår en lösning på nämnda problem genom att söka ut två regioner, en inre region som användaren förmodligen befinner sig i och en yttre region som användaren säkerställt befinner sig i. Genom denna ansats kan behörigheter beviljas endast om den auktoriserade regionen befinner sig inom användarens säkerställda område, vilket illustreras i figur 17 nedan. (Shin & Atluri, 2009)



Figur 17: Minimalt och maximalt möjligt område (Shin & Atluri, 2009, s. 10)

Kirkpatrick och Bertino (2010) beskriver också hur de hanterar förekomsten av användare som förflyttar sig utanför den geografiska avgränsning där en roll definierats, och beviljad åtkomst i sådana fall ska upphävas. De beskriver en modell för åtkomstkontinuitet där användarna tvingas att med jämna mellanrum bekräfta sin position. I sådana fall där en användare plötsligt befinner sig utanför det tillåtna området är denne oförmögen att bekräfta en godkänd position, och användarens existerande behörighet återkallas. (Kirkpatrick & Bertino, Enforcing spatial constraints for mobile RBAC systems, 2010)

I modellen FPM-RBAC, presenterad av Unat och Caglayan (2013), behandlas rörlighet som ett fenomen som uppstår när en mobil enhet ansluter till en ny domän i ett mobilt nätverk. Det är således inte användarens egentliga geografiska position som behandlas i modellen, utan snarare den domän i nätverket till vilket användaren är ansluten (Unal & Caglayan, 2013). Figur 18 nedan illustrerar hur rörligheten presenteras i FPM-RBAC.

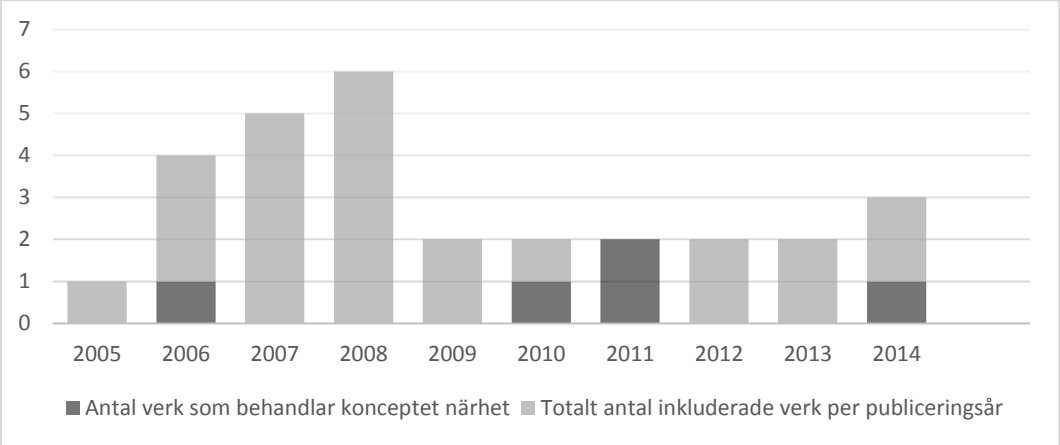


Figur 18: Rörlighet i FPM-RBAC (Unal & Caglayan, 2013, s. 331)

Om en användare förflyttar sig till en nätverksdomän loggas denne in, och om användaren förflyttar sig ut ur domänen loggas denne ut. (Unal & Caglayan, 2013)

I det inkluderade materialet beskrivs hur användares rörlighet påverkar den geografiska avgränsningen, och hur denna kan hanteras i åtkomstkontrollen.

5.3.5 Koncept E: Närhet



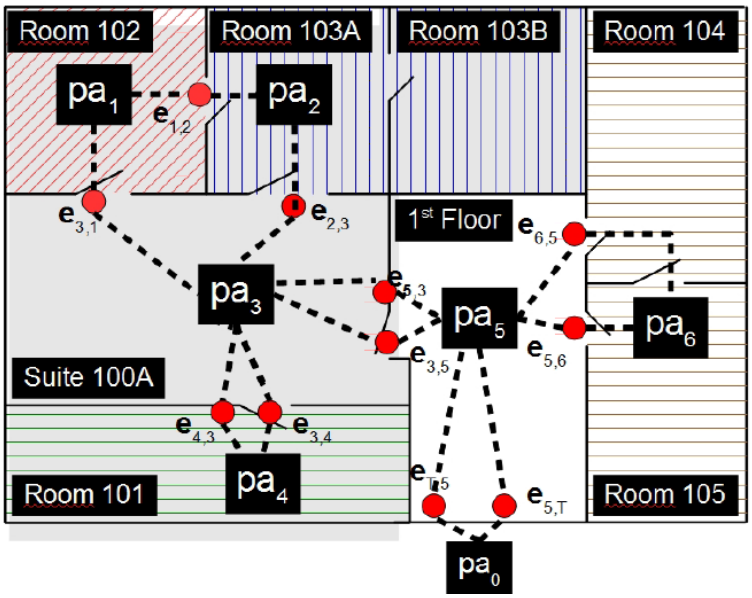
Figur 19: Antal inkluderade verk som per år behandlar konceptet närhet

I figur 19 ovan illustreras hur konceptet närhet behandlats i det inkluderade materialet fördelat på år för publicering.

PBAC (Proximity Based automated Access Control) är en modell avsedd att förbättra arbetsflödet hos akuta vårdavdelningar genom att automatisera åtkomstkontrollen. Medicinsk personal bereds åtkomst till resurser baserat på närhet till den aktuella resursen samt vilken roll som innehas av den personal som efterfrågar resursen. Närheten till resursen bestäms av användarens position och en fördefinierad zon kring resursen, vilken personal måste befinna sig i för att tillåtas åtkomst. Då modellen är avsedd att användas i sjukhusmiljöer inomhus läggs vikt vid att närhetszonerna definieras i tre dimensioner. I den prototyp som tagits fram och testats i verklig miljö har Ultra Wide Band-teknik använts för att fastställa användarposition och närhetszon. (Gupta, Mukherjee, & Venkatasubramanian, 2006)

Även Kirkpatrick och Bertino (2010) föreslår en arkitektur ämnad att användas i inomhusmiljöer som exempelvis sjukhus. De utgår därför från att den enhet som lagrar positionsinformation är fast installerad i byggnaden och använder så kallad NFC-teknologi (Near Field Communication) för att avgöra positioner och tilldela åtkomst baserat på närhet till efterfrågad resurs. (Kirkpatrick & Bertino, Enforcing spatial constraints for mobile RBAC systems, 2010)

I modellen Prox-RBAC, en vidareutveckling av GEO-RBAC, införs också konceptet närhet i den rollbaserade åtkomstkontrollen. Exempelvis kan ett system som hanterar känsliga data enligt Prox-RBAC förhindra åtkomst till känsliga dokument såvida någon civilperson är närvarande. Modellen är främst avsedd för inomhusbruk, och bygger på en rumslig modell där regioner fördelas på olika skyddade regioner. En skyddad region är enligt Prox-RBAC ett fysiskt avgränsat område, exempelvis ett rum eller en våning, med ett begränsat antal ingångar som kräver auktorisering vid inträde, vilket illustreras i figur 20 nedan.

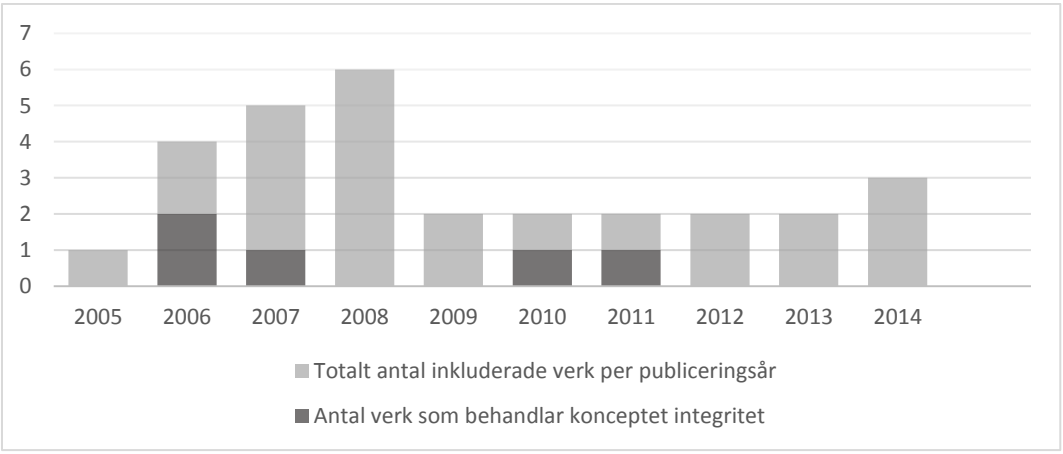


Figur 20: Rumslig modell i Prox-RBAC (Kirkpatrick, Damiani, & Bertino, Prox-RBAC: A Proximity-based Spatially Aware RBAC, 2011)

Gupta et al. (2014) definierar fem olika typer av närhet; geografisk, attributbaserad, social, nät och tidsmässig närhet. Geografisk närhet innebär att två objekt befinner sig inom ett givet avstånd i den rumsliga dimensionen. Attributbaserad närhet uppstår när två objekt delar en eller flera attribut eller befinner sig i rumsliga områden som har samma attribut. Social närhet innebär att två objekt i en topologisk karta befinner sig inom ett visst antal stegs avstånd. Nätnärhet är när två objekt samtidigt närvarar i samma uppkopplade kommunikationssession. Tidsmässig närhet är när två objekt närvarar vid händelser som uppstår inom en avgränsad tidsperiod. Författarna presenterar en modell som är tillräckligt generell för att hantera samtliga av ovan nämnda typer av närhet. (Gupta, Kirkpatrick, & Bertino, 2014)

I det inkluderade materialet beskrivs hur avståndet mellan olika objekt kan användas för att specificera åtkomstkontrollen.

5.3.6 Koncept F: Integritet



Figur 21: Antal inkluderade verk som per år behandlar konceptet integritet

I figur 21 ovan illustreras hur konceptet integritet behandlas i de inkluderade verken fördelat på år för publicering. Konceptet har bland inkluderat material senast behandlats 2011.

Ray et al. (2006) framhåller vikten av att hålla platsinformation skyddad, och menar att lokaliserande information som läcker kan orsaka såväl intrång på en användares personliga integritet som att utgöra en grund för attacker från personer med ont uppsåt. (Ray, Kumar, & Yu, LRBAC: A Location-Aware Role-Based Access Control Model, 2006)

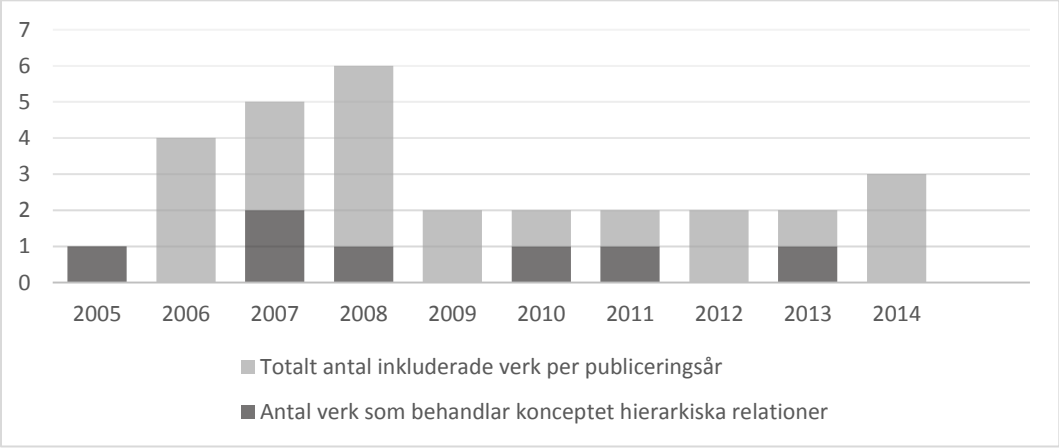
Också Kumar och Newman (2006) understryker känsligheten hos platsinformation. I modellen STRBAC inför de en ny typ av synlighetsbehörighet i syfte att möjliggöra beslut kring på vilken detaljnivå en medlem av en viss roll ska kunna inhämta positionen hos ett visst objekt (Kumar & Newman, 2006).

Atluri och Chun (2007) menar att positionsdata för användare och objekt inte är det enda att tänka på när det gäller integritet och geografiska data, och beskriver vidare att även högupplösta och detaljerade geospatiala satellitbilder kan ligga till grund för intrång på personlig såväl som nationell säkerhet. De presenterar i och med GSAS en modell som tillåter restriktion av åtkomsträttigheter baserat på sådana satellitbilders upplösning, hur stor yta som täcks av varje pixel i en bild. (Atluri & Chun, 2007)

Kirkpatrick och Bertino (2010) föreslår en arkitektur där en användares integritet skyddas genom att låta användarens roll fungera som en pseudonym för dennes identitet. De menar att om mappningen mellan användare och roller och kontrollen av åtkomst gentemot en roll sker på två skilda servrar är det enbart den server som hanterar användarrollmappningen som faktiskt behöver kännedom om användarens identitet. I den fortsatta behandlingen av användarens åtkomstbegäran berörs endast användarens rolltillhörighet, tillsammans med platsinformationen. Identitetsdata skyddas i kommunikationen med rollmappningsservern genom kryptering med en nyckel, vilken endast användaren och servern känner till. (Kirkpatrick & Bertino, Enforcing spatial constraints for mobile RBAC systems, 2010)

I det inkluderade materialet understryks vikten av att beakta integritet i behandlandet av geografiska data, och åtgärder för att förbättra detta föreslås.

5.3.7 Koncept G: Hierarkiska relationer



Figur 22: Antal inkluderade verk som per år behandlar konceptet hierarkiska relationer

I figur 22 ovan illustreras hur konceptet hierarkiska relationer behandlas i det inkluderade materialet, fördelat på år för publicering. Första gången konceptet behandlas i de inkluderade verken är 2005.

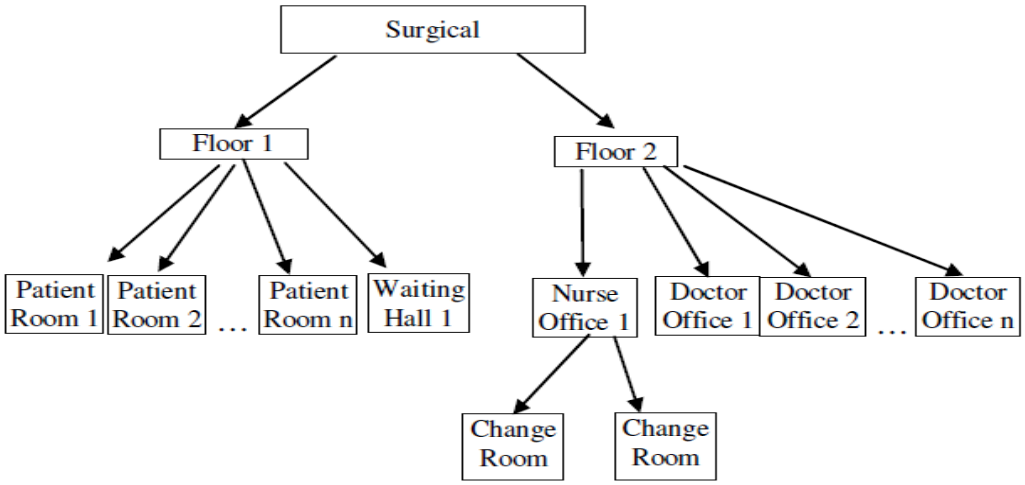
Förutom att på samma vis som RBAC stödja rollhierarkier där roller kan ärva behörigheter från andra roller i ett nedstigande led presenterar GEO-RBAC också konceptet startad roll. Om en ärvande roll

startas, startas också den roll från vilken den startade rollen ärver. Konceptet rollschema införs också i modellen, vilket innebär att (Bertino, Catania, Damiani, & Perlasca, 2005)

GSAS stödjer också en rollhierarki, där en rumslig och tidsmässig roll kan ärva rättigheter från en annan rumslig och tidsmässig roll (Atluri & Chun, 2007).

Ray och Toahchoodee (2007) beskriver en rad olika typer av hierarkiska relationer som ingår i deras modell. En senior roll kan från en junior roll ärva behörigheter, vilket kan ske både genom att ärva också tids- och rumsrestriktioner eller inte. En användare som kan aktivera en senior roll kan också aktivera en junior roll. Detta kan också eventuellt innefatta restriktioner som begränsar aktiveringen till samma tid och plats som den juniora rollen kan användas. (Ray & Toahchoodee, A Spatio-Temporal Role-Based Access Control Model, 2007)

Tahir (2008) introducerar i en vidareutveckling av sin tidigare presenterade modell C-RBAC hierarkiska relationer mellan positioner, domäner och ändamål. Ett objekt som befinner sig under ett annat i hierarkin övertar också egenskaper som det övre objektet uppbär (Tahir, 2008). I figur 23 nedan illustreras hur hierarkiska relationer mellan topologiska positioner kan te sig på en kirurgisk avdelning i ett sjukhus.



Figur 23: Hierarkiska relationer mellan topologiska positioner (Tahir, 2008, s. 34)

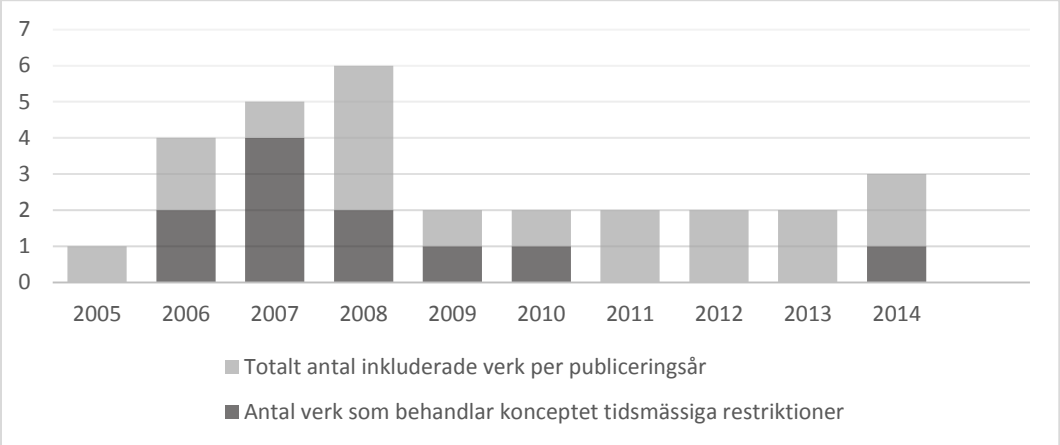
I den modell som presenteras av Chen et al. (2010) är det möjligt för roller ingå i ett hierarkiskt förhållande på samma sätt som i den standardiserade RBAC-modellen. (Chen, Wang, Wen, Huang, & Chen, 2010)

Också Kirkpatrick, Damiani och Bertino (2011) beskriver i sin modell Prox-RBAC, baserad på den tidigare presenterade modellen GEO-RBAC, hur hierarkiska relationer är möjliga mellan olika skyddade regioner. Ett rum kan tillexempel hierarkiskt organiseras under en våning. (Kirkpatrick, Damiani, & Bertino, Prox-RBAC: A Proximity-based Spatially Aware RBAC, 2011)

Modellen FPM-RBAC tillhandahåller liksom den standardiserade RBAC stöd för rollhierarkier. Utöver detta introducerar modellen även stöd för objekttypshierarkier, att objekt sammankopplas med mer generella objekttyper som kan ärva attribut från varandra. (Unal & Caglayan, 2013).

I det inkluderade materialet beskrivs hur hierarkiska relationer kan implementeras i rollbaserad åtkomstkontroll med geografisk avgränsning. Det kan handla om huruvida roller kan ärva egenskaper från andra roller, men även hur olika rumsliga områden kan organiseras hierarkiskt.

5.3.8 Koncept H: Tidsmässiga restriktioner



Figur 24: Antal inkluderade verk som per år behandlar konceptet tidsmässiga restriktioner

Figur 24 ovan illustrerar hur konceptet tidsmässiga restriktioner behandlas i det inkluderade materialet. Konceptet har främst behandlats före 2010.

I den modell för åtkomstkontroll till trådlösa nätverk som beskrivs av Tomur och Erten (2006) hanteras tidsaspekten genom att göra åtkomsten till det trådlösa nätverket möjlig endast under fördefinierade tidsperioder. (Tomur & Erten, 2006)

Kumar och Newman (2006) tillhandahåller också i modellen STRBAC möjlighet att tidsbegränsa åtkomst till resurser. Dagliga, veckoliga, månatliga och årliga perioder definieras som återkommande tidsintervall, vilka kan sammankopplas med de behörigheter som en roll innehar. (Kumar & Newman, 2006)

Atluri och Chun (2007) introducerar i modellen GSAS tidskonceptet för de spatiala data som åtkomstkontrollen är tänkt att skydda. Användare kan begränsas till att endast beredas åtkomst till sådana spatiala data som innehar tidsstämplar inom ett sådant tidsspann som användaren tilldelats åtkomst. (Atluri & Chun, 2007)

Ray och Toahchodee (2007) betonar att det är viktigt att skilja på olika typer av tidsmässig information. De identifierar två typer av tidsmässig information med olika betydelser, tidsögonblick och tidsintervall. Tidsögonblick definieras som en distinkt tidpunkt längs en tidslinje, och tidsintervall definieras som en uppsättning tidsinstanser antingen kan efterfölja varandra kontinuerligt eller icke kontinuerligt genom avbrott. (Ray & Toahchoodee, A Spatio-Temporal Role-Based Access Control Model, 2007)

Fu och Xu (2007) använder tidsperioder inom vilka en användare tillåts åtkomst. En aktiv behörighet förfaller när tidsperioden passerat. (Fu & Xu, 2007)

Aich et al. (2007) uppger själva att deras modell STARBAC så vitt de vet är den första konkreta modellen för rollbaserad åtkomstkontroll med stöd för både rumsliga och tidsmässiga restriktioner. Den centrala tanken hos STARBAC är att föra samman rumsliga och tidsmässiga restriktioner genom att introducera spatiotemporala villkor i syfte att kontrollera åtkomsten vid en viss punkt i tid och rum. Konceptet spatiotemporala villkor, som är uppbyggt av en samling tidsmässiga villkor och en samling rumsliga villkor, fungerar som ett fönster vilket den tidsmässiga och rumsliga punkten måste befinna sig inom för att beredas åtkomst. (Aich, Sural, & Majumdar, 2007)

Samuel et al. (2008) menar att arbete under krisomständigheter kräver att tidsmässiga restriktioner enkelt kan förändras. Under en kris kan en roll behöva arbeta under tider som avviker från det normala, och under en längre varaktighet än vänligt. (Samuel, Ghafoor, & Bertino, 2008)

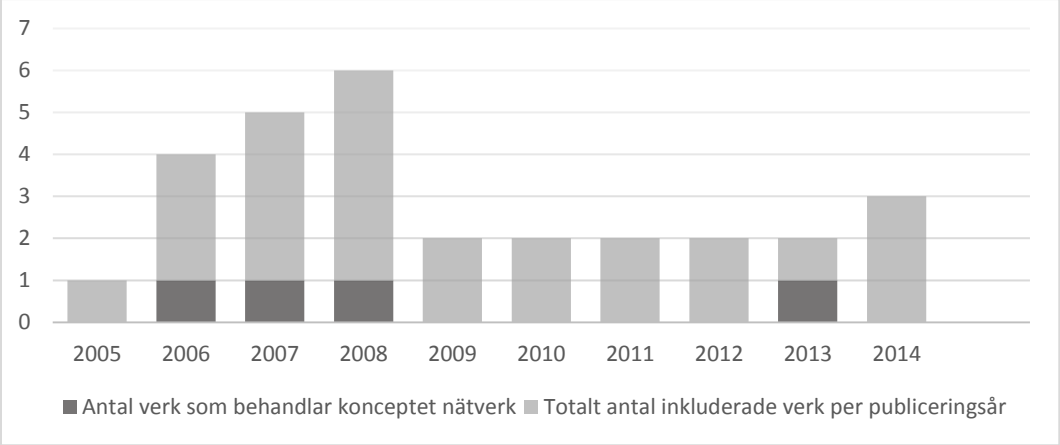
Kulkarni och Tripathi (2008) innefattar tidsaspekten i sin modell, men beskriver endast på en hög nivå hur behörigheter ska vara möjliga att endast gälla under redan fördefinierade tidsperioder. (Kulkarni & Tripathi, 2008)

I modellen ESTARBAC kan en användares möjlighet begränsas att påta sig en roll begränsas tidsmässigt, istället för att tidsmässigt begränsa åtkomsten till resursen. (Aich, Mondal, Sural, & Majumdar, 2009)

Chen et al. (2010) presenterar likaså en modell där åtkomst till objekt kan begränsas till endast visa tidsperioder (Chen, Wang, Wen, Huang, & Chen, 2010), en möjlighet också åtkomstkontrollmodellen MSTAC erbjuder (Zhang, Gao, Ji, Sun, & Bao, 2014).

I det inkluderade materialet beskrivs hur tid kan användas för att utöver rumsliga aspekter ytterligare förhöja den detaljrikedom med vilken åtkomstkontrollen kan avgöra åtkomst till data.

5.3.9 Koncept I: Nätverk



Figur 25: Antal inkluderade verk som per år behandlar konceptet nätverk

I figur 25 illustreras hur konceptet nätverk behandlas i det inkluderade materialet.

Tomur och Erten (2006) föreslår en rollbaserad arkitektur för åtkomstkontroll av trådlösa nätverk på företagsnivå baserad på tids- och platsinformation, som genom att implementera sedan tidigare väl beprövade säkerhetstekniker förminskar risken för sårbarheter. Användarens position bestäms inte geografiskt, utan lokaliseras istället genom det subnät vilken användarens IP-adress tillhör. (Tomur & Erten, 2006)

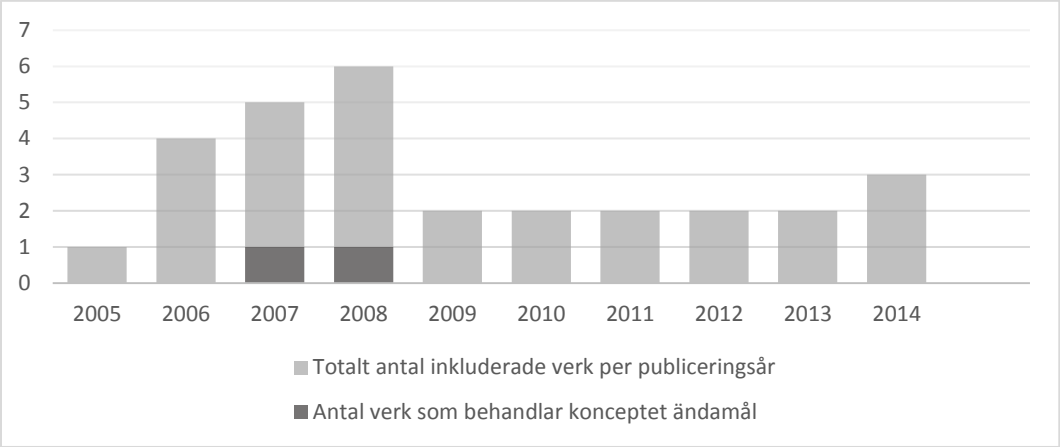
Fu och Xu (2007) bygger sin åtkomstkontrollmodell kring mobila enheter i nätverksmiljöer. En användare med en mobil enhet är inte ständigt uppkopplad till samma nätverksnod, den uppkopplade nätverksnoden förbyts snarare när användaren befinner sig närmre en annan nätverksnod. (Fu & Xu, 2007)

Compagnoni et al. (2008) definierar med modellen BACIR ett tillvägagångsätt för att upprätthålla rollbaserad åtkomstkontroll med geografisk avgränsning i syfte att styra åtkomsten av nätverk. I modellen används det logiska begreppet omgivning. En omgivning kan exempelvis vara ett klassrum på ett universitet, men också rent logiska omgivningar ingår. En rent logisk omgivning kan vara laptop, i vilken samtliga studenter som ansluter till nätverket genom sina bärbara datorer befinner

sig. Detta till skillnad från sådana studenter som kanske befinner sig i ett klassrum, men på universitets stationära datorer. (Compagnoni, Gunter, & Bidinger, 2008)

Unal och Caglayan (2013) visar i sin modell FPM-RBAC hur rollbaserad åtkomstkontroll kan implementeras för att kontrollera åtkomst i mobila nätverk. Användarens position bestäms inte heller i FPM-RBAC av den precisa fysiska geografiska positionen, utan snarare av den del av ett mobilt nätverk som användarens enhet är uppkopplad till. (Unal & Caglayan, 2013)

5.3.10 Koncept J: Ändamål

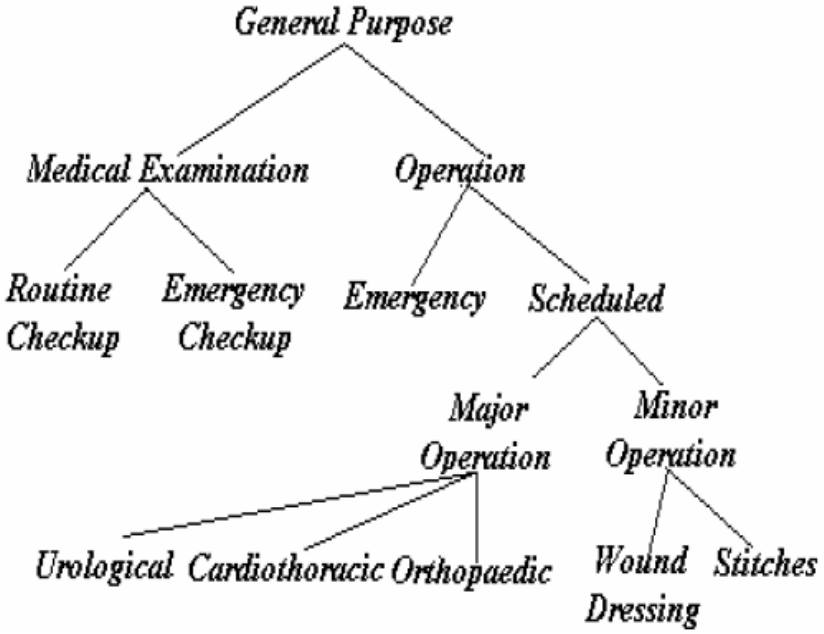


Figur 26: Antal inkluderade verk som per år behandlar konceptet ändamål

I figur 26 ovan illustreras hur konceptet ändamål behandlats i det inkluderade materialet. Konceptet har endast behandlats i två verk, 2007 och 2008.

Tahir (2007) menar att ändamål beskriver den anledning, av vilken en organisations resurser används. Ändamål är en samling fördefinierade syften, och kan vara exempelvis *administration*, *utveckling*, *kontakt* eller *telemarketing*. Ändamål kan antingen vara tillåtna eller förbjudna, och organiseras i en hierarki för att underlätta hanteringen av dessa. Genom att använda ändamål förhöjs graden av anpassningsbarhet hos den rollbaserade åtkomstkontrollen. (Tahir, 2007)

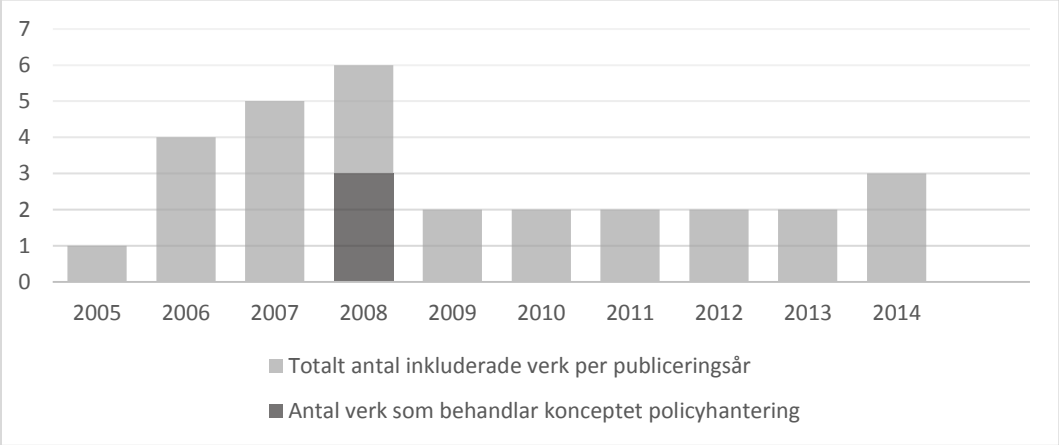
I en efterföljande modell introducerar Tahir (2008) också konceptet hierarkiska relationer mellan sådana ändamål. Ett underordnat ändamål uppbär också de egenskaper som dess överordnade ändamål uppbär (Tahir, 2008). I figur 27 nedan illustreras hur sådana hierarkiska relationer kan struktureras mellan ändamål i en sjukhusmiljö.



Figur 27: Hierarkiska relationer mellan ändamål (Tahir, Hierarchies in Contextual Role-Based Access Control Model (C-RBAC), 2008, s. 39)

I det inkluderade materialet beskrivs hur det syfte med vilket en användare vill beredas åtkomst till resurser kan användas för att avgöra huruvida detta ska tillåtas eller inte.

5.3.11 Koncept K: Policyhantering



Figur 28: Antal inkluderade verk som per år behandlar konceptet policyhantering

I figur 28 ovan illustreras hur konceptet policyhantering hanteras i det inkluderade materialet. Konceptet har behandlats av tre inkluderade verk, varav samtliga publicerats 2008.

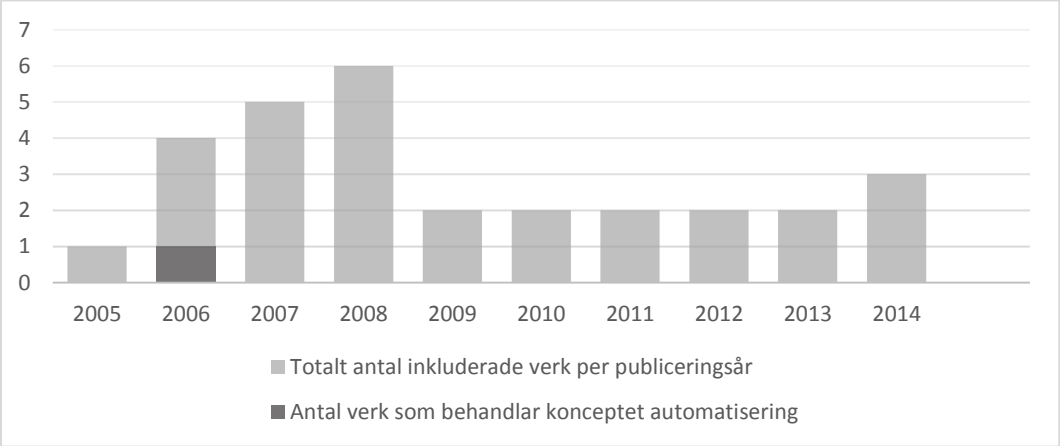
Samuel et al. (2008) diskuterar hur rollbaserade åtkomstkontrollpolicys kan anpassas efter att möta de behov som uppstår vid kris- och katastrofsituationer, och nämner orkanen Katrina som lamslog delar av USA 2005 som ett exempel på en sådan situation. De introducerar i syfte att hantera sådana särskilda situationer de två koncepten *normala restriktioner* och *krisrestriktioner*. Normala restriktioner är sådana restriktioner som används i det vardagliga arbetet hos en organisation, medan krisrestriktioner är skräddarsydda för katastrofsituationer och endast aktiveras när en sådan uppstår. (Samuel, Ghafoor, & Bertino, 2008)

Bhatti et al. (2008) presenterar ett verktyg de konstruerat i syfte att hantera rollbaserade åtkomstkontrollpolicys i den tidigare presenterade modellen GEO-RBAC, liksom arkitekturen hos detta verktyg. Verktyget visar genom ett grafiskt användargränssnitt hur geometrier för roller och behörigheter relaterar till varandra. (Bhatti, Damiani, Bettis, & Bertino, 2008)

Damiani et al. (2008) diskuterar likaså hur den tidigare presenterade modellen GEO-RBAC ska kunna administreras, och presenterar i detta syfte modellen GEO-RBAC Admin. Modellen möjliggör bland annat att geometriskt utformade domäner kan organiseras i en hierarkisk struktur. Damiani et al. (2008) visar även upp en prototyp på ett verktyg som implementerar GEO-RBAC Admin. (Damiani, Bertino, & Silvestri, 2008)

I det inkluderade materialet beskrivs hur policyer för rollbaserad åtkomstkontroll med geografisk avgränsning kan hanteras, och prototyper för detta presenteras.

5.3.12 Koncept L: Automatisering



Figur 29: Antal inkluderade verk som per år behandlar konceptet automatisering

I figur 29 ovan illustreras hur konceptet automatisering behandlas i det inkluderade materialet. Konceptet har endast behandlats en gång, i ett verk som publicerats 2006.

PBAC, Proximity Based automated Access Control, presenteras som en åtkomstkontrollmodell som syftar till att automatisera befintliga arbetsflöden i sjukhusmiljöer genom att minska behovet av manuella åtgärder för att garantera att känslig patientinformation behandlas på ett säkert vis. Genom att automatisera åtkomstkontrollen till att automatiskt beviljas när behörig sjukhuspersonal befinner sig i närheten av den resurs denne vill nå menar författarna att vårdgivare får mer tid att fokusera på sitt egentliga arbete, patienten. (Gupta, Mukherjee, & Venkatasubramanian, 2006)

6. Slutsatser och diskussion

I följande kapitel besvaras arbetets frågeställningar. Diskussioner förs också kring arbetets genomförande, och detta utvärderas kritiskt.

6.1 Områdesöversikt

Arbetets första frågeställning löd: *Vad är idag ”state-of-the-art” inom ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning?*

Den systematiska litteraturgenomgången har visat att *state-of-the-art* inom ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning generellt utgörs av två större inriktningar, användarpositionsavgränsning och datapositionsavgränsning.

I användandet av användarpositionsavgränsning kontrolleras åtkomsten till geografiska data såväl som åtkomsten till icke rumsliga data baserat på användarens fysiska eller logiska position. Användarens fysiska position representeras av ett geometriskt objekt där dess koordinater bestämmer det geografiska läget, medan användarens logiska position kan bestämmas av dennes topologiska relation till sin omgivning. Inom den rollbaserade åtkomstkontrollen med användarpositionsavgränsning är det frekvent förekommande att kombinera positionsavgränsningar med tidsmässiga restriktioner, där den tidpunkt då användaren söker nå data måste befinna sig inom ett fördefinierat tidsspann.

Genom att använda rollbaserad åtkomstkontroll med datapositionsavgränsning hanteras i stället kontrollen av åtkomst till geografiska data, och en användare beviljas åtkomst endast till sådana data som geografiskt befinner sig inom en fördefinierad yta där dennes roll tilldelats behörighet för åtkomst. Användarens positions behandlas inte, men datapositionsavgränsning är möjlig att kombinera med användarpositionsavgränsning för att uppnå än högre auktoriseringsprecision.

En stor del av det material som ingått i studien har publicerats mellan 2006 och 2008, vilket kan sättas i samband med hur flera författare beskriver att den samtidiga framväxten av mobila enheter med positioneringsmöjligheter ökat behovet av rollbaserad åtkomstkontroll med geografisk avgränsning. Denna trend har tagit fokus från kontrollen av åtkomst till geografiska data, även om datapositions-avgränsning åter tagit plats under de senaste åren.

6.2 Forsknings- och utvecklingsbehov inom ämnesområdet

Arbetets andra frågeställning löd: *Vilka forsknings- och utvecklingsbehov finns idag inom ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning?*

Under genomförandet av den systematiska litteraturgenomgången har ett antal forsknings- och utvecklingsbehov identifierats. Det mest framträdande området i behov av vidare utveckling utgörs av problemet kring hur tillförlitligheten hos positionsdata till en högre grad kunna säkerställas. Vidare arbete krävs också för att kunna bemöta hur åtkomstkontrollen ska hantera oförutsedda kris-situationer, liksom för att hantera de aspekter som hierarkiska relationer kan medföra. I efterföljande segment beskrivs de utvecklingsbehov som identifierats mer utförligt.

Korrekthet hos positionsdata

Bertino et al. (2005) föreslår vidare studier kring autentiseringen av platsinformation. Ulltveit-Moe och Oleshchuk (2012) menar också att det krävs vidare arbete för att säkerställa att geografiska användarpositioner som avgörs med mobila enheters inmätta GPS-data faktiskt är korrekta. Sådana data enkelt kan modifieras eller förfalskas i till exempel en mobiltelefon (Ulltveit-Moe & Oleshchuk, 2012). Då Kirkpatrick och Bertino (2010) menar att vidare arbete krävs för att med en högre grad av

precision och större tillförlitlighet kunna avgöra när rumsliga avgränsningar korsas av en användare skulle detta förbättra också den rörlighetsbaserade åtkomstkontrollen. I den förenklade användar-positioneringsmekanism för trådlösa nätverk baserat på nätverksinformation som presenteras av Tomur & Erten (2006) hade införandet av en kompletterande GPS-positionering bidragit till en bättre lokaliseringsprecision och därmed en högre säkerhetsnivå (Tomur & Erten, 2006). Kirkpatrick och Bertino (2011) menar vidare att det finns ett behov av att vidareutveckla kontrollen av att den som använder en mobil enhet med positionsbaserad åtkomstkontroll faktiskt är dess ägare.

Policyhantering och administration

Samuel et al. (2008) resonerar kring hur katastrofer, stora olyckor och andra krissituationer medför nya svårigheter för upprätthållandet av åtkomstkontroll. De menar att det är svårt att förutse och i förväg komponera åtkomstpolicys som är tillämpliga på alla tänkbara krissituationer, vilket situationen vid orkanen Katrina och tsunamin i Asien 2004 används som exempel på (Samuel, Ghafoor, & Bertino, 2008). Utformningen av ett generellt ramverk över hur rollbaserad åtkomstkontroll med okända restriktioner kan utformas för användning vid kris- och katastrofsituationer kan därför utgöra ett förslag på vidare studier.

Hierarkiska relationer

Tahir (2008) framhåller att hierarkiska relationer i rollbaserad åtkomstkontroll kan orsaka konflikter, och risken för att detta inträffar kan förhöjas när hans föreslagna hierarkiska relationer mellan positioner, domäner och ändamål används (Tahir, 2008). En studie över hur sådana hierarkiska aspekter påverkar rollbehörigheternas integritet vid användandet av rollbaserad åtkomstkontroll skulle kunna reda ut sådana frågor. Compagnoni et al. (2008) beskriver hur rollbaserad åtkomst-kontroll kan förlängas ytterligare genom att införa nya tillvägagångssätt för att strukturera roller och rollhierarkier, exempelvis genom att definiera strukturer över vilka roller som samtidigt får användas av en användare. De beskriver också ett behov av vidare diskussioner kring hur användare som lämnar ett område där denne uppbär en viss behörighet för att sedan återvända till detta ska hanteras. Ett förhållningssätt är att kräva att användaren återigen aktiverar tidigare aktiverade roller, ett annat är att aktivering sker automatiskt när användaren åter stiger in i det geografiska avgränsningsområdet. Skapandet av en sådan händelsebaserad modell för att stödja fortsatt användande är en möjlig ingång till vidare forskning.

Övriga utvecklingsbehov

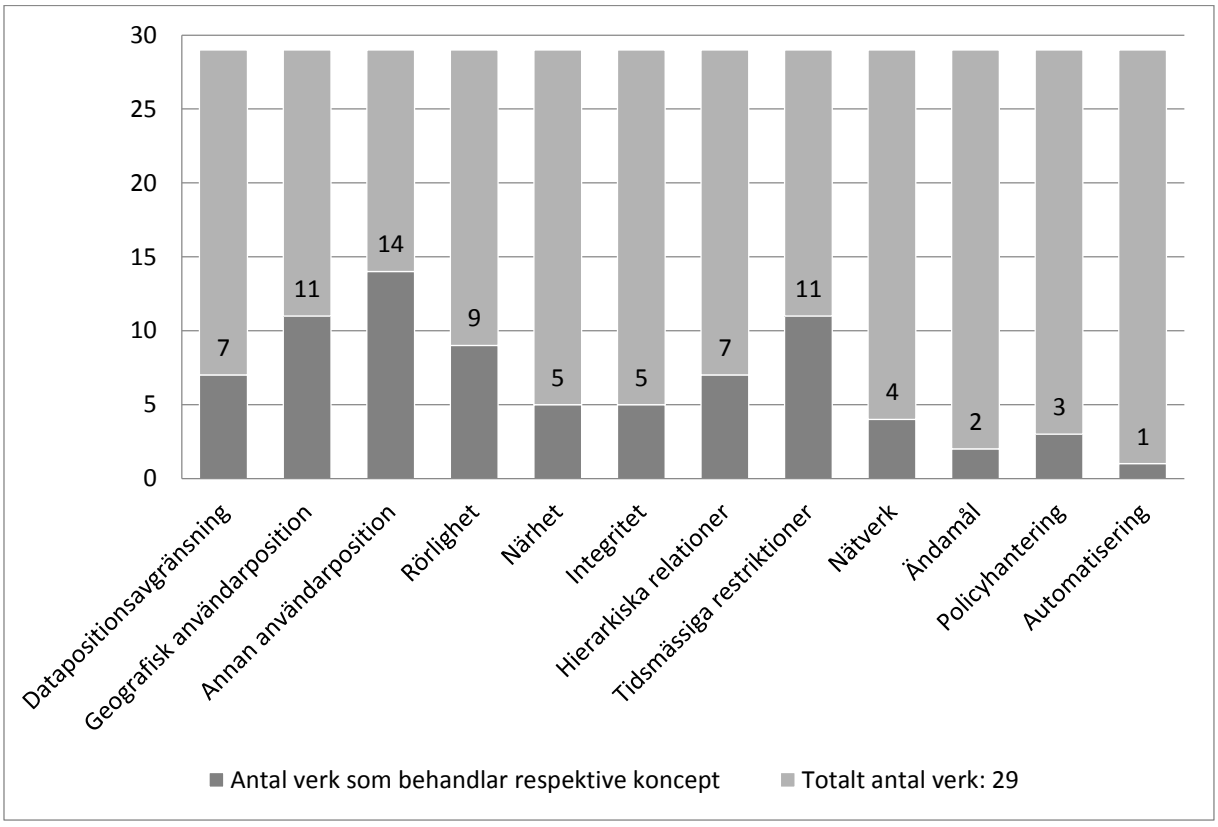
Det har också varit märkbart att litteraturen kring ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning vanligtvis behandlar läsrättigheter snarare än skrivrättigheter. Att implementera skrivrättigheter i ett sådant system skulle medföra ytterligare faktorer att ta hänsyn till. Ett exempel på detta är att reda ut hur samtidiga databastransaktioner av geografiska data i ett system med rollbaserad åtkomstkontroll med geografisk avgränsning kan behandlas. Att upprätthålla användarens integritet vid positionsbaserad åtkomstkontroll är inte någon kontroversiell målsättning inom ämnesområdet, även om frågan inte behandlats särskilt grundligt i det inkluderade materialet. Vidare studier kring hur användarpositionsdata lagras och hanteras i system med rollbaserad åtkomstkontroll med användarpositionsavgränsning skulle utgöra ett intressant uppslag för vidare studier.

6.3 Diskussion

Den systematiska litteraturgenomgången har visat att state-of-the-art kring ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning främst fokuserar på restriktioner baserat på användarpositionering eller datapositionsavgränsning. Det finns inom den vetenskapligt granskade

litteraturen idag en uppsjö olika modeller för att hantera sådana avgränsningar, och vissa verk har stuckit ut ur mängden som särskilt inflytelserika. GEO-RBAC, den åtkomstkontrollmodell som presenterats av Bertino et al. (2005), har refererats från en stor del av de övriga verk som inkluderats i studien. Det är också det enskilda verk som citerats flest gånger (243) enligt programvaran Publish or Perish. De idéer om att tillämpa såväl geografiska som logiska användarpositioner i åtkomstkontrollen som presenteras i GEO-RBAC har vunnit genomslag och återanvänts i en rad efterföljande verk. Bland andra inflytelserika åtkomstkontrollmodeller kan nämnas LRBAC (Ray, Kumar, & Yu, LRBAC: A Location-Aware Role-Based Access Control Model, 2006) och CA-RBAC (Kulkarni & Tripathi, 2008) som citerats 97 respektive 153 gånger enligt Publish or Perish.

Två parallella grenar för vad åtkomstkontrollen ska baseras på har urskilt sig i analysen. I den största andelen av inkluderade verk styrs åtkomstkontrollen med grund i någon form av rumslig användarposition, medan åtkomstkontrollen i andra inkluderade verk baseras på positionen hos de geografiska data i systemet som ska skyddas. Bland de i den systematiska litteraturgenomgången inkluderade verken är dock den positionsbaserade ansatsen betydligt mer behandlad. Vilken av de bägge ansatserna som är lämplig att tillämpa är naturligtvis beroende av karaktären hos det system där åtkomstkontrollen ska appliceras. En stor andel av litteraturgenomgångens inkluderade verk (11 av 29) involverar också tidsmässiga restriktioner tillsammans med rumsliga restriktioner, vilket avsevärt förhöjer den detaljnivå med vilken åtkomstkontrollen kan styras. Även användares rörlighet är ett vanligt koncept inom ämnesområdet rollbaserade åtkomstkontrollen med geografisk avgränsning, och 9 av 29 inkluderade verk behandlar företeelsen i någon utsträckning. En mindre andel av litteraturgenomgångens inkluderade verk (5 av 29) behandlar integritetsmässiga aspekter, vilket kan tyckas vara en låg siffra då geografiska data likt Ray et al. (2006) beskriver kan vara av privat eller för individer och organisationer känslig natur. Hur stor andel av i studien inkluderade verk som behandlar respektive koncept illustreras i efterföljande figur 30.



Figur 30: Andel verk som behandlar respektive koncept

Ämnesområdet rollbaserad åtkomstkontroll med geografisk avgränsning är ett intressant område som förtjänar fortsatt uppmärksamhet, och likt studien visar finns ett flertal aspekter inom ämnesområdet att arbeta vidare med.

6.4 Utvärdering

Det exakta recall-värde som den systematiska litteraturgenomgången uppmäter är naturligtvis inte möjligt att själv bedöma, även om målsättningen hela tiden har varit att nå ett högt sådant. Det är likt Webster och Watson (2002) beskriver mycket sannolikt att det existerar material som hade varit relevant för studien men som av misstag försummats. Då arbetets ambition har varit att ge en områdesöversikt på ämnet rollbaserad åtkomstkontroll med geografisk avgränsning hade dock en inkludering av enstaka sådana förbisedda verk troligtvis inte påverkat utgången. Arbetet har endast innefattat publicerat vetenskapligt material som genomgått peer review-granskning, vilket medför att det kan finnas relevanta verk som är producerade men ännu inte publicerade. Det kan ta flera år från tidpunkten då en artikel skrivs till det att den faktiskt publiceras i en journal.

Jag har aldrig tidigare genomfört en systematisk litteraturgenomgång i sådan utsträckning som i detta arbete, och det är fullt möjligt att en van utförare hade bidragit med ett än mer omfattande kunskapsbidrag. En för mig aningen oväntad svårighet som uppstått under genomförandet har varit att identifiera koncept i genomgånget material. Många vetenskapliga artiklar är inte särskilt lättlästa, och att identifiera och fördela de koncept som behandlas och beskrivs av författarna med från varandra vitt skilt språkbruk och abstraktionsnivå har krävt en större arbetsinsats och mer tid än vad jag väntat mig. Det är självklart också möjligt att vissa misstag har begåtts eller att missuppfattningar har skett i tolkningen av materialet. Genom att påvisa transparens i arbetet förhöjs dock dess tillförlitlighet, och eventuella misstag kan enklare upptäckas av läsaren. Då arbetet haft en explorativ ansats där ambitionen varit att utforska ett ämnesområde anser jag att det metodologiska valet att genomföra en systematisk litteraturgenomgång varit fullt lämpligt. Eftersom arbetet inkluderat ett i sammanhanget litet antal vetenskapliga verk är det svårt att på ett säkert vis dra några vetenskapliga kvantitativa slutsatser av det. Detta faktum till trots kan numeriska data kring behandlingen av ämnesområdet agera fingervisning för en läsare som söker introduceras till ämnet.

Då arbetet från början var avsett att behandla rollbaserad åtkomstkontroll med geografisk avgränsning inom den nationella vägdatabasen, NVDB, har det också under i det syftet genomförda intervjuer uppenbarats möjligheter till vidare arbete. Det finns svårigheter kring att få in dataleveranser till NVDB från en del av de parter som är avtalsmässigt bundna att leverera data. Grunden till detta har ansetts vara att ex. vissa kommuner inte behärskar ämnets komplexitet. Att närmare undersöka detta fenomen skulle kunna utgöra ett uppslag till vidare studier. Det har också framkommit att de relativa värden med vilka företeelser placeras ut på referenslänkar har en mycket precis upplösning, med en noggrannhet på millimeternivå. En utredning kring huruvida en sådan precision faktiskt är nödvändig, samt hur detta påverkar prestandan vid datahantering i NVDB skulle kunna utgöra ytterligare ett uppslag på fortsatt arbete.

Referenser

Aich, S., Mondal, S., Sural, S., & Majumdar, A. K. (2009). Role Based Access Control with Spatiotemporal Context for Mobile Applications. *Transactions on Computational Science IV* (pp. 177-199). Springer-Verlag.

Aich, S., Sural, S., & Majumdar, A. (2007). STARBAC: Spatiotemporal Role Based Access Control. *OTM'07 Proceedings of the 2007 OTM confederated international conference on On the move to meaningful internet systems: CoopIS, DOA, ODBASE, GADA, and IS - Volume Part II* (pp. 1567-1582). Vilamoura, Portugal: Springer-Verlag.

ANSI. (2004). *Role Based Access Control, 359-2004.* ANSI. New York: American National Standards Institute, Inc.

Atluri, V., & Chun, S. A. (2007, Januari). A geotemporal role-based authorisation system. *International Journal of Information and Computer Security, 1*(1/2), 143-168.

Belussi, A., Bertino, E., Catania, B., Daminani, M., & Nucita, A. (2004). An authorization model for geographical maps. *GIS '04 Proceedings of the 12th annual ACM international workshop on geographic information systems* (pp. 82-91). New York: ACM.

Bertino, E. (2003, September). RBAC models - concepts and trends. (E. H. Spafford, Ed.) *Computers and Security, 22*(6), 511-514.

Bertino, E., & Kirkpatrick, M. S. (2011). Location-Based Access Control Systems for Mobile Users - Concepts and Research Directions. *SPRINGL '11 Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS* (pp. 49-52). Chicago, USA: ACM.

Bertino, E., Catania, B., Damiani, M. L., & Perlasca, P. (2005). GEO-RBAC: A Spatially Aware RBAC. *SACMAT '05 Proceedings of the tenth ACM symposium on Access control models and technologies* (pp. 29-37). New York: ACM.

Bhatti, R., Damiani, M. L., Bettis, D. B., & Bertino, E. (2008, Mars). Policy Mapper: Administering Location-Based Access-Control Policies. *Internet Computing, IEEE, 12*(2), 38-45.

Björklund, M., & Paulsson, U. (2003). *Seminarieboken - att skriva, presentera och opponera* (1:a ed.). Lund: Studentlitteratur.

Booth, A., Papaioannou, D., & Sutton, A. (2012). *Systematic Approaches to a Successful Literature Review.* London: SAGE Publications Ltd.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007, April). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software, 80*(4), 571-583.

Buckland, M., & Gey, F. (1994, Januari). The Relationship between Recall and Precision. *Journal of the American Society for Information Science, 45*(1), 12-19.

Chen, H.-C., Wang, S.-J., Wen, J.-H., Huang, Y.-F., & Chen, C.-W. (2010, Augusti). A Generalized Temporal and Spatial Role-Based Access Control Model. *Journal of Networks, 5*(8), 912-920.

Compagnoni, A., Gunter, E. L., & Bidinger, P. (2008, Maj). Role-based access control for boxed ambients. *Theoretical Computer Science, 398*(1-3), 203-216.

Damiani, M. L., Bertino, E., & Silvestri, C. (2008, September). Spatial Domains for the Administration of Location-based Access Control Policies. *Journal of Network and Systems Management, 16*(3), 277-302.

DoD. (1985). *Trusted Computer System Evaluation Criteria, 5200.28-STD.* United States Government Department of Defense.

Ferraiolo, D. F., & Kuhn, R. D. (1992). Role-Based Access Controls. *15th National Computer Security Conference* (pp. 554-563). Baltimore: National Institute of Standards And Technology.

Ferraiolo, D. F., Kuhn, R. D., & Chandramouli, R. (2007). *Role-Based Access Control* (2nd ed.). Boston: Artech House.

Franqueira, V. N., & Wieringa, R. J. (2012, Juni). Role-Based Access Control in Retrospect. *Computer, 45*(6), 81-88. Retrieved Mars 30, 2015

Fransson, J. (2007). *Effektivare informationssökning på webben: En handbok i konsten att söka information.* Ronneby: Hexa Förlag.

Fu, S., & Xu, C.-Z. (2007, Juli). Coordinated access control with temporal and spatial constraints on mobile execution in coalition environments. *Future Generation Computer Systems, 23*(6), 804-815.

Google. (n.d.). *Google Scholar*. Retrieved Maj 5, 2015, from Toppublikationer - Teknik och datavetenskap: https://scholar.google.com/citations?view_op=top_venues&hl=sv&vq=eng

Gupta, A., Kirkpatrick, M. S., & Bertino, E. (2014, Mars). A Formal Proximity Model for RBAC Systems. *Computers & Security, 41*, 52-67.

Gupta, S., Mukherjee, T., & Venkatasubramanian, K. (2006). Proximity Based Access Control in Smart-Emergency Departments. *Proceedings of 4th IEEE Conference on Pervasive Computing Workshops* (pp. 512-516). Pisa: IEEE.

Harrie, L. (2012). *Geografisk informationsbehandling: Teori, metoder och tillämpningar* (5:e ed.). (L. Harrie, Ed.) Lund: Studentlitteratur.

Heywood, I., Cornelius, S., & Carver, S. (2011). *An Introduction to Geographical Information Systems* (4:e ed.). Harlow: Pearson.

Huisman, O., & de By, R. A. (2009). *Principles of Geographic Information Systems: An Introductory Textbook* (4:e ed., Vol. I). Enschede: International Institute for Geo-Information Science and Earth Observation.

Högskolan Dalarna. (2013, December 17). Forskningsetiska anvisningar för examens- och uppsatsarbeten vid Högskolan Dalarna. (Rektor, Ed.) Retrieved April 23, 2015, from http://www.du.se/Global/dokument/Styrdokument-ny/Forskning/3 Regel/Forskningsetiska anvisningar för examens- och uppsatsarbeten.pdf

Högskolan Dalarna. (2014, Maj 7). Akademisk hederlighet handlar om att inte fuska eller plagiera - Information om plagiat och upphovsrätt. Retrieved Maj 28, 2015, from http://www.du.se/PageFiles/116999/PlagiatSVENSK.pdf

Högskolan Dalarna. (2015, Maj 4). *Ämneskategorier Teknik & Tillämpad vetenskap*. Retrieved Maj 5, 2015, from Högskolan Dalarna: http://kq3er2xz6l.search.serialssolutions.com/?V=1.0&L=KQ3ER2XZ6L&S=SC&C=TE

Ibrahim, M. H., Hefny, H. A., & Hamza, N. (2014, Februari). Contextual View-based Access Control Model for Spatial Data on Web. *International Journal of Computer Applications, 87*(15), 38-42.

Kirkpatrick, M. S., & Bertino, E. (2010). Enforcing spatial constraints for mobile RBAC systems. *SACMAT '10 Proceedings of the 15th ACM symposium on Access control models and technologies* (pp. 99-108). Pittsburgh, USA: ACM.

Kirkpatrick, M. S., Damiani, M. L., & Bertino, E. (2011). Prox-RBAC: A Proximity-based Spatially Aware RBAC. *GIS '11 Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems* (pp. 339-348). New York: ACM.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering.* Keele University, Department of Computer Science. Keele, UK: EBSE. Retrieved April 30, 2015, from http://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

Kulkarni, D., & Tripathi, A. (2008). Context-aware role-based access control in pervasive computing systems. *SACMAT '08 Proceedings of the 13th ACM symposium on Access control models and technologies* (pp. 113-122). Estes Park, USA: ACM.

Kumar, M., & Newman, R. E. (2006). STRBAC - An Approach Towards Spatio-Temporal Role-Based Access Control. *Proceedings of the 3rd IASTED International Conference on Communication, Network and Information Security* (pp. 150-155). Cambridge: IASTED/ACTA Press.

Lehtinen, R., Russell, D., & Gangemi Sr., G. (2011). *Computer Security Basics* (2nd ed.). (T. Apandi, Ed.) O'Reilly Media.

Marelli, A. F. (2005, Augusti). The Performance Technologist's Toolbox: Literature Review. *Performance Improvement, 44*(7), 40-44.

Mutch, J., & Anderson, B. (2011). *Preventing Good People from Doing Bad Things: Implementing Least Privilege.* (J. Pepper, Ed.) New York: Apress.

NVDB. (n.d.). *Om NVDB*. Retrieved April 7, 2015, from NVDB: http://www.nvdb.se/sv/Om-NVDB/

Nyberg, R. (2000). *Skriv vetenskapliga uppsatser och avhandlingar med stöd av IT och Internet* (4:e ed.). Lund: Studentlitteratur.

Oates, B. J. (2006). *Researching Information Systems and Computing.* London: SAGE Publications Ltd.

O'Connor, A. C., & Loomis, R. J. (2010). *2010 Economic Analysis of Role-Based Access Control.* National Institute of Standards and Technology, RTI Project Number 0211876.

Rajpoot, M. S. (2013, Oktober). A Location-based Secure Access Control Mechanism for Geospatial Data. *International Journal of Computer Applications, 79*(11), 28-32.

Ray, I., & Toahchoodee, M. (2007). A Spatio-Temporal Role-Based Access Control Model. *Proceedings of the 21st annual IFIP WG 11.3 working conference on Data and applications security* (pp. 211-226). Redondo Beach, USA: Springer-Verlag.

Ray, I., Kumar, M., & Yu, L. (2006). LRBAC: A Location-Aware Role-Based Access Control Model. *Information Systems Security: Second International Conference, ICISS* (pp. 147-161). Kolkata, Indien: Springer Berlin Heidelberg.

Samuel, A., Ghafoor, A., & Bertino, E. (2008, Januari). Context-Aware Adaptation of Access-Control Policies. *Internet Computing, IEEE, 12*(1), 51-54.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996, Februari). Role-Based Access Control Models. *IEEE Computer, 29*(2), 38-47.

Shin, H., & Atluri, V. (2009). Spatiotemporal Access Control Enforcement under Uncertain Location Estimates. *Data and Applications Security XXIII: 23rd Annual IFIP WG 11.3 Working Conference* (pp. 159-174). Montreal, Kanada: Springer Berlin Heidelberg.

Staples, M., & Niazi, M. (2007, September). Experiences using systematic review guidelines. *Journal of Systems and Software, 80*(9), 1425-1437.

Tahir, M. N. (2007). C-RBAC: Contextual Role-Based Access Control Model. *Ubiquitous Computing and Communication Journal, 2*(3), 67-74.

Tahir, M. N. (2008, Augusti). Hierarchies in Contextual Role-Based Access Control Model (C-RBAC). *International Journal of Computer Science and Security (IJCSS), 2*(4), 28-42.

Thi, K. T., Dang, T. K., Kuonen, P., & Drissi, H. C. (2012). STRoBAC - Spatial Temporal Role Based Access Control. *Computational Collective Intelligence. Technologies and Applications: 4th International Conference, ICCCI 2012* (pp. 201-211). Ho Chi Minh City, Vietnam: Springer Berlin Heidelberg.

Tomur, E., & Erten, Y. (2006, September). Application of temporal and spatial role based access control in 802.11 wireless networks. *Computers & Security, 25*(6), 452-458.

Ulltveit-Moe, N., & Oleshchuk, V. (2012). Mobile Security with Location-Aware Role-Based Access Control. *Mobile Security with Location-Aware Role-Based Access Control: Third International ICST Conference MobiSec* (pp. 172-183). Aalborg, Denmark: Springer Berlin Heidelberg.

Unal, D., & Caglayan, M. U. (2013, Januari). A formal role-based access control model for security policies in multi-domain mobile networks. *Computer Networks, 57*(1), 330-350.

Webster, J., & Watson, R. T. (2002, Juni). Analyzing the past to prepare for the future: Writing. *MIS Quarterly, 26*(2), xiii-xxiii.

Wennström, H.-F. (2015). *Geografiskt informationssystem: NE.* Retrieved April 7, 2015, from Nationalencyklopedin: http://www.ne.se/uppslagsverk/encyklopedi/lång/geografiskt-informationssystem

Zhang, A.-j., Gao, J.-x., Ji, C., Sun, J.-y., & Bao, Y. (2014, September). Multi-granularity spatial-temporal access control model for web GIS. *Transactions of Nonferrous Metals Society of China, 24*(9), 2946-2953.

Bilagor

I efterföljande avsnitt finns de bilagor som är relevanta för arbetets transparens, men inte bedömts vara lämpliga att presenteras i uppsatsens huvudsakliga del.

Bilaga 1: Logg över sökningar och urval

Sökinställningar Summon:
Sortering efter relevans, endast peer-review, fr.o.m. 1990

Sökinställningar Google Scholar:
Sortering efter relevans, fr.o.m. 1990 (manuell peer-review-kontroll)

DATUM	SÖKTJÄNST	SÖKTERMER	URVAL		
			1	**2**	**3**
2015-05-07	Summon	(role-based) AND (access control) AND (spatial)	34	13	8
2015-05-08	Google Scholar	*role-based + access control + spatial*	75	32	18
2015-05-11	Summon	*(role-based) AND (access control) AND (model) AND (geo)*	9	-	-
2015-05-11	Summon	*(rbac) AND (geographical)*	1	-	-
2015-05-11	Summon	*(roles) AND (authorization) AND (gis)*	3	1	1
2015-05-11	Summon	*(role-based) AND (security) AND (location)*	8	3	1
2015-05-11	Google Scholar	*role-based + access control + model + geo*	6	2	1
2015-05-11	Google Scholar	*roles + authorization + gis*	-	-	-
		Totalt:	136	51	29

Notering: Efter att de inledande sökningarnas resultat genomgåtts mycket grundligt gav resterande sökningar endast en mycket liten mängd (eller inget) nytt material med relevans för arbetet.

Bilaga 2: Exkluderade verk med bristande relevans

Verk	Noteringar
Location constraints in digital rights management *Muhlbauer, Safavi-Naini, Sheppard, Surminen (2008)*	Handlar inte om rollbaserad åtkomstkontroll.
A new medium access control protocol based on perceived data reliability and spatial correlation in wireless sensor network *Zhang, Zhao, Liang, Liu (2012)*	Handlar inte om rollbaserad åtkomstkontroll.
Situation, Team and Role based Access Control *Kawagoe, Kasai (2011)*	Handlar inte om geografiska avgränsningar.
An Access Control Model for Geographic Data in an XML-based Framework *Purevjii, Amagasa, Imai, Kanamori (2004)*	Handlar inte om rollbaserad åtkomstkontroll.
Access Control in Collaborative Systems *Tolone, Ahn, Pai (2005)*	Beskriver bara rollbaserad åtkomstkontroll mycket grundligt.
A location-based policy specification languange for mobile devices *Finnis, Saigal, Iamnitchi, Ligatti (2010)*	Handlar inte om rollbaserad åtkomstkontroll.
Resolving authorization conflicts by ontology views for controlled access to a digital library *Dasgupta, Pal, Mazumdar (2015)*	Handlar inte om rollbaserad åtkomstkontroll.
Fuzzy Role-Based Access Control Martinez-Garcia, Navarro-Arribas, Borelli (2011)	Handlar inte om geografiska avgränsningar.
A formal privacy system and its application to location based services *Gunter, May, Stubblebine (2005)*	Handlar inte om rollbaserad åtkomstkontroll.
Purpose Based Access Control of Complex Data for Privacy Protection *Byun, Bertino, Li (2005)*	Handlar inte om geografiska avgränsningar.
Data security in location-aware applications an approach based on RBAC *Damiani, Bertino, Perlasca (2007)*	Duplicering. Beskriver GEO-RBAC.
A Spatio-temporal Access Control Model Supportin Delegation for Pervasive Computing Applications *Ray, Toahchoodee (2008)*	Duplicering. Samma artikel redan inkluderad under annat namn.
On the Formal Analysis of a Spatio-temporal Role-Based Access Control Model *Toahchoodee, Ray (2008)*	Behandlar till största del en redan inkluderad modell. Resterande information tillför inget nytt relevant.
Using Alloy to Analyze a Spatio-Temporal Access Control Model Supporting Delegation *Toahchoodee, Ray (2009)*	Behandlar till största del en redan inkluderad modell. Resterande information behandlar mest Alloy.
Ensuring Spatio-Temporal Access Control for Real-World Applications *Toahchoodee, Ray, Anastasakis, Georg, Bordbar (2009)*	Behandlar till största del en redan inkluderad modell. Resterande information tillför inget nytt relevant.

Bilaga 3: Verk som inte varit åtkomliga över Internet

Titel	År	Författare
Enforcing role based access control model with multimedia signatures	2009	Bouna, Chbeir, Marrara
Enforcing role based access control model with multimedia signatures	2014	Guerroumi, Pathan
Dynamic deployment of context-aware access control policies for constrained security devices	2011	Preda, Cuppens, Cuppens-Boulahia
Method for automatic escalation of access rights to the electronic health record	2006	Hansen, Fensli
A delegation model for extended RBAC	2010	Ben Ghorbel, Cuppens, Cuppens-Boulahia
Security Access Control Based on Multi-user Spatial Database [J]	2004	Yong, Mao
Context-role based access control for context-aware application	2006	Park, Han, Chung
LoT-RBAC: a location and time-based RBAC model	2005	Chandran, Joshi
Spatial context in role-based access control	2006	Zhang, He, Shi
Ex-RBAC: An extended role based access control model for location-aware mobile collaboration system	2007	Cui, Chen, Gu
A formal model for access control with supporting spatial context	2007	Zhang, He, Shi
Requirements for a location-based access control model	2008	Decker
A spatio-temporal role-based access control model for wireless LAN security policy management	2010	Bera, Ghosh, Dasgupta
Definition of the Constraint with Spatial Characters	2009	S Ju, Y Gu, Z Tang, W Chen
Content-oriented Multi-level Security Authorization of Remote Sensing Images	2013	Ye, Chunxia, Xiaojun

Bilaga 4: Kvalitetsutvärdering

Kriterium	Beskrivning	Poängsättning
Antal citeringar	Det antal gånger som verket enligt programvaran *Publish or Perish* citerats i andra verk.	Fler än 0: 0,5 poäng Fler än 10: 1 poäng Fler än 50: 2 poäng
Problemformulering	Verket utgår från en väldefinierad problemformulering eller frågeställning.	Ja: 1 poäng Delvis: 0,5 poäng Nej: 0 poäng
Språkbruk	Det språkbruk som används i verket ger ett seriöst intryck.	Ja: 1 poäng Delvis: 0,5 poäng Nej: 0 poäng

Verk	Antal citeringar	Problemformulering	Språkbruk	Poäng
7	1 p (12 citeringar)	0,5 p (Delvis)	1 p (Ja)	2,5 p
11	0,5 p (8 citeringar)	0,5 (Delvis)	1 p (Ja)	2 p
8	1 p (16 citeringar)	1 p (Ja)	1 p (Ja)	3 p
20	1 p (14 citeringar)	0,5 (Delvis)	1 p (Ja)	2, 5 p
3	1 p (12 citeringar)	0,5 p (Delvis)	1 p (Ja)	2,5 p
5	0,5 p (1 citering)	1 p (Ja)	1 p (Ja)	2,5 p
1	0,5 p (3 citeringar)	1 p (Ja)	1 p (Ja)	2,5 p
10	0 p (0 citeringar)	0,5 p (Delvis)	1 p (Ja)	1,5 p
14	2 p (243 citeringar)	1 p (Ja)	1 p (Ja)	4 p
17	2 p (97 citeringar)	1 p (Ja)	1 p (Ja)	4 p
21	1 p (21 citeringar)	1 p (Ja)	1 p (Ja)	3 p
28	1 p (29 citeringar)	0,5 p (Delvis)	1 p (Ja)	2,5 p
4	1 p (41 citeringar)	1 p (Ja)	1 p (Ja)	3 p
6	2 p (113 citeringar)	1 p (Ja)	1 p (Ja)	4 p
12	0,5 p (9 citeringar)	0,5 p (Delvis)	1 p (Ja)	2 p
27	2 p (50 citeringar)	1 p (Ja)	1 p (Ja)	4 p
9	2 p (153 citeringar)	0,5 p (Delvis)	1 p (Ja)	3,5 p
15	0,5 p (4 citeringar)	1 p (Ja)	1 p (Ja)	2,5 p
25	0,5 p (8 citeringar)	1 p (Ja)	1 p (Ja)	2,5 p
23	1 p (31 citeringar)	0,5 p (Delvis)	1 p (Ja)	2, 5 p
26	1 p (12 citeringar)	1 p (Ja)	1 p (Ja)	3 p
13	1 p (34 citeringar)	1 p (Ja)	1 p (Ja)	3 p
16	1 p (11 citeringar)	1 p (Ja)	1 p (Ja)	3 p
22	1 p (12 citeringar)	1 p (Ja)	1 p (Ja)	3 p
18	0,5 p (5 citeringar)	0,5 p (Delvis)	1 p (Ja)	2 p
29	0,5 p (6 citeringar)	0,5 p (Delvis)	1 p (Ja)	2 p
19	0 p (0 citeringar)	0,5 p (Delvis)	1 p (Ja)	1,5 p
2	0,5 p (6 citeringar)	0,5 p (Delvis)	1 p (Ja)	2 p
24	1 p (14 citeringar)	1 p (Ja)	1 p (Ja)	3 p

Bilaga 5: Dataextraheringsformulär

Dataextraheringsformulär

Datum för extrahering:

YYYY-MM-DD

Titel	
Källa	**Årtal**
Författare	**Typ**
Nyckelord	**Antal citeringar**

Sammanfattning

…

Slutsatser

…

Vidare studieförslag

…

Ytterligare noteringar

…