Tillgänglighet, pålitlighet och säkerhet inom datormolnet

Är datormolnet bristfälligt?

Kandidatavhandling

Våren 2010

Datavetenskap vid Åbo Akademi

Skribent: Nico Hållfast

Handledare: Ivan Porres

Referat

Datormolnet anses som en ny möjlighet för att utnyttja datorer, eftersom datormolnet erbjuder möjligheten att använda datorer som en tjänst. Denna möjlighet har medfört att flera användare söker sig till att använda datormolnet på grund av dess flexibilitet jämfört med traditionell datoranvändning. Det har dock uppstått debatt över huruvida datormolnet är pålitligt, tillgängligt och säkert. I denna avhandling kommer datormolnets eventuella bristfälligheter att evalueras. Avhandlingen kommer också att ge en översikt över vad datormolnet är, hurdana tjänster det erbjuder och ge exempel över kända datormoln. Evalueringen av pålitligheten, tillgängligheten och säkerheten av datormolnet kommer att göras genom att ta upp väsentliga problem för var och en av egenskaperna. Sedan kommer lösningar för problemen att presenteras, och avslutningsvis kommer det att värderas huruvida det finns olösta problem med datormolnet och om datormolnet är bristfälligt.

Nyckelord

Datormolnet, tillgänglighet, pålitlighet, säkerhet

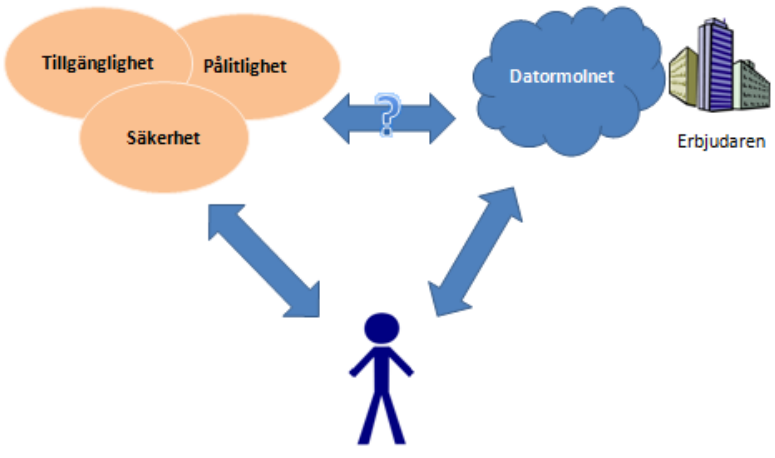
Innehållsförtäckning

1. Inledning 1
2. Datormolnet 2
2.1. Definition av datormolnet 2
2.2. Kärnegenskaper av datormolnet 3
2.3. Exempel på utility computing 4
3. Problem i datormolnet 5
3.1. Tillgänglighet 5
3.1.1. Inlåsning av data 6
3.1.2. DDOS-attacker mot datormolnet 7
3.1.3. Allmänna problem med tillgänglighet 7
3.2. Pålitlighet 7
3.2.1. Övergivning av kontroll av data 8
3.2.2. Oförutsebar prestanda 9
3.2.3. Pålitlighet av datormolnerbjudaren 9
3.3. Säkerhet 10
3.3.1. Problem med kryptering och skyddandet av data 10
3.3.2. Problem med isolering 11
4. Lösningar till problemen 12
4.1. Tillgänglighet 12
4.1.1. Lösningar för inlåsning av data 12
4.1.2. Lösningar för DDOS-attacker 13
4.1.3. Lösningar för allmänna problem med tillgänglighet 14
4.2. Pålitlighet 14
4.2.1. Lösningar till övergivning av kontroll av data 14
4.2.2. Lösningar för oförutsebar prestanda 16
4.2.3. Lösningar för pålitligheten av datormolnerbjudaren 16
4.3. Säkerhet 17
4.3.1. Lösningar för kryptering och skyddandet av data 17
4.3.2. Lösningar för problemen med isolering 18
5. Sammanfattning och diskussion – är datormolnet bristfälligt? 19
Litteraturlista 21

1. Inledning

Datormolnet (för en definition av datormolnet se rubrik 2.1. ”Definition av datormolnet”) har ansetts, och anses ännu idag, som en stor möjlighet för flera olika användare. Med hjälp av datormolnet kan man använda datorer som en tjänst. Man kan med andra ord jämföra datormolnet med elektricitet, vatten och andra tjänster där man betalar för tjänsterna efter användning (Armburst, o.a., 2009). Detta har lett till att flera olika användare, speciellt företag, använder datormolnet för att minimera kostnaderna för deras IT. Vid användningen av datormolnet behöver ett företag inte investera i till exempel lokala servrar, utan företaget kan istället använda sig av servrarna i datormolnet. Genom detta kan investeringskostnaderna för IT minimeras (Jensen;Schwenk;Gruschka;& Iacono, 2009).

Syftet med denna avhandling är att undersöka huruvida det finns bristfälligheter i datormolnet, genom att ta upp väsentliga problem i datormolnet. Det är viktigt att hitta lösningar till problemen, eftersom man då kan öka nyttjandet av datormolnet (Armburst, o.a., 2009). Problemen är delade i tre olika områden: *tillgänglighet*, *pålitlighet* och *säkerhet*. Denna uppdelning är gjord eftersom dessa tre olika problemområden anses vara önskvärda egenskaper för tjänster som används i realtid (Kuhlin & Thielmann, 2005). Till exempel anses problemen med säkerhet vara en av de väsentligaste inom dagens datormoln. I en studie gjord av Launchpad Europe svarade 109 IT-Experter på frågor angående datormolnet. I studien framkom det att säkerhet är huvudskälet till att datormolnet inte används i många företag (Launchpad Europe, 2009).



Figur 1. En grafisk representation av problemställningen i avhandlingen

Avhandlingen kommer att presentera de väsentligaste problemen inom alla de tre delområdena, det vill säga tillgängligheten, pålitligheten och säkerheten. I Figur 1 presenteras problemställningen av avhandlingen. Efter att alla problem har presenterats, kommer lösningar för dessa problem att tas upp. I sammanfattningen evalueras sedan huruvida datormolnet är bristfälligt, det vill säga hur många av de väsentliga problemen är lösta och hur många är olösta.

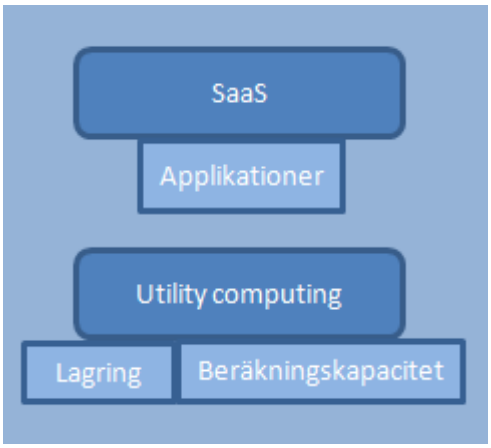
2. Datormolnet

I detta kapitel presenteras definition för vad ett datormoln är och vad det kan användas till, eftersom konceptet med datormoln kan anses vara oklart och svårt att klart definiera (Armburst, o.a., 2009). Tre exempel på populära datormoln: Amazon EC2, Google App Engine och Force.com kommer även att diskuteras.

I uppsatsen motsvarar ordet *datormolnet* det engelska ordet *cloud computing*. Ordet *molnet* kan också användas som en översättning till *cloud computing* (Söderling, 2010), men jag anser personligen att ordet datormolnet ger en mera klar bild över vad termen betyder och vad det används till.

2.1. Definition av datormolnet

Till datormolnet tillhör mjukvara som körs på flera enheter samtidigt, och som erbjuds till en kund över ett nätverk – oftast Internet. Till datormolnet tillhör även den hårdvara och systemmjukvara som erbjuder dessa mjukvarutjänster (Armburst, o.a., 2009). Tjänsterna kan därför klassas att tillhöra två olika lager (se Tabell 1.): *software as a service* eller SaaS och *utility computing*. Det bör noteras att det finns andra uppdelningar för tjänsterna, till exempel kan *utility computing* delas upp i *infrastructure as a service* eller IaaS och *platform as a service* eller PaaS (Jensen;Schwenk;Gruschka;& Iacono, 2009). Problemet med denna uppdelning är dock den att det är svårt att klassa hurdana tjänster tillhör till IaaS och hurdana tillhör PaaS. Därför är det mera klart att använda uttrycket utility computing som ett samlingsbegrepp för både IaaS och PaaS (Armburst, o.a., 2009).



Tabell 1. Lagren i datormolnet. Till SaaS tillhör applikationer som erbjuds åt användarna och till utility computing tillhör hårdvaran som kör själva applikationerna.

De tidigare nämnda tjänsterna kan befinna sig i tre olika typer av datormoln: *privata*, *publika* eller *hybrida*. Det privata datormolnet är ett moln som är begränsat till endast vissa användare, till exempel endast till de anställda av ett visst företag. Det publika datormolnet är motsatsen till det privata eftersom det erbjuder tjänster till alla användare, utan begränsningar. Ett hybriddatormoln är en kombination av dessa två, kombinationen erbjuder således tjänster från det privata och det publika datormolnet samtidigt (Söderling, 2010). Det bör noteras att i allmänhet används ordet datormolnet för att endast omfatta det publika datormolnet, även fast det kan delas upp i tre olika typer (Armburst, o.a., 2009).

2.2. Kärnegenskaper av datormolnet

Grundtanken bakom datormolnet är att en datormolnanvändare kan snabbt och enkelt börja använda en tjänst, till exempel använda beräkningskapacitet för att köra ett program, och lika snabbt och enkelt anlita mera resurser för att köra programmet snabbare. Användaren kan också fria resurserna lika effektivt, detta koncept kallas skalbarhet. Skalbarheten möjliggör att en datormolnanvändare inte behöver oroa sig för att på förhand planera hur mycket resurser man reserverar för att utföra arbetet (Armburst, o.a., 2009).

Skalbarheten har introducerat ett annat koncept för datormolnet, att användaren endast betalar för de resurser som är i användning. Det resulterar i att användaren inte heller måste planera ekonomin på förhand, utan kan planera sina kostnader i realtid i samband med reservationen av nya resurser. Denna kostnadseffektiva modell leder i sin tur till det, att användarna inte reserverar

onödiga eller oanvända resurser, utan de frigörs tillbaka till datormolnet för annan användning (Buyya;Yeo;Venugopal;Broberg;& Brandic, 2008).

Från företagens synvinkel är användningen av datormolnet ett kostnadseffektivt val. Vanligtvis investerar och köper företagen hård- och mjukvara för privat användning, men eftersom företagen oftast inte utnyttjar hela den investerade hårdvaran kommer nyttan av användningen av den kostnadseffektiva modellen i datormolnet att speciellt synas vid tidpunkter där servrarna inte används till hundra procent (Grossman, 2009) (Armburst, o.a., 2009).

Virtualisering och virtuella maskiner är en viktig teknologi bakom datormolnet och hur det fungerar. Genom virtualisering kan en erbjudare av datormolnet erbjuda sina användare en konstgjord omgivning med beräkningskapacitet, lagring och nätverk utan att behöva ge användarna direkt tillgång till den konkreta hårdvaruomgivningen. Virtualiseringen tillsammans med skalbarheten gör att datormolnet är flexibelt och kan erbjuda effektiva tjänster (Buyya;Yeo;Venugopal;Broberg;& Brandic, 2008).

Från en användares synvinkel kan andra viktiga egenskaper av datormolnet identifieras, till exempel fungerar datormolnet i stort sett på alla plattformar och operativsystem eftersom man kommer åt användargränssnittet via webbläsaren (för SaaS) eller via olika webbtjänster (för utility computing) (Jensen;Schwenk;Gruschka;& Iacono, 2009).

2.3. Exempel på utility computing

I dagens läge erbjuds olika slags utility computing plattformar för användare; plattformarna kan variera allt från att erbjuda en låg nivå av abstraktion, så som Amazon EC2, till att erbjuda en hög nivå av abstraktion, som till exempel Google App Engine eller Force.com (Armburst, o.a., 2009). De olika nivåerna av abstraktion ger användarna möjlighet att välja hurdana program de kan köra på datormolnet.

Med en låg abstraktionsnivån kan användarna i stort sett köra alla typer av program på datormolnet (Amazon Web Services LLC, 2010). Datormolnen som erbjuder en hög nivå av abstraktion begränsar hurdana program

som kan köras på datormolnet, till exempel kan användaren av Force.com endast köra program som använder sig av Salesforce.coms egna databaser (Salesforce.com, inc., 2010). Medan en användare av Google App Engine endast kan köra program på App Enginen som är gjorda med en viss applikationsstruktur, såsom Googles App Engine Framework (Google, 2010). Den höga abstraktionsnivån medför dock, att den automatiska skalbarheten fungerar i stort sett automatiskt och behöver inte därför bestämmas på förhand av programmeraren (Armburst, o.a., 2009).

3. Problem i datormolnet

Denna rubrik kommer att ta upp och behandla relevanta problem för datormoln. Rubriken kommer huvudsakligen att behandla utility computing och dess problem och bristfälligheter. Rubriken är indelat i tre underrubriker: tillgänglighet, pålitlighet och säkerhet. För vissa av problemen kommer exempelfall att tas upp.

3.1. Tillgänglighet

Rubriken kommer att behandla problemet med tillgänglighet. Fokuseringen kommer att ligga på både problem med tillgängligheten av sparade data inne i datormolnet och på problem med tillgängligheten av själva datormolnet. Rubriken 3.1.1 ”Inlåsning av data” kommer att behandla ett särskilt problem som uppstår när data inte är tillgängligt för användaren. Den andra rubriken, 3.1.2. ”DDOS-attacker mot datormolnet” kommer att ta upp problemet med planerade attacker mot datormoln, attacker som påverkar tillgängligheten av datormolnet. I den tredje rubriken, 3.1.2. ”Allmänna problem med tillgänglighet” kommer allmänna problem med tillgänglighet i datormolnet att presenteras.

Allmänt kan det konstateras att problemen med tillgänglighet påverkar både användaren av datormolnet och erbjudaren av datormolnet. För användaren kan problemen med tillgänglighet orsaka att användaren måste byta datormolnerbjudare. Tillgänglighetsproblem kan orsaka för en datormolnerbjudare att den får ett dåligt rykte, vilket kan leda till att erbjudaren tappar möjligheten att få nya kunder och vidare kan det leda till att erbjudaren tvingas till att stänga sin tjänst (ENISA, 2009).

3.1.1. Inlåsning av data

Inlåsning av data är ett problem som framkommer när en kund vill få ut lagrade data från datormolnet, men kan av någon orsak inte få ut dem. Problemet är speciellt viktigt när en användare av ett datormoln vill byta från en datormolnerbjudare till en annan, till exempel på grund av ekonomiska förutsättningar eller ouppfyllda krav av den nuvarande datormolnerbjudaren (ENISA, 2009). Orsakerna för inlåsning av data kan variera från opassande *Application Programming Interfacer* eller API:er till att datormolnet där data är sparad helt enkelt stänger ner sin tjänst på grund av en konkurs (Armburst, o.a., 2009). Förutsättningarna för att inlåsning av data kan hända beror mycket på datormolnerbjudaren, men det beror även på i vilket lager i datormolnet data är sparad i (ENISA, 2009).

Inlåsning av data i SaaS orsakas oftast av API:er som datormolnerbjudaren har, vilka kunden använder sig av för att exportera data från molnet. Problemet uppstår när datormolnerbjudaren har en opassande API, som gör exporteringen av data blir problematisk eller helt omöjlig. Till exempel kan API:er orsaka att data inte kan tas ut från datormolnet, eller att data som kommer ut från datormolnet är i ett opassande format. Likadant som för SaaS, orsakas inlåsning av data i utility computing av opassande API:er (ENISA, 2009).

Från kundens synvinkel är inlåsning av data problematiskt, men sett från synvinkeln av datormolnerbjudaren kan inlåsning av data verka som ett lockande alternativ för att upprätthålla sin kundbas. Genom att begränsa – eller till och med helt ta bort – möjligheten för att få ut data från datormolnet, kan en datormolnerbjudare försäkra sig om att kunderna inte flyttar till någon annan datormolnerbjudare (ENISA, 2009).

Ett exempel av inlåsning av data, där en erbjudare av ett datormoln stängde sin tjänst, hände den åttonde augusti 2008 när The Linkup stängde sin tjänst (Krigsman, 2008). The Linkup, som erbjöd datalagring inne i ett datormoln, var tvungen att stänga tjänsten när 45 procent av data lagrat av kunderna förlorades på grund av ett misstag (Armburst, o.a., 2009).

3.1.2. DDOS-attacker mot datormolnet

En *distributed denial of service-attack* eller DDOS-attack, är ett problem som påverkar tillgängligheten av ett datormoln. I en DDOS-attack mot ett datormoln utsätts datormolnet för en så kallad *flooding*-attack. Attackens syfte är att hindra normala användare från att använda datormolnet. DDOS-attackerna utförs med hjälp av flera datorer som skickar falska eller onödiga förfrågningar till datormolnet (Stein & John, 2003), och försöker på så sett få hela datormolnet eller delar av datormolnet att kollapsa.

Arkitekturen av datormolnet ändrar avsevärt på påverkningarna som en DDOS-attack kan ha, jämfört med en DDOS-attack mot en traditionell server. På grund av den stora tillgången av resurser inom ett datormoln kan datormolnet försöka hindra attacken genom att allokera nya resurser till att svara automatiskt på frågorna som attackeraren skickar. Allokeringen av de nya resurserna kan dock ställa till med nya problem (Jensen;Schwenk;Gruschka;& Iacono, 2009). Dessa problem kommer att tas upp och behandlas under rubriken 4.1.2. ”Lösningar till DDOS-attacker”.

3.1.3. Allmänna problem med tillgänglighet

Till allmänna problem med tillgänglighet kan klassas sådana problem som påverkar hårdvaran av datormolnet, och hur den fungerar. Till sådana problem tillhör bland annat problem i strömförsörjningen, kylningen och själva hårdvaran (Magnusson, 2010).

De allmänna problemen kan leda till att hela datormolnet slutar fungera, till exempel på grund av störningar i strömförsörjningen. I ett fall orsakade en storm i Virginia i USA, att ena av Amazons viktigaste datacenter låg nere i sex timmar under den nionde december 2009 (Brooks, Amazon outage caused by power failure during Virginia storm, 2009). I ett annat exempelfall orsakade en blixt att användarna inte kunde kontakta Amazons EC2s webbserver under 40 minuter (Brooks, Users undeterred by Amazon EC2 lightning snafu, 2009).

3.2. Pålitlighet

Ett stort problem som datormoln möter är huruvida användarna av datormolnen kan lita på erbjudarna och deras datormoln (Urquhart, 2009). Till exempel företag

kan använda sig av datormolnet för att hantera sensitiv data, därför måste kraven på pålitlighet uppfyllas före företagen kan tänka sig använda datormolnet (Armburst, o.a., 2009).

Under denna rubrik kommer de största problemen som relaterar till pålitlighet att presenteras. Huvudsakligen kommer problemen att behandla hur användaren kan lita på erbjudaren av datormolnet.

3.2.1. Övergivning av kontroll av data

När en användare skickar upp sina data till datormolnet, överger användaren delvis kontrollen över datan. Denna flytt av kontroll kan leda till det faktum att användaren inte säkert kan veta var data är sparat inne i datormolnet och, framför allt, vem som har tillgång till datan (ENISA, 2009).

För företagen, som använder sig av datormolnet, kan problem med datakontroll uppstå när företaget vill försäkra sig om att data sparas endast i servrar inom ett visst land eller område. Sådana krav kan uppstå för företag som inte vill ta risken för att data sparas i länder där naturkatastrofer kan hända (Chandramouli & Mell, 2010). Kravet kan även uppstå för företag som önskar undgå risken för att data kan läsas i ett annat land av landets juridiska organisationer, till exempel kan data av en europeisk kund läsas i USA på grund av den amerikanska *PATRIOT Acten* (Armburst, o.a., 2009). Kraven på att data ska vara sparad inom ett visst område eller land, kan vara svåra att uppfylla på grund av datormolnets arkitektur och hur datormolnerbjudaren har tagit tillsyn till dessa krav (Chandramouli & Mell, 2010).

Företagen som har känslig företagsdata, såsom kunddata, sparade inne i molnet kan ställa specifika krav på pålitligheten av datormolnet och datormolnets erbjudare. Sådana krav är till exempel det, att ett företag kan kräva att data sparat inne i datormolnet revideras av en utomstående aktör. Revideringen försäkrar företaget om att data som är sparat inne i molnet inte ändras, tas bort eller läses av datormolnerbjudaren, eller till och med av andra användare av datormolnet (Armburst, o.a., 2009). Största problemet för revideringen är hur den i praktiken kan implementeras i datormolnet och dess arkitektur.

Normalt sett om en användare sparar data lokalt, i en lokal server, kan användaren ta säkerhetskopior på dessa data. För företag, kan data säkerhetskopieras från företagets servrar med jämna mellanrum (Chandramouli & Mell, 2010). Men i ett fall där företaget använder sig av datormolnet för att spara data, kan övergivningen av kontrollen av data resultera i att företagen inte kan försäkra sig om att data kan säkerhetskopieras (Chandramouli & Mell, 2010).

3.2.2. Oförutsebar prestanda

Oförutsebar prestanda är ett problem med pålitligheten, eftersom en användare av datormolnet vill försäkra sig om att man får den nivå av prestanda som man kräver, och inte måste oroa sig över att nivån av prestanda varierar under användningen. Eftersom datormolnet använder virtualisering för att dela upp hårdvaran till flera olika användare, genom att dela hårdvaran till flera virtuella maskiner, kommer hårdvaran att utsättas för förfrågningar av flera olika användare samtidigt (Buyya;Yeo;Venugopal;Broberg;& Brandic, 2008).

När flera virtuella maskiner använder sig av samma hårdvara, speciellt I/O-enheter, kan de virtuella maskinerna utsättas för stora variationer i till exempel skrivtiden till en hårdskiva. I utförda mätningar har variationer på 16% hittats i skrivtiderna till hårdskivor. I likadana mätningar har en variation på under 4% i lästiderna till hårdskivorna uppmätts (Armburst, o.a., 2009). Dessa variationer orsakar att användarna av datormolnet upplever prestandan som oförutsebar och opålitlig (Armburst, o.a., 2009).

3.2.3. Pålitlighet av datormolnerbjudaren

När en användare använder sig av ett datormoln, flyttar datormolnets användare delvis över ansvaret och riskerna till datormolnerbjudaren. I denna överflyttning av ansvar kan legala problem uppstå (Armburst, o.a., 2009). På grund av detta uppstår det krav av användaren på datormolnerbjudaren och dess pålitlighet (ENISA, 2009). Kraven på pålitligheten hos datormolnerbjudaren kan bestå av allt från krav på att datormolnerbjudaren inte använder sig av utlokalisering, till krav på att datormolnerbjudaren använder sig av professionell arbetskraft (ENISA, 2009).

När en datormolnerbjudare anlitas av ett företag, för att sköta om till exempel datalagring, anlitar företaget datormolnerbjudaren direkt. Men i ett fall

där datormolnerbjudaren använder sig av utlokaliserade datalager, har inte företaget i fråga någon direkt kontroll över de utlokaliserade datalagren. Kraven mellan företaget och datormolnerbjudaren kan skilja sig avsevärt från kraven mellan datormolnerbjudaren och de utlokaliserade datalagren (ENISA, 2009). De outsourcade datalagren behöver inte nödvändigtvis följa likadan lagstiftning som datormolnerbjudaren (ENISA, 2009).

För företag, kan problem i pålitligheten av datormolnerbjudaren leda till allvarliga problem. Bland annat kan pålitlighetsproblemen orsaka att företagen har svårt att uppnå någon nytta med att använda datormolnet. I värsta fall kan företagets strategi skadas, vilket kan leda till att företaget inte alls kan uppfylla sina affärsmål (ENISA, 2009).

3.3. Säkerhet

Detta kapitel kommer att presentera problem med säkerhet inom datormolnet. Problemen kommer att behandla kryptering och skyddning av data, problem med de allmänna säkerhetsstandarderna som används i datormolnet och problem med isolering inne i datormolnet.

3.3.1. Problem med kryptering och skyddandet av data

I fall där användarna av datormolnet vill lagra viktig data inne i datormolnet, till exempel när ett företag använder sig av datormolnet för att lagra kunddata, uppstår det krav på att sekretessen av dessa data kan uppnås. I praktiken betyder detta att två typer av data måste kunna skyddas: både data som är lagrat och data som flyttas (Chandramouli & Mell, 2010). Problem som presenteras i denna rubrik är nära relaterade till problemen som presenterades i kapitlet 3.2.1. ”Övergivning av kontroll av data”, eftersom pålitligheten av datormolnerbjudaren kan förbättras om erbjudaren kan försäkra användarna att data är korrekt skyddat i molnet.

Arkitekturen av datormolnet bygger på att data flyttas frekvent både mellan användaren och datormolnet och även inuti datormolnet. Det vill säga att i datormolnet flyttas data oftare än jämfört med traditionella arkitekturer. När data flyttas ofta, växer risken med att data kan läsas av en otillåten part. Till exempel kan en otillåten part läsa och modifiera data i flytt med hjälp av en så kallad ”man i mitten”-attack (ENISA, 2009).

För att skydda data som är lagrat i molnet, behöver datormolnerbjudaren använda sig av kryptering för att skydda data. Problemet som uppstår med krypteringen har att göra med datormolnets arkitektur, och problemet med att ansvaret för säkerheten av data flyttas delvis från användaren till erbjudaren (Chandramouli & Mell, 2010). På grund av detta uppstår det problem med hanteringen av krypteringsnycklarna – vem ska ha tillgång till krypteringsnycklarna (Cloud Security Alliance, 2009)?

3.3.2. Problem med isolering

Med isolering i datormolnet förstås det, att vissa resurser tilldelade till en användare inte kan användas av en annan användare samtidigt. Inom datormolnet uppfattas problemen som kan uppstå med isolering viktiga, eftersom dålig isolering kan leda till att bland annat sensitiv data lagrad i datormolnet blir tillgänglig för otillåtna användare (ENISA, 2009). Isolering är också viktigt på grund av arkitekturen av datormolnet; resurserna ska tilldelas till flera användare samtidigt, och det måste garanteras att dessa resurser tilldelas korrekt till användarna (ENISA, 2009).

Eftersom resurserna i datormolnet delas mellan användarna med hjälp av virtualisering och virtuella maskiner, uppstår bristfällig isolering mellan de virtuella maskinerna som körs inne i datormolnet (Cloud Security Alliance, 2009). I ett hypotetiskt problemfall kan en virtuell maskin komma åt andra virtuella maskiner, och läsa data som de andra virtuella maskinerna behandlar. En sådan virtuell maskin kallas för en *rogue virtual machine*, det vill säga en skadlig virtuell maskin (Chandramouli & Mell, 2010).

De skadliga virtuella maskinerna kan användas inne i datormolnet på grund av implementeringssättet, det vill säga på grund av det sättet hur de virtuella maskinerna kommunicerar med varandra inne i datormolnet. De virtuella maskinerna kommunicerar med varandra via hårdvaran i datormolnet och inte via nätverk. På grund av att kommunikationen sker via hårdvaran, kan inte traditionella sätt att kontrollera nätverkssäkerheten användas på de virtuella maskinerna, utan andra sätt för att kontrollera de virtuella maskinerna måste hittas (Chandramouli & Mell, 2010) (Cloud Security Alliance, 2009).

Om isoleringen i datormolnet är bristfälligt, det vill säga om en skadlig virtuell maskin finns i ett datormoln, kan användarna av datormolnet önska försäkran på att deras virtuella maskiner inte skadas av den. Detta ställer till med nya problem, till exempel kan användarna av datormolnet önska sig att flytta ut sina virtuella maskiner från en erbjudare till en annan. Problemet med en sådan lösning är hur man i praktiken kan flytta en virtuell maskin från en datormolnerbjudare till en annan (Chandramouli & Mell, 2010).

4. Lösningar till problemen

Under denna rubrik behandlas lösningar till de problemen som presenterades i kapitlet 3. ”Problem inom datormolnet”. Om inte någon direkt lösning till ett visst problem existerar, kommer möjliga sätt för att minimera påverkningen av problemet att presenteras.

4.1. Tillgänglighet

Rubriken och underrubrikerna kommer att behandla problemen med tillgänglighet och presentera lösningar som varierar från samarbete, till upprätthållning av standarder och krav. Lösningarna hjälper både användarna och erbjudarna av datormolnet.

4.1.1. Lösningar för inlåsning av data

För att hitta en lösning till inlåsning av data måste problemet först delas upp i två delar: problemen med opassande och ostandardiserade API:er samt problemen med att datormolnerbjudaren stänger ner tjänsten. Efter att uppdelningen är gjord, kan man försöka hitta lösningar var och en av dem.

Opassande och ostandardiserade API:er har uppstått eftersom ingen centralorganisation för datormolnet har bestämt sig för att upprätthålla någon API-standard som datormolnerbjudare skulle kunna följa. Standardiserade API:er skulle lösa inlåsning av data och det skulle även göra det möjligt för användare att lättare byta datormolnerbjudare (Armburst, o.a., 2009). Med standardiserade API:er skulle användare också kunna utnyttja flera datormolnerbjudare samtidigt, utan att ha risken att data kommer att vara opassande med varandra. Standardiserade API:er skulle också lösa problemet med att en datormolnerbjudare utnyttjar inlåsning av data för att upprätthålla sin

kunddatabas, eftersom en erbjudare skulle inte längre kunna låsa in användaren till datormolnet (Armburst, o.a., 2009).

Problemet med att en datormolnerbjudare stänger av sitt datormoln kan lösas på flera sätt. En möjlighet är att användaren använder sig av flera datormolnerbjudare samtidigt. Då minimerar användaren riskerna associerade med att datormolnerbjudaren försvinner, eftersom samma data finns då lagrat hos en annan erbjudare och kan därifrån fortsätta att användas (Armburst, o.a., 2009).

Rätt användning av ett *service level agreement* eller ett SLA leder också till att risken med inlåsning av data minimeras. Ett SLA är ett lagligt dokument där både användaren av datormolnet och datormolnerbjudaren binder sig till att följa vissa regler. Därför kan man i ett SLA inkludera punkter om vad både erbjudaren och användaren ska göra för att minimera risken för inlåsning av data. Punkter kan också läggas till där det beskrivs hur man hanterar eventuell inlåsning av data. Sådana punkter kan vara speciellt viktiga för företag där det är ytterst viktigt att företaget kan fortsätta med sina operationer även om inlåsning av data har uppstått (Kandukuri;Paturi;& Rakshit, 2009).

4.1.2. Lösningar för DDOS-attacker

I rubriken 3.1.2. ”DDOS-attacker mot datormoln” presenterades lösningen för hur DDOS-attacker kan hanteras i datormolnet. Lösningen var att datormolnet kan automatiskt allokera nya resurser för att hantera den inkommande attacken. Problem kan dock uppstå med denna lösning.

När resurserna allokeras till att hantera den inkommande attacken, kan möjligtvis tillgängligheten av andra tjänster i datormolnet påverkas (Jensen;Schwenk;Gruschka;& Iacono, 2009). Detta sker på grund av att attackeraren kan försöka, istället för att ta ner hela datormolnet, att ta ner endast en server i molnet. När denna server sedan är nere, kan till och med hela datormolnet slutligen kollapsa och sluta ta emot användarnas förfrågningar (Jensen;Schwenk;Gruschka;& Iacono, 2009).

För att ett datormoln ska kunna hantera en inkommande DDOS-attack, måste resurserna i datormolnet motsvara resurserna som attackeraren har tillgängligt under attacken. Om resurserna i datormolnet överskrider attackerarens,

kommer DDOS-attacken inte att lyckas eftersom datormolnet kommer att kunna hantera den (Armburst, o.a., 2009). Exempelkalkyleringar har bevisat att DDOS-attackeraren behöver stora ekonomiska- och hårdvaruresurser, för att kunna motsvara resurserna som finns i datormolnet. För att utföra en lyckad attack, måste attackeraren även ha mycket tid för att utföra attacken (Armburst, o.a., 2009).

4.1.3. Lösningar för allmänna problem med tillgänglighet

Lösningar till de allmänna problemen med tillgänglighet kan hittas i olika certifikat som datormolnerbjudarna kan använda. Certifikaten försäkrar kunden om att erbjudaren kommer att ta ordentliga åtgärder om ett eventuellt problem med tillgänglighet uppstår (Magnusson, 2010).

4.2. Pålitlighet

Under denna rubrik kommer lösningar till problemen som presenterades i kapitlet 3.2. ”Pålitlighet” att gås igenom. Huvudsakligen kommer lösningarna att behandla erbjudaren av datormolnet, och hur erbjudaren kan förbättra pålitligheten. Vissa av lösningarna kommer dock även att behandla användaren av datormolnet. Allmänt kan det konstateras att pålitligheten av datormolnet troligtvis kommer att förbättras av erbjudare som lyckas locka många användare till sig, och på så sätt få ett positivt rykte för datormolnet (Armburst, o.a., 2009).

4.2.1. Lösningar till övergivning av kontroll av data

Problemen som togs upp i rubriken 3.2.1. ”Övergivning av kontroll av data” var: problemen med data sparad inne i ett visst område, problemen med revidering av data och problemen med säkerhetskopiering av data. I denna rubrik kommer lösningar till varje av dessa problem att försöka hittas.

Lösningen till svårigheten med att data ska vara sparad inne i ett visst område, eller ett visst land, kan lösas av datormolnerbjudaren. Då måste datormolnerbjudaren ha servrar placerade i flera olika regioner och nationer, och även ha en möjlighet för användaren att sedan kontrollera var data ska placeras. Till exempel har Amazon en möjlighet för användaren att precisera i vilket område användaren vill att data ska vara sparat (Armburst, o.a., 2009). Genom denna enkla lösning kan datormolnerbjudaren lösa problemet med data och dess placering. För att vidare försäkra användaren om att data säkert är sparat i det

korrekta området kan man kräva att det i SLA:t ingår uppgifter om datas placering (Kandukuri;Paturi;& Rakshit, 2009).

För att försäkra att en användares data är korrekt placerad i datormolnet kan revidering av data användas. Problemet med revidering är dock hur den kan implementeras korrekt i datormolnet. Till exempel kan revideringen läggas till som ett lager under det virtualiserade lagret. På så sätt tillförsäkrar man användaren av datormolnet att inget program som körs på andra virtuella maskiner i datormolnet kan påverka revideringen genom att skicka fel data till revideraren (Armburst, o.a., 2009). För att ännu försäkra användaren om att de data som är sparade i datormolnet är korrekta, kan SLA:t användas för att få ett bindande kontrakt mellan användaren och erbjudaren av datormolnet (ENISA, 2009). I SLA:t kan man då lägga till punkter för att data ska kunna revideras och genom revideringen bevisa att data är korrekt (Kandukuri;Paturi;& Rakshit, 2009).

Att segmentera data mellan flera datormolnerbjudare är en lösning för problemet med att ha säkerhetskopior på data sparade inne i molnet (Chandramouli & Mell, 2010). Genom att ha segmenterade data kan användarna av datormolnet flytta data mellan datormolnerbjudarna, och undvika risken med att data förloras. En effektiv segmentering av data kräver dock att datormolnen har standardiserade API:er. De standardiserade API:erna gör att data kan direkt flyttas från ett datormoln till ett annat (Chandramouli & Mell, 2010).

Om en användare inte vill använda sig av flera datormoln för att försäkra sig om att data är säkert, måste användaren använda sig av datormolnerbjudare som har säkerhetskopieringsmöjligheter (Chandramouli & Mell, 2010). Till exempel erbjuder Amazon Amazon RDS (Relational Database Service) för sina användare för säkerhetskopiering. I denna tjänst ingår gratis säkerhetskopiering för upp till 100% av data sparat i databasen (Amazon Web Services LLC, 2010).

4.2.2. Lösningar för oförutsebar prestanda

För att lösa problemen med variationerna i både svar- och skrivtiderna till I/O-enheterna kan två olika sätt användas. Antingen kan man förbättra arkitekturen av själva hårdvaran eller använda sig av annan hårdvara i I/O-enheterna. Förbättringen av arkitekturen leder till att avbrotten av I/O-enheterna effektiveras (Armburst, o.a., 2009).

Nuförtiden används skivminnen för att lagra data i datormolnet, men genom att byta till snabbare flashminnen skulle datormolnerbjudarna kunna minimera riskerna med oförutsebar prestanda (Armburst, o.a., 2009). I Tabell 2 presenteras en jämförelse av åtkomsttiderna för både skivminnen och flashminnen.

Media	Åtkomsttid	
	Läs	Skriv
Skivminne	12.7 ms (2 K)	13.7 ms (2 K)
Flashminne	80 µs (2 K)	200 µs (2 K)

Tabell 2. Jämnförelse av åtkomsttiderna för både skivminnen å flashminnen (Ming;Yan;& Jiajin, 2009).

Eftersom flashminnen är snabbare än skivminnen, skulle en användning av dem i datormolnet resultera i ett större genomflöde av hanterade läs- och skrivförfrågningar, vilket i sin tur skulle minimera variationen i läs- och skrivtiderna (Armburst, o.a., 2009). Användningen av flashminnen skulle också minska energianvändningen av datormolnet, eftersom flashminnen använder mindre energi än de mekaniska skivminnen (Armburst, o.a., 2009).

4.2.3. Lösningar för pålitligheten av datormolnerbjudaren

Pålitligheten av datormolnerbjudaren omfattade problem såsom oprofessionell personal och dilemman med outsourcing. I grunden är dessa problem konkreta svårigheter som uppstår på grund av att ansvaret flyttas från användaren till erbjudaren av datormolnet. Därför kan ingen teknisk lösning hittas till dessa problem, utan man måste söka en förklaring i relationen mellan användaren och erbjudaren (ENISA, 2009).

Innan en användare börjar använda datormolnet, rekommenderas det att användaren jämför olika datormolnerbjudare och vad de erbjuder. Målet med denna jämförelse är att användaren kan försäkra sig om att erbjudaren möter kraven på pålitligheten (ENISA, 2009). För att vidare försäkra pålitligheten av erbjudaren kan SLA:t användas. Eftersom SLA:t är det enda kontraktet som används mellan en användare och erbjudare, kan man ha SLA:t att inkludera punkter som minimerar riskerna med pålitlighetsproblemen mellan användaren och erbjudaren (Kandukuri;Paturi;& Rakshit, 2009).

4.3. Säkerhet

För problemen som presenterades i rubriken 3.3. ”Säkerhet” kommer det att presenteras lösningar under denna rubrik. De presenterade lösningarna kommer att kräva att både datormolnerbjudaren och datormolnets användare tar tag i problemen. I rubriken 4.3.1. ”Lösningar för kryptering och skyddandet av data” presenteras lösningar för både användaren av datormolnet och erbjudaren av datormolnet.

4.3.1. Lösningar för kryptering och skyddandet av data

I rubriken 3.3.1. ”Problem med kryptering och skyddandet av data” togs två olika problem upp. Problemen som presenterades var skyddandet av data i flytt och problemen med skyddandet av data som är lagrade.

Lösningen för skyddandet av lagrat data var kryptering, men oklarheter uppstod med hanteringen av krypteringsnycklarna. Ingen klar lösning för hanteringen av krypteringsnycklarna har ännu uppstått, men det finns sätt för hur man kan minimera riskerna associerade med krypteringsnycklarna (Chandramouli & Mell, 2010) (Cloud Security Alliance, 2009). Till exempel kan användaren av datormolnet minimera risken med att krypteringsnycklarna hamnar till en otillåten part, genom att inte spara krypteringsnycklarna hos erbjudaren av datormolnet utan att spara de lokalt. Med en sådan lösning måste dock användaren antingen skicka nycklarna till erbjudaren av datormolnet när enkryptering eller dekryptering behövs, eller enkryptera och dekryptera data lokalt och sedan skicka data tillbaka till datormolnet. (Cloud Security Alliance, 2009). Om krypteringsnycklarna skickas till erbjudaren måste användaren dock försäkra sig om att erbjudaren tar bort allt nyckelmaterial efter att det inte behövs mera

(Encrypted Storage and Key Management for the Cloud, 2009). Säkerhetskopiering av krypteringsnycklarna är också viktigt, eftersom om krypteringsnycklarna tappas bort har inte användaren längre tillgång till data som är sparade med de krypteringsnycklarna (Cloud Security Alliance, 2009).

Skyddandet av data i flytt kan lösas i datormolnet genom att använda sig av olika säkerhetsprotokoll. Användaren kan utnyttja TLS, *transport layer security*, för att uppnå en säker flytt av data mellan användaren av datormolnet och datormolnet (Network Working Group, 2008) (Chandramouli & Mell, 2010) (Jensen;Schwenk;Gruschka;& Iacono, 2009).

4.3.2. Lösningar för problemen med isolering

I rubriken 3.3.2. ”Problemen med isolering” presenterades säkerhetsproblemet i datormolnet där skadliga virtuella maskiner kan komma åt andra virtuella maskiner i datormolnet. Problemet uppstod på grund av att isoleringen mellan de virtuella maskinerna är bristfällig och även på grund av hur de virtuella maskinerna kommunicerar med varandra i datormolnet.

För att lösa den bristfälliga isoleringen kan en hypervisor användas. En hypervisor kan brukas för att kontrollera att alla virtuella maskiner som körs på hårdvaran är isolerade och att de inte kan skada varandra. Detta uppnås bland annat med hjälp av olika meddelanden som genereras av hypervisorn när olika väsentliga säkerhetsproblem identifieras. Såsom när en skadlig virtuell maskin har hittats i datormolnet. (Amazon Web Services LLC, 2009) (Chandramouli & Mell, 2010). Det bör dock noteras att även om en hypervisor används, kan olika bristfälligheter i själva hypervisorn orsaka att skadliga virtuella maskiner kan användas (ENISA, 2009) (King;Chen;Ya-Min;Verbowski;Wang;& Lorch, 2006).

Om en skadlig virtuell maskin har hittats, kan användaren av datormolnet möjligen önska sig att flytta över sina virtuella maskiner till ett annat datormoln. För att detta ska vara möjligt måste datormolnerbjudarna använda sig av liknande standarder för att importera och exportera de virtuella maskinerna (Chandramouli & Mell, 2010). Om användaren söker sig att flytta över de virtuella maskinerna i realtid måste även hårdvaran av datormolnen vara liknande. Instruktionsuppsättningen av den tidigare hårdvaran och den nya hårdvaran är alltså densamma (Chandramouli & Mell, 2010).

5. Sammanfattning och diskussion – är datormolnet bristfälligt?

I detta kapitel kommer en sammanfattning av de presenterade problemen och lösningarna att göras, genom att undersöka huruvida problemen blev lösta, eller om frågor ännu är obesvarade. Efter att denna sammanfattning är gjord, kan man svara på frågan huruvida datormolnet är bristfälligt.

För att klart illustrera problemen och lösningarna presenteras en tabell över problemen och deras lösningar i Tabell 3. Från tabellen kan man läsa att för varje problem som togs upp hittades alltid en lösning. Eftersom man hittade en lösning för varje problem, kunde man dra slutsatsen att det inte finns några problem, eller bristfälligheter i datormolnet. Personligen anser jag dock att det finns problem och bristfälligheter i datormolnet, men att de kan lösas i framtiden.

Problem	Lösning
Inlåsning av data	·Standardiserade API:er ·Använda flera datormoln samtidigt ·SLA
DDOS-attacker mot datormolnet	·Tillräckligt mycket resurser i datormolnet
Allmänna problem med tillgänglighet	·Certifikat
Övergivning av kontroll av data	·Ha möjligheten att precisera placering av data ·Segmentering av data + ha möjlighet till säkerhetskopiering
Oförutsebar prestanda	·Förbättring av hårdvaruarkitektur ·Anvädning av flashminnen
Pålitlighet av datormolnerbjudaren	·Jämföra datormolnerbjudare ·SLA
Problem med kryptering och skyddandet av data	·Spara krypteringsnycklarna lokalt ·Anvädning av skyddade anslutningar vid flytt av data
Problem med isolering	·En säker hypervisor ·Erbjuda realtidsflyttning av virtuella maskiner

Tabell 3. Sammanfattning av problemen och deras lösningar

Jag anser att problem med inlåsning av data och problem med isolering är de största bristfälligheterna i datormolnet, eftersom lösningarna till dessa problem är sådana som inte ännu kan erbjudas av alla datormoln. Problemen

är också viktiga, speciellt för företag som söker sig att använda datormolnet, eftersom de kan ställa till med ekonomiska problem (ENISA, 2009). Till exempel problem med inlåsning av data kunde lösas genom att standardisera API:er som datormolnen har. En sådan lösning är dock tidskrävande, och kan inte implementeras genast. En liknande, tidskrävande, lösning kunde hittas till att lösa problem med isolering, där datormolnet kunde lösa problem med skadliga virtuella maskiner genom att erbjuda realtidsflyttning av virtuella maskiner.

Lösningarna som kräver standardisering av datormolnen är tidsödande, eftersom det kräver att alla erbjudare ändrar sina datormoln för att följa en viss standard. Men i framtiden kan man dock tänka sig att olika organisationer, som till exempel Open Cloud Consortium som är en organisation som försöker skapa standarder till datormolnet, kommer att lyckas skapa standarder som kan implementeras i alla datormoln (Open Cloud Consortium, 2009).

Även om vissa av problemen är ännu olösta, kan man tänka sig att man kan minimera risken med att problemen blir allvarliga genom att användaren och erbjudaren använder sig av SLA:t och andra legala kontrakt. SLA:t kan användas för att specificera hur inlåsning av data hanteras (Kandukuri;Paturi;& Rakshit, 2009). Om en SLA används rätt, kommer den att minimera riskerna med inlåsning av data, och på så sätt också minimera bristfälligheterna av datormolnet.

Allmänt kan det konstateras att bristfälligheterna i datormolnet kan minimeras genom att användaren noggrant kontrollerar hur datormolnet som den tänker använda är. Till exempel kan användaren kontrollera hurdan säkerhetskopiering datormolnet erbjuder, eller hurdana standarder datormolnet följer. Om detta görs korrekt, uppstår inga falska förhoppningar i till exempel pålitlighet mellan användaren och erbjudaren av datormolnet. Och samtidigt har också riskerna för att bristfälligheter finns minimerats.

Litteraturlista

Amazon Web Services LLC. (2010). *Amazon Elastic Compute Cloud (Amazon EC2)*. Hämtat från Amazon Web Services: http://aws.amazon.com/ec2/ den 12 Mars 2010

Amazon Web Services LLC. (2010). *Amazon Relational Database Service (Amazon RDS)*. Hämtat från Amazon Web Services: http://aws.amazon.com/rds/ den 17 Mars 2010

Amazon Web Services LLC. (November 2009). *Amazon Web Services: Overview of Security Process document.* Hämtat från Amazon Web Services: http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf den 22 Mars 2010

Armburst, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., o.a. (2009). *Above the Clouds: A Berkeley View of Cloud Computing* . Electrical Engineering and Computer Sciences University of California at Berkeley.

Brooks, C. (den 9 December 2009). *Amazon outage caused by power failure during Virginia storm*. Hämtat från SearchCloudComputing.com: http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_gci1376474,00.html den 3 Mars 2010

Brooks, C. (den 17 Juni 2009). *Users undeterred by Amazon EC2 lightning snafu*. Hämtat från SearchCloudComputing.com: http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_gci1359572,00.html den 13 Mars 2010

Buyya, R., Yeo, C., Venugopal, S., Broberg, J., & Brandic, I. (2008, September 23). *Cloud computing and emerging IT platforms: Vision, hype, andreality for delivering computing as the 5th utility* . Future Generation Computer Systems.

Chandramouli, R., & Mell, P. (2010). State of Security Readiness. *Crossroads - The ACM Student Journal* , 23-25.

Cloud Security Alliance. (den 17 December 2009). *Security Guidance for Critical Areas of Focus in Cloud Computing.* Hämtat från Cloudsecurityalliance.org: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf den 22 Mars 2010

Encrypted Storage and Key Management for the Cloud. (den 23 Juli 2009). Hämtat från Cryptoclarity: http://www.cryptoclarity.com/CryptoClarityLLC/Welcome/Entries/2009/7/23_Encrypted_Storage_and_Key_Management_for_the_cloud.html den 16 Februari 2010

ENISA. (den 20 November 2009). Cloud Computing Risk Assessment.

Google. (2010). *App Engine Frameworks*. Hämtat från Code.google.com: http://code.google.com/p/tipfy/wiki/AppEngineFrameworks den 12 Mars 2010

Grossman, R. (2009, Mars/April). The Case for Cloud Computing. *IT Professional* , pp. 23-27.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. (2009). *On Technical Security Issues in Cloud Computing* . Horst Görtz Institute for IT Security Ruhr Universtiy Bochum.

Kandukuri, B., Paturi, R., & Rakshit, A. (2009). *Cloud Security Issues* . Advanced Software Technologies International Institute of Information Tehcnology Pune, India.

King, S. T., Chen, P. M., Ya-Min, W., Verbowski, C., Wang, H. J., & Lorch, J. R. (2006, Maj 21-24). Sub Virt: Implementing malware with virtual machines. *2006 IEEE Symposium on Security and Privacy* .

Krigsman, M. (den 27 Augusti 2008). *MediaMax / The Linkup: When the cloud fails*. Hämtat från ZDNet: http://blogs.zdnet.com/projectfailures/?p=999 den 12 Mars 2010

Kuhlin, B., & Thielmann, H. (2005). Real-time business requires security, trust and availability. i *The Practical Real-Time Enterprise Facts and Perspectives* (ss. 275-284). Berlin: Springer Berlin Heidelberg.

Launchpad Europe. (den 25 November 2009).
Security concerns influence organisational enthusiasm for adopting cloud technologies, s ays Launchpad Europe. Hämtat från Launchpad-Europe.com: http://www.launchpad-europe.com/images/PR07LPDE-ITSecurityintheCloudFV.pdf den 20 March 2010

Magnusson, A. (den 17 Februari 2010). *Ökad risk med data i molnet*. Hämtat från TechWorld.se: http://techworld.idg.se/2.2524/1.291066/okad-risk-med-data-i-molnet den 12 Mars 2010

Ming, D., Yan, Z., & Jiajin, L. (2009). Using Flash Memory as Storage for Read-intensive Database. *Database Technology and Applications, 2009 First International Workshop on* (pp. 472 - 475). Wuhan, Hubei: Glorious Sun Sch. of Bus. & Manage., Donghua Univ., Shanghai, China.

Network Working Group. (Augusti 2008). *The Transport Layer Security (TLS) Protocol Version 1.2*. Hämtat från The Internet Engineering Task Force (IETF): http://www.ietf.org/rfc/rfc5246.txt den 23 Mars 2010

Open Cloud Consortium. (2009). *About OCC*. Hämtat från Opencloudconsortium.org: http://opencloudconsortium.org/about-occ/ den 29 Mars 2010

Salesforce.com, inc. (2010). *Unlimited real-time database customizations*. Hämtat från Salesforce.com: http://www.salesforce.com/platform/cloud-platform/database.jsp den 12 Mars 2010

Stein, L., & John, S. (den 23 Februari 2003). *8. Securing against Denial of Service attacks*. Hämtat från The World Wide Web Security FAQ: http://www.w3.org/Security/Faq/wwwsf6.html den 12 Mars 2010

Söderling, M. (den 2 Februari 2010). *Så fungerar molnet*. Hämtat från TechWorld.se: http://techworld.idg.se/2.2524/1.290664 den 26 Februari 2010

Urquhart, J. (den 9 Januari 2009). *The biggest cloud-computing issue of 2009 is trust*. Hämtat från Cnet.com: http://news.cnet.com/8301-19413_3-10133487-240.html den 15 Mars 2010