Åbo Akademi

Utmaningar och säkerhetshot i molntjänster

Jimmy Westerlund 39053

Kandidatavhandling i datateknik

Våren 2018

Handledare: Dragos Truscan

Referat

Syftet med denna avhandling är att klargöra vad molntjänster är, säkerhetshot inom molntjänster samt hur man kan förebygga dessa hot.

I det första och andra kapitlet går jag genom molntjänsters uppbyggnad och användningsområden. I det tredje kapitlet går jag genom olika former av utmaningar som kan uppstå vid användningen av molntjänster och vilka metoder man kan använda för att förebygga och lösa dessa problem. Jag kommer främst att fokusera på datasäkerhet, men även andra former av utmaningar kommer att nämnas. Avhandlingen avslutas med en kort diskussion kring de behandlade områden.

Innehåll

1. Inledning

År 1963 blev Massachusetts Institute of Technology (MIT) beviljade två miljoner dollar av DARPA (the Defense Advanced Research Projects Agency) för Project MAC [14]. Målet med projektet var att utveckla en dator som två eller flera personer kunde använda samtidigt. Detta var en början till vad som i dag kännetecknas som molntjänster.

Amazon var en av första stora företagen som började erbjuda olika former av tjänster via moln. År 2006 lanserades Amazon Web Services, som bland annat erbjöd molnbaserad lagring och beräkningskraft [14]. Google kom tätt efter och samma år introducerades Google Docs, som gav användaren möjligheten att editera och spara dokument i en molnmiljö.

För 10 år sedan var molntjänster i allmänhet ännu relativt nya för företag. I en undersökning 2008 svarade endast 12% av företagen att de föredrog molnbaserade lösningar [15]. År 2018 förväntas å andra sidan det genomsnittliga företaget att ha över 50% av program och it-infrastruktur i moln [2].

Molntjänster erbjuder möjligheten att ersätta gamla system på ett kostnadseffektivt och smidigt sätt. Den ökade popularitet en av molntjänster medför dock också nya utmaningar som inte existerat i traditionella it-lösningar. I avhandlingen kommer jag att behandla uppbyggnaden av molntjänster, vilka utmaningar och risker inom datasäkerhet som kan uppstå samt möjliga metoder för att lösa problemen.

2. Molntjänster

Hårdvaran och idén för molntjänster har funnits sedan 60-talet, men kombinationen av ny teknik och nya koncept är orsakerna till molntjänsternas framgång under 2000-talet. Genom molntjänster kan man använda både mjukvara och hårdvara virtuellt, vilket betyder att man kan hyra den tjänst som behövs via internet, istället för att köpa mjukvaran och/eller hårdvaran. Mjukvarulicenser är i vanliga fall väldigt dyra, men i molntjänster kan kunden betala licenser i form av prenumerationer.

Det finns ingen generell definition för begreppet molntjänster, eftersom det är ett väldigt omfattande område utan tydliga gränser. Enligt Vic (J.R.) Winkler, som skrivit boken ”Securing The Cloud: Cloud Computer Security Techniques and Tactics”, är molntjänster följande: ”Tjänster som uttrycks, levereras och konsumeras över internet eller ett privat nätverk. Molntjänster varierar från Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) och Software-as-a-Service (SaaS) och inkluderar allt annat som använder dessa tjänster för att skapa nya tjänster. Dessa tjänster kan implementeras privat, offentligt eller i kombination.” (egen översättning från engelska) [1].

Grunden av ett moln kan grovt delas in i fem kategorier [1]:

- *Infrastruktur:* En samling av servrar, datorlagring, och nätverkskomponenter som är gjorda för att hantera snabb tillväxt som traditionell it-infrastruktur inte skulle klara av.
- *Nätverk:* Molntjänster används av kunden via internet. Nätverket bör vara väldigt pålitligt och för att uppfylla säkerhetsbestämmelser används ofta flera parallella nätverk för att separera offentliga data från privat data.
- *Virtualisering:* Detta innebär att dela in en fysisk server i flera virtuella servrar eller en fysisk resurs, exempelvis lagring, i flera virtuella lagringsutrymmen. Det är en kostnadseffektiv lösning som ger väldigt mycket flexibilitet eftersom fysiska resurser snabbt kan virtualiseras och tas i- eller ur bruk.
- *Mjukvara:* För att knyta samman ett moln krävs mjukvara som möjliggör bokföring, säkerhet, leverering och administration av infrastrukturen. Mjukvaran ger även möjlighet att ta en tjänst i- eller ur bruk automatiskt.

- *Servicegränssnitt:* Användargränssnittet mellan kunden och leverantören, körs via en webbläsare eller ett API (application programming interface). Användarvänliga gränssnitt med självbetjäning är nyckeln till framgång ur leverantörens synvinkel. Det sparar tid och pengar för båda parter eftersom kunden själv kan reglera sina virtuella tillgångar via en webbläsare utan att leverantören behöver ingripa.

IDG Enterprise utförde en undersökning år 2016, med målet att samla in information om olika företags anpassningar av molntjänster [2]. I undersökningen deltog 925 personer från företag världen över, från branscherna: finansiella tjänster (13%), utbildning (12%), högteknologi (11%), statliga och icke-vinstdrivande (10%) och tjänster (9%) [2]. Undersökningen visade att företag i medeltal hade förflyttat 45% av applikationer och it-infrastruktur till moln år 2016, och andelen förväntas stiga till ungefär 60% under år 2018. Av företagen använde 70% åtminstone en molnapplikation eller någon del av it-infrastrukturen i moln, och de resterande 30% hade planer för att ta i bruk molntjänster under de kommande 1–3 åren. Det finns fyra huvudsakliga positiva aspekter av molnlösningar som attraherar it-beslutsfattare, de är: sänka total ägandekostnad, ersättning av gamla system, möjliggöra affärskontinuitet, samt ökad utvecklingshastighet. Stora företag (mer än 1000 anställda) är mer benägna än mindre företag att satsa deras molnbudget på att utvecklingshastighet, testning och stordatastrategier. Mindre företag är å andra sidan mer benägna att satsa på affärskontinuitet och säkerhet [2]. Företag satsade i medeltal 28% av deras it-budget på molntjänster år 2016.

2.1 Lager i molnet

Molntjänster är uppbyggda på olika sätt baserat på användningsområde. Det finns ett flertal olika modeller som används som riktlinjer vid utveckling och beskrivning av molntjänster. De tre vanligaste är Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) och Infrastructure-as-a-Service (IaaS). Förkortat kallas dessa SPI-modellen. De tre modellerna bygger ofta på varandra, men kan också implementeras enskilt.

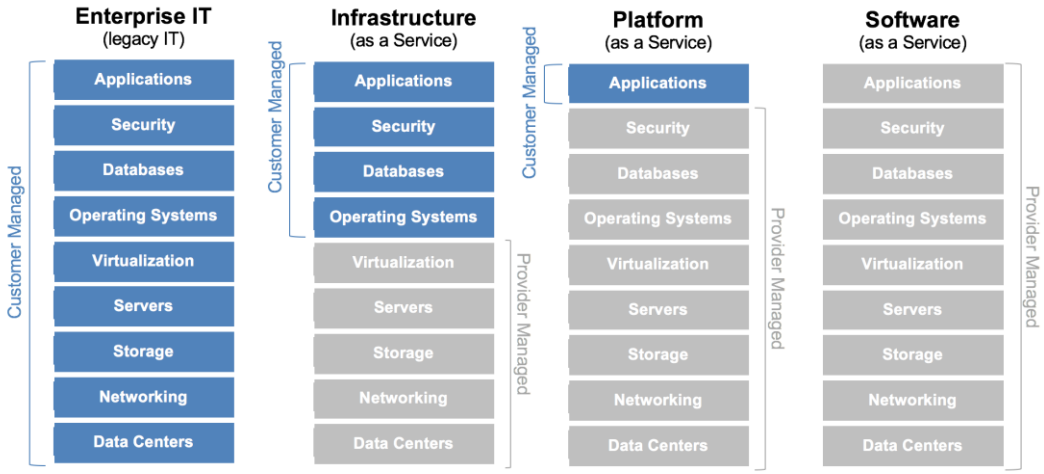
Ett genomsnittligt företag planerar att fördela sin molnbudget på följande vis [2]:

- 45% på Software-as-a-Service

- 30% på Infrastructure-as-a-Service
- 19% på Platform-as-a-Service
- 6% på övriga as-a-Service modeller

Skillnaden mellan stora företag (mer än 1000 anställda) och mindre företag är att stora företag planerar att investera mer på PaaS, medan mindre företag satsar mer än stora företag på SaaS [2].

Figur 1 visar traditionell IT struktur (längst till vänster) i jämförelse med SPI-modellen. I IaaS hanterar kunden en hel del själv (målat i blått), såsom applikationer, säkerhet, databaser och operativsystem. I PaaS hanterar kunden endast applikationer och i SaaS hanterar molnleverantören allt. Molnleverantörer är företag som är specialiserade inom molnbaserade lösningar, t.ex. infrastruktur, lagring och program.



Figur 1: Traditionell IT (till vänster) jämfört med SPI-modellen. Källa: https://apprenda.com/

2.1.1 Infrastructure-as-a-Service

Infrastructure-as-a-Service erbjuder konsumenten ett virtuellt datacenter som omfattar servrar, nätverk, lagring och säkerhet. Konsumenten har kontroll över operativsystem, lagring och utveckling av applikationer, men inte molninfrastrukturen.

Fördelarna med IaaS är huvudsakligen skalbarhet och kostnadseffektivitet. Ifall konsumenten behöver mera eller mindre infrastruktur kan detta smidigt regleras enligt behov. Kostnaderna i IaaS har direkt anknytning till resursanvändning.

Några välkända exempel på IaaS leverantörer är Amazon EC2 och RackSpace [1].

2.1.2 Platform-as-a-Service

Platform-as-a-Service erbjuder konsumenten en miljö för utveckling, testning, distribution och uppdatering av applikationer, samt ett moln för konsumentens slutliga applikation eller tjänst. Konsumenten behöver ingen kunskap om vad som händer i molninfrastrukturen, men han har kontroll över den utvecklade applikationen. PaaS är väldigt nära släkt med SaaS, men i PaaS är syftet med tjänsten utvecklingsmiljön.

Fördelarna med PaaS är bland andra prisvärda verktyg och en smidig utvecklingsmiljö. Konsumenten betalar endast för de resurser som används, vilket ger möjlighet att använda verktyg som i annat fall skulle vara för dyra.

Exempel på PaaS applikationer är Microsoft Azure och Google App Engine [3].

2.1.3 Software-as-a-Service

Software-as-a-Service ger konsumenten möjligheten att använda leverantörens applikationer över ett moln. Som i PaaS behöver konsumenten ingen kunskap om vad som händer i molninfrastrukturen och är befriad från hantering och underhåll gällande nätverk, servrar och lagring [1]. Denna tjänst kan antingen hyras eller betalas enligt användning.

SaaS är en flexibel lösning som passar bra speciellt ifall konsumentens användningsbehov av en viss applikation varierar mycket. Exempel på applikationer som använder SaaS modellen är Google’s Gmail, Netflix och Dropbox [1][3]. SaaS kommer oftast i form av prenumeration.

2.2 Distributionsmodeller i molntjänster

En distributionsmodell representerar en viss typ av moln. Huvudsakligen kategoriseras molnen till en distributionsmodell baserat på äganderätt, storlek och tillgång. De fyra främsta distributionsmodellerna är offentliga-, privata-, bransch- och hybrida moln. Varje modell har sina för- och nackdelar gällande flexibilitet, kostnad och säkerhet. Alla dessa aspekter behandlas i de kommande underkapitlen.

År 2016 hade det genomsnittliga företaget 45% av sin it-miljö i moln [2]. Av denna andel var 23% i privata moln, 15% i offentliga moln, och 7% i hybrida moln. Förhållandet mellan privat- och offentligt moln varierar med företagsstorlek, mindre företag väljer oftast offentliga moln, medan större företag (mer än 1000 anställda) föredrar privata moln.

2.2.1 Offentliga moln

Molntjänster under denna kategori är tillgängliga för allmänheten eller en industrikoncern och ägs av en organisation som säljer molntjänster [5]. I offentliga moln erbjuds resurser som en tjänst, vanligtvis över en internetanslutning. Användaren behöver inte köpa hårdvara för att använda tjänsten och betalar enligt hur mycket resurser som används. Leverantören hanterar infrastrukturen och reglerar resurser enligt användarens behov [1]. Användare av offentliga molntjänster är oftast privata användare och ansluter till internet via en internetleverantörs nätverk. Exempel på leverantörer av offentliga molntjänster är Google, Amazon och Microsoft [4].

En stor fördel med offentliga molntjänster är kostnadseffektivitet, eftersom användaren endast betalar för använda resurser. Dessutom har användaren tillgång till toppmodern it-infrastruktur utan att behöva köpa och underhålla den. Användaren är befriad från underhåll av datorcentret som kör den offentliga molntjänsten i fråga. Leverantören har ansvar för att lösa eventuella problem i bakomliggande hårdvara och mjukvara.

Den största nackdelen med offentliga moln är att avancerade säkerhets- och sekretessbestämmelser är bortom deras förmågor. Det finns många lagar som offentliga molntjänster inte kan uppfylla eftersom deras användare delar samma it-infrastruktur. Exempelvis vid hantering av personuppgifter är det viktigt att tänka

på dataskyddsförordningen (GDPR), vars syfte är: ”att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.” [9]. Ett annat problem är att användaren inte nödvändigtvis vet var data sparas eller hur det är säkerhetskopierat.

Offentliga moln lämpar sig väl för utvecklingsplattformar eller webbläsare, för stor databehandling som ställer stora krav på datorresurser och för företag som inte har avancerade säkerhetskrav.

2.2.2 Privata moln

Privata molntjänster är väldigt likt offentliga molntjänster. En tydlig skillnad mellan de två är att en privat molntjänst oftast är ämnad för en organisation. Den ägs, hanteras och drivs av organisationen, en tredje part eller i någon kombination av dem [5]. Tjänster som tillhör den privata sektorn kan i de flesta fall uppfylla säkerhetskrav som offentliga molntjänster inte kan. Detta är väldigt händigt för organisationer som har strikta bestämmelser om datasäkerhet inom olika avdelningar av organisationen.

Den största fördelen med privata molntjänster är att de kan skräddarsys enligt kundens behov. Kostnaden av privata molntjänster kan vara både en för- och nackdel. Ifall organisationen redan från förr äger ett datacenter och deras arbetsmängd inte varierar mycket kan privata molntjänster vara en kostnadseffektiv lösning. Om organisationen å andra sidan inte äger ett datacenter kan detta vara en dålig lösning, eftersom ett datacenter med personal är dyrt att skaffa.

Säkerhetsrisker finns dock också inom privata molntjänster. Fokuset är här att säkra utrustningen i virtualiseringsmiljön [1]. All hårdvara, mjukvara tillhörande datacentret administreras av organisationen eller en tredje part [5]. Till skillnad från offentliga molntjänster måste organisationen själv lösa eventuella problem gällande datacentret.

2.2.3 Branschmoln

Denna typ av molntjänster är avsedd för användning av en gemenskap av konsumenter från organisationer inom en viss bransch [5]. Exempelvis kan två

organisationer använda samma branschmolntjänst ifall de har liknande säkerhetskrav. Lika som för privata molntjänster administreras branschmolntjänster av de involverade organisationerna eller av en tredje part.

Eftersom denna distributionsmodell fungerar likadant som privata molntjänster är för- och nackdelarna också de samma. En avgörande skillnad är dock att branschmoln kan spara stora summor pengar. Flera organisationer med gemensamma intressen kan slå ihop sig och dela på kostnaden av ett eller flera datacenter, medan de behåller alla fördelar med privata molntjänster. Ur ett säkerhetsperspektiv är denna distributionsmodell också detsamma som privata molntjänster, givet att organisationerna har identiska juridiska restriktioner och överensstämmelser [1].

Denna distributionsmodell är ännu relativt ny i jämförelse med offentliga- och privata moln, men den har stor potential och dess användning har ökat kraftigt [4].

2.2.4 Hybrida moln

Den sista och mest komplexa distributionsmodellen är hybrida moln, som är en kombination av åtminstone ett offentligt moln och ett privat moln. I vissa fall är det dock en kombination av alla tre modeller [1].

Hybrida moln formas när en organisation utvecklar ett privat moln men även vill ha med egenskaper från offentliga- eller branschmoln. Oftast tas denna distributionsmodell i bruk när ett företag först utvecklar ett internt privat moln för den viktigaste infrastrukturen, följt av upptäckten att det inte är ekonomiskt lönsamt att implementera de resterande molnrelaterade funktionaliteterna internt [1]. Hybrida moln erbjuds vanligtvis på ett av två sätt: en leverantör har ett privat moln och bildar ett partnerskap med en leverantör av offentliga moln, eller en leverantör av offentliga moln bildar ett partnerskap med en leverantör av privata moln [4].

Ett vanligt exempel är att hybrida moln används för testning eller kvalitetssäkring. I detta exempel används ett privat moln för att köra ett företags infrastruktur, medan testning av en ny produkt, ett nytt system eller en uppgradering körs i ett offentligt moln. Detta kan vara en mycket smidig och kostnadseffektiv lösning, eftersom

användningen av den offentliga molntjänsten kan avslutas när testningen är genomförd [1].

Idén med hybridmodellen är alltså att kombinera de olika distributionsmodellerna på ett sådant vis att slutprodukten är en molntjänst med så många goda egenskaper som möjligt medan nackdelarna är så få som möjligt. I teorin är det lätt att välja vilka egenskaper man vill behålla och vilka som ska bort, men i praktiken är det inte så lätt.

För många företag är denna distributionsmodell en bra lösning. Kombinationen av offentliga- och privata moln ger bra kontroll och säkerhet, medan skalbarheten inte är något problem [4]. De offentliga molnen ger möjlighet att driva kortlivade projekt kostnadseffektivt. De ger även möjlighet till s.k. ”cloud-bursting”, vilket innebär att ett privat moln temporärt kan utvidgas till ett offentligt moln när efterfrågan på datorkapacitet hastigt ökar och överskrider kapaciteten av det privata molnet [4].

Det finns dock nackdelar även i hybrida moln och vissa företag har inte möjlighet att fullständigt använda sig av dem på grund av lagliga skäl. Företag och organisationer som hanterar känsliga kunddata kan stöta på problem vad det gäller kombinationen av privata- och offentliga moln, eftersom kunddata inte får lagras och hanteras externt av en tredje part [1].

3. Utmaningar och möjliga lösningar

Övergången till och användningen av molntjänster är långt ifrån problemfri. I grund och botten kan utmaningarna indelas i tre kategorier: juridik, arkitektur samt datasäkerhet [1].

I undersökningen som presenterades i kapitel 2 svarade 4 av 5 att de ville ha säljares hjälp med att sälja fördelarna med moln till interna intressenter [2]. I synnerhet kände de att de behövde hjälp med att lugna intressenter om molnsäkerhet. Säkerhetsaspekten i molntjänster är med andra ord av stor vikt.

3.1 Datasäkerhet

Genom outsourcing förlorar användarna den fysiska kontrollen över data eftersom den lagras i en avlägsen server och de överlåter kontrollen till en molnleverantör eller en tredje part [10]. Det finns många hot mot moln, inte bara från en utomstående men också från en insider, som kan använda molnets sårbarheter för att göra skada. Dessa hot kan äventyra datasekretess, dataintegritet och tillgänglighet av data [10]. Otillförlitliga leverantörer kan även dölja dataintrång för att rädda deras rykte, de kan även frigöra lite utrymme genom att radera mindre använda data. De största hoten vad gäller datasäkerhet är just nu dataintrång, dataförlust och överbelastningsattacker.

I undersökningen som presenterades i kapitel 2 svarade 4 av 5 att de ville ha säljares hjälp med att sälja fördelarna med moln till interna intressenter [2]. I synnerhet kände de att de behövde hjälp med att lugna intressenter om molnsäkerhet.

3.1.1 Informationsläckage

En molnmiljö innehåller en massa data från flera olika användare och organisationer. Eventuella läckage i denna molnmiljö skulle avslöja alla användares och organisationers data [10]. På grund molntjänsters arkitektur kan kunder som använder olika applikationer på virtuella maskiner dela samma databas, vilket betyder att eventuella läckage kommer att påverka alla som delar samma databas. De vanligaste orsakerna till informationsläckage är dataintrång och skadlig programvara [10].

3.1.2 Dataförlust

Företag lägger allt större andel av data i moln, men det är viktigt att tänka på att data kan gå förlorat, även i moln. Dataförlust kan orsakas av många olika orsaker, exempelvis sabotageattacker, serverkraschar, eller att leverantören oavsiktligt raderar data utan säkerhetskopiering [10]. Naturkatastrofer, som jordbävningar och bränder kan även leda till dataförlust. Händelser som leder till att skada krypteringsnycklar kan också leda till dataförlust.

För att undvika dataförlust kan man enligt Cloud Security Alliance (CSA) vidta följande åtgärder [10]:

- Skydda data som är i rörelse genom kryptering.
- Använda en stark API för tillträdeskontroll.
- Använda välutvecklade metoder för generering, lagring, förstörelse samt hantering av krypteringsnycklar.
- Specificera i ett kontrakt strategier för säkerhetskopiering och retention av data

3.1.3 Överbelastningsattacker

Somliga organisationer är mer sårbara för överbelastningsattacker (eng. Denial of Service) än andra, t.ex. de som erbjuder tjänster som måste vara tillgängliga varje dag, dygnet runt. En överbelastningsattack innebär att någon avsiktligen använder upp alla tillgängliga resurser, vilket leder till att en tjänst blir långsam eller helt slutar fungera [10]. Distribuerade överbelastningsattacker är en värre variant som innebär att många datorer används samtidigt för att angripa och överbelasta ett nätverk. Denna metod är svårare att förhindra och spåra.

I artikeln ” How to counter DDoS attacks in Cloud Computing” skriver Rick Blaisdell om några metoder för att skydda mot överbelastningsattacker [11]. Enligt Blaisdell bör man tänka på internet-bandbredd, en reserv-internetanslutning, sårbarheter i systemet, intrångsdetektion, och konfigurering av brandvägg. Ett överflöd av internet bandbredd betyder att attackeraren måste anstränga sig hårdare för att överbelasta nätverket, för att ytterligare säkra systemet bör man även ha en skild internetanslutning som kan användas i nödfall. Det är också viktigt att

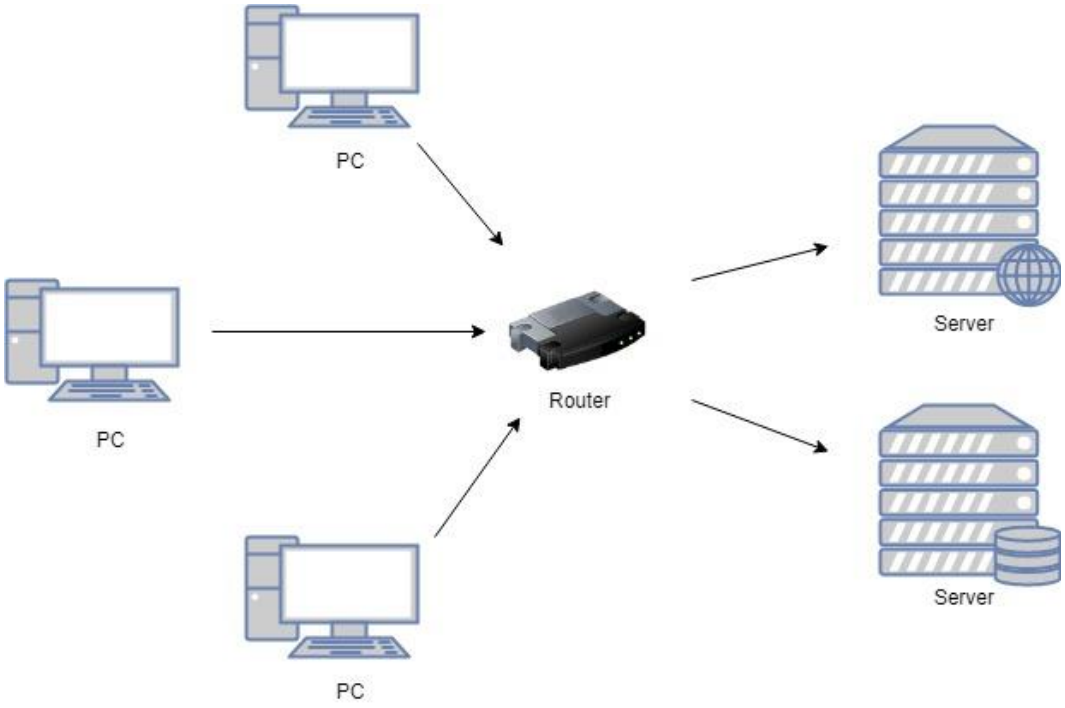
använda verktyg för att hitta eventuella sårbarheter i systemet, t.ex. föråldrad mjukvara. En brandvägg som är väl konfigurerad blockerar okända IP-adresser, medan ett program för intrångsdetektion (eng. intrusion detection system) slår larm om oönskad nätverkstrafik.

3.1.4 Felkritisk systemdel

En felkritisk systemdel (eng. single point of failure, SPOF) kan förekomma både i hårdvara och i mjukvara. Det är en svag länk i ett system som löper risk för att påverka hela systemets tillgänglighet och tillförlitlighet, det kan leda till dataförlust och i värsta fall kan den orsaka att systemet helt slutar fungera [10]. I mjukvara orsakar en felkristisk systemdel en s.k. flaskhalseffekt, som slöar ner systemet. Vad gäller molntjänster kan felkritiska systemdelar påträffas i själva molnarkitekturen hos leverantören.

Ett exempel på ett sådant system illustreras i Figur 2 på följande sida, var all trafik mellan användare och servrar går genom en endaste router. I detta fall är routern en felkritisk systemdel, eftersom användarna tappar kontakten med båda servrarna helt och hållet ifall routern slutar fungera.

För att eliminera felkritiska systemdelar i molnarkitekturen man använda redundans, både i hårdvara och i mjukvara [4]. Detta innebär att ha ett överflöd av identiska komponenter så att när en komponent i systemet slutar fungera fortsätter en annan komponent, utan avbrott. I hårdvara gäller detta t.ex. servrar, var man vanligtvis löser problemet genom att installera ett serverkluster. I mjukvara kan en lösning på detta problem vara att köra flera identiska instanser av mjukvaran parallellt [4].



Figur 2: System med en router som felkritisk systemdel.

3.1.5 Inlåsning

I undersökningen om molnanvändning utförd av IDG Enterprise fanns det en stor oro kring problemet att ”bli inlåst” hos en molnleverantör, speciellt i privata molntjänster [2]. Detta innebär att när en organisation är beroende av ett externt moln, på ett sådant vis att det inte lätt går att byta leverantör. En sådan situation kan skapas när ett företag till exempel tar i bruk en molntjänst för att hantera kundrelationer. Tid och pengar investeras i programmet för att skräddarsy det enligt företagets behov och stora mängder data processas och sparas i molnet. Om tjänsten dock bygger på proprietära format eller API: er, äger kunden endast all data, medan leverantören äger programmet [1]. Ifall kunden bestämmer sig för att byta leverantör kan det uppstå svåra problem, eftersom det utvecklade programmet som verksamheten är beroende av inte ägs av kunden. Även överföringen av data till en ny leverantör kan ställa till problem, om data också är proprietär. Ett annat scenario med samma problem vore om leverantören av någon anledning går i konkurs eller byter affärsmodell.

De flesta stora molnleverantörerna har lyckligtvis tagit hänsyn till detta problem. I dag undviks problemet oftast genom att erbjuda kunden möjlighet att närsomhelst

exportera data från en molntjänst [1]. Kunden bör dock observera att alla leverantörer inte nödvändigtvis använder samma dataformat, vilket kan leda till svårigheter vid överföring av data från en leverantör till en annan.

Ett praktiskt exempel på en leverantör som avvärjt inlåsningar på ett smidigt sätt är Google [1]. I Google Docs kan användaren när som helst exportera sina Google dokument, även till andra format som används av exempelvis Microsoft.

3.2 Datakryptering

I detta kapitel går jag grundligt genom krypteringens funktion i molntjänster. Modern kryptering innebär att skydda sekretessen av privata kommunikationsmedel genom metoder för att säkerställa integritet av innehåll, autentisering av användare och digitala signaturer [1]. Kryptografi är en central del av datasäkerhet i molntjänster och det finns många olika algoritmer för att konvertera oformaterad text krypterad text. Några krav som alla funktionella algoritmer uppfyller är dock [1]:

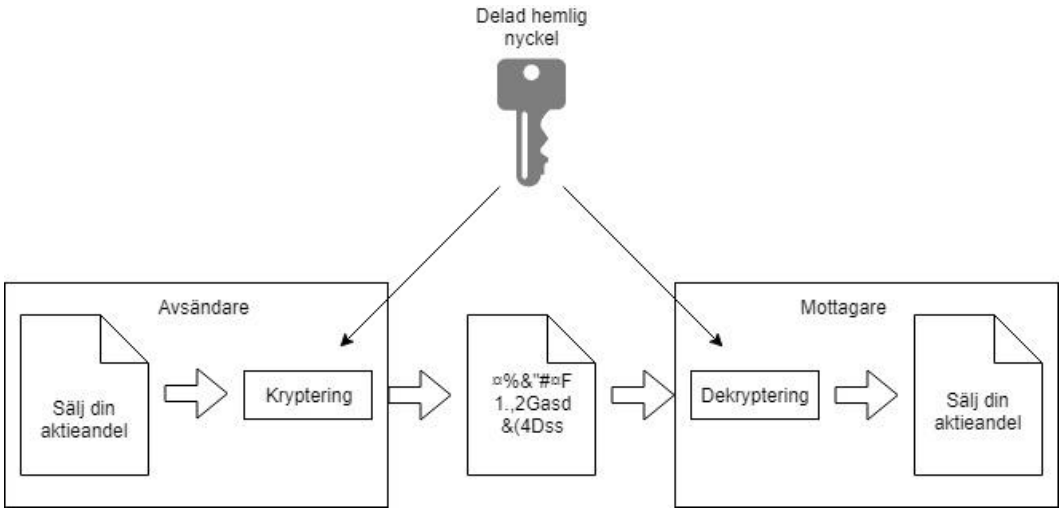
- Algoritmen och implementationen bör beräkningsmässigt vara effektiv, både på kryptering och dekryptering.
- Algoritmen måste vara öppen för analysering av kryptografer och andra.
- Krypterade data måste motstå attacker, även av ett stort antal datorer.

Det finns huvudsakligen två kategorier av kryptografi, symmetrisk och asymmetrisk [1].

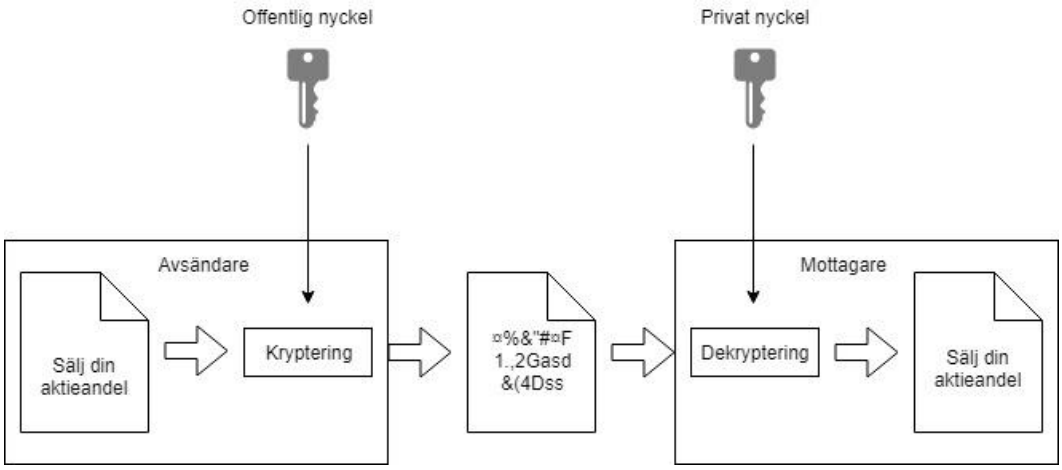
I symmetrisk kryptering (Figur 3) används samma nyckel för både kryptering och dekryptering. Denna egenskap ger en bred användbarhet, men nyckelhanteringen kan bli för komplicerad när symmetrisk kryptering används för kommunikation mellan parter. Om det inte redan existerar ett säkert kommunikationsmedel mellan parterna är det svårt att hålla nyckeln hemlig [1].

I asymmetrisk kryptering (Figur 4) används två olika nycklar. En offentlig nyckel används för kryptering, medan en privat nyckel för dekryptering. Fördelen med detta är att den offentliga nyckeln, som namnet implicerar, inte måste hållas hemlig och den kan delas utan att äventyra säkerheten. En annan fördel med denna metod är att den kan användas till annat än bara kryptering. En privat nyckel kan användas

för att autentisera en användare, den kan även användas för att inleda en säker kanal eller anslutning mellan kommunicerande parter [1].



Figur 3: Symmetrisk kryptering



Figur 4: Asymmetrisk kryptering

3.2.1 Kryptering av data i vila

För att skydda data i vila behövs kryptering. Med data i vila menas all lagrade data, t.ex. ett företags filer på en server eller säkerhetskopierade versioner av filer som

existerar någonstans utanför företaget [1]. Stark kryptering krävs, eftersom data i vila kan vara lagrat över långa perioder vilket ger utomstående personer god tid att försöka bryta krypteringen.

Några olika former av kryptering av data i vila är [1]:

- Fullständig diskkryptering: Alla applikationer och all data som existerar på en krypterad hårdskiva är krypterade. Detta är inte en bra lösning, eftersom krypteringen sker via operativsystemet och kan därmed ha en negativ inverkan på både prestanda och hållbarhet.
- Filsystem: I denna metod krypteras och dekrypteras data-kataloger.
- Individuella filer: Filer krypteras enskilt, istället för en hel hårdskiva eller katalog.
- Kryptering via en applikation: En applikation hanterar kryptering och dekryptering av all data som går genom applikationen.

Oberoende av vilka former av kryptering som implementeras är det kritiskt att upprätthålla ett väl-fungerande system för nyckelhantering, d.v.s. utbyte, lagring och användning av krypteringsnycklar [1].

3.2.2 Kryptering av data i rörelse

Data i rörelse omfattar all data som är i ett tillstånd av förflyttning från en lagringsplats till en annan, vilket sker när någon t.ex. laddar upp data till ett moln [1]. Det omfattar även data som inte sparas permanent någonstans, t.ex. an användares användarnamn och lösenord på en webbsida. En risk vad gäller data i rörelse är att en tredje part kan ha tillgång till data medan den är i rörelse från ett tillstånd till ett annat.

Den vanligaste metoden för att säkra data i rörelse är kryptering i kombination med autentisering [1]. Kryptering används för att försäkra att all data hålls hemlig ifall det sker ett informationsläckage mellan två parter, medan autentisering används för att försäkra att kommunicerande parter verkligen är vem de säger att de är.

4. Diskussion

När jag först började läsa om molntjänster visste jag inte direkt hur omfattande begreppet var. Min uppfattning var att det handlade mestadels om uthyrning av lagringskapacitet, som t.ex. Dropbox, men det visade sig att begreppet innebär mycket mer än det.

Baserat på de mångsidiga och kostnadseffektiva egenskaperna molntjänster har tror jag definitivt att användningen av dem kommer att fortsätta öka, speciellt inom företag. Möjligheten att skära ner ägandekostnaderna för it-infrastruktur genom att använda molntjänster är en av de största orsakerna till att allt fler företag skiftar till molnbaserade lösningar. Populariteten av hybrida molntjänster kommer troligtvis att ytterligare öka, eftersom den formen av molnuppbyggnad tillåter kunden att dra nytta av både offentliga- och privata moln.

Av de hot inom datasäkerhet som behandlats i avhandlingen är de största hoten enligt mig överbelastningsattacker och dataförlust. Molntjänstleverantörer tar risker i beaktan, men dessa två hot kan vara de svåraste att skydda sig mot. Det är näst intill omöjligt att helt och hållet eliminera alla svagheter i ett datasystem, och eftersom molntjänster ännu är relativt nya kommer troligen nya svagheter att upptäckas och utnyttjas. Dataförlust tror jag att kommer vara ett fortskridande problem, eftersom det kan ske på grund av den mänskliga faktorn. En person kan orsaka dataförlust i misstag eller på flit, men i båda fallen är det svårt att förhindra. Dataförlust kan ytterligare orsakas av externa faktorer, exempelvis naturkatastrofer eller katastrofala bränder, vilka inte går att förhindra.

Litteraturförteckning

[1] Winkler, V., (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*.

[2] IDG Enterprise, (2016). *Cloud Computing Survey*

Källa: http://core0.staticworld.net/assets/2016/11/03/cloud_exec_summ_2016.pdf [Hämtad 15.02.2018]

[3] Bernheim, L. (2017) *IaaS vs. PaaS vs. SaaS Cloud Models (Differences & Examples)*

Källa: http://www.hostinga0dvice.com/how-to/iaas-vs-paas-vs-saas/ [Hämtad 15.02.2018]

[4] *"Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review"* http://www.mecs-press.net/ijcnis/ijcnis-v6-n3/IJCNIS-V6-N3-3.pdf

[5] *"The NIST Definition of Cloud Computing"* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[6] *https://www.infinera.com/top-five-cloud-migration-challenges-enterprises-solve/*

[7] http://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises&oldid=305208

[8] SPOF: https://www.ijsr.net/archive/v3i4/MDIwMTMxNDY1.pdf

[9] https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/introduktion-till-dataskyddsforordningen/dataskyddsforordningens-syfte/

[10] Datasäkerhet: https://thesai.org/Downloads/Volume7No4/Paper_64-Data_Security_Privacy_Availability_and_Integrity.pdf

[11] DOS: https://rickscloud.com/how-to-counter-ddos-attacks-in-cloud-computing/

[12] Kryptering: http://www.iraj.in/journal/journal_file/journal_pdf/4-204-1452580599110-115.pdf

[13] Kryptering: http://apprize.info/security/cryptography/7.html

[14] Historia: http://www.dataversity.net/brief-history-cloud-computing/

[15] Cloud vs. On-premise: https://www.softwareadvice.com/buyerview/deployment-preference-report-2014/