Examensarbete

HÖGSKOLAN I SKÖVDE

FÖRTROENDE OCH SÄKERHET I PUBLIKA MOLN

En undersökning av molnkonsumentens förtroende till molnleverantören

TRUST AND SECURITY IN PUBLIC CLOUDS

A survey of cloud consumers trust in the cloud provider

Examensarbete inom huvudområdet informationsteknologi
Grundnivå nivå 30 Högskolepoäng
Vårtermin 2022

Oscar Bergström

Handledare: Christian Lennerholt
Examinator: Mikael Berndtsson

Sammanfattning

Molntjänster i olika former har fått en allt större roll för IT-drift inom många organisationer. Framförallt grundat i det faktum att molnteknik bidrar till förbättrad drift genom tillgång till ökad skalningsförmåga, vilket möjliggör att organisationer på ett flexibelt sätt kan hantera snabba förändringar vid inkommande arbetsbelastning. Att implementera egen lokal IT kräver även en hög kapacitet och stark resurstillgång, faktorer som inte alltid finns till hands. Beskrivna anledningar tillsammans med effekterna av Covid-19 pandemin har gjort att implementering och bruk av molntjänster ökat.

Fördelarna kommer dock inte utan nackdelar, molntjänster erbjuds ofta via molnleverantörer, vilket i sig inte behöver innebära en riskfaktor. Molntjänsternas struktur går däremot att koppla till en uppsjö av relaterade säkerhetsrisker, vilka till största del måste hanteras av leverantören. Konsumenten blir således beroende av att leverantören bibehåller säkerheten i molnet, ett stort förtroende placeras därmed till en extern aktör. Detta arbete fokuserar därför på att analysera hur konsumenten upplever förtroendet till leverantörens förmåga att bibehålla säkerheten relaterat till de säkerhetsrisker som kunnat kopplas till molntjänster. För att undersöka konsumentens upplevda förtroende till leverantören har en fallstudie med intervjuer som datainsamlingsmetod genomförts, fokus låg på att undersöka individer verksamma inom IT-branschen relaterat till molnfrågor.

Resultat visade på att förtroendet till leverantören i generell bemärkelse är högt, konsumenten litar på leverantörens förmåga att skydda tjänsterna mot intrång och bibehålla tillgängligheten. Vanligen rör det sig om stora välkända aktörer, konsumenten upplevde att detta talade för kapacitet och därmed en säkrare tjänst. Komplikationer uppkommer snarare kring juridiska aspekter och vem som äger tillgång till data, i detta anseende ansågs leverantörerna som mindre förtroendeingivande.

Nyckelord: *Cloud Computing, Cloud, Consumer trust, Trust, Information security, Data security och Service providers.*

INNEHÅLLSFÖRTECKNING

1 Inledning

Molntjänster har blivit en allt viktigare komponent för att bidra till att möjliggöra organisationers IT-lösningar (Kelly, Pitropakis, Mylonas, McKeown & Buchanan 2021). Molnbaserad IT bidrar till flexibilitet och ökad skalningsförmåga, vilket kan konstateras vara mycket fördelaktiga egenskaper (Tabrizchi & Kuchaki 2020). Skalningsförmågan innebär möjligheten att tillföra systemresurser till IT efter behov baserat på inkommande arbetsbelastning (Yan, Hao, Cheng & Zhou 2018). Molnbaserade lösningar kan därför ofta ses som ett flexibelt och kostnadseffektivt alternativ. Trots konstaterade fördelar, uppkommer även en mängd frågor kopplade till säkerhetsarbetet och risker direkt relaterat till molnet (Tabrizchi & Kuchaki 2020).

Molnleverantörer tillhandahåller olika typer av tjänstemodeller baserade i molnet, vilka är riktade till konsumenter (Yan et al. 2018). Dessa benämns vanligen efter tre kategorier: Iaas, Paas eller SaaS och representerar olika nivåer i molnet (Ziani & Medouri 2018). Reglering av konsumerad tjänst styrs via ett leveransavtal eller SLA, där dikteras relationen mellan konsument, leverantör och vilka åtagande respektive part innehaver (Subramanian & Jeyaraj 2018). Bristande förståelse för hur datalagring i molnet fungerar och hur systemresurser tillförs gör det svårt för konsumenten att försvara sig mot olika angrepp (Tabrizchi & Kuchaki 2020). Molntjänster tillhandahålls vanligtvis via en extern aktör även benämnt som molnleverantör, molnet benämns i dessa fall som ett publikt moln vilket innebär en delad tillgång av molnnätverket givet åt ett flertal olika kunder som gemensamt konsumerar tjänsten (Ziani & Medouri 2018). Molntjänster bidrar således till en delad IT-miljö, även känt som multi-tenant, vilket innebär att flera virtuella maskiner (gäster) delar på resurser tillhandahållet via samma underliggande infrastruktur (Yan et al. 2018; Ziani & Medouri 2018). Multi-tenancy är en viktig komponent i molnet men också en främjande orsak till olika typer av säkerhetsrisker (Yan et al. 2018). För att bibehålla säkerhet i molnet krävs ett konstant arbete, så som ett rigoröst uppdaterande av system och tillskaffande av aktuella kunskaper kring olika typer av säkerhetshot (Kelly et al. 2021).

Utöver de redan befintliga fördelarna som kunnat konstateras locka till etablering av IT i molnet, har covid-19 pandemin ytterligare bidragit till att accelerera implementation av molnbaserade tjänster. Pandemins indirekta konsekvenser på hur människor arbetar har påverkat hur molntjänster används och accelererat bruket av olika tjänstemodeller, så som olika typer av kommunikationsmedel, vilka ofta är baserade i molnet (Alashhab, Anbar, Singh, Leau, Al-Sai & Alhayja'a 2021). Molntjänsternas implementation har som ett resultat förändrat vårt koncept för bruk och ägande av data, förändringens effekter kan ha en bidragande påverkan på konsumentens förtroende till molnleverantören (Van der Werff, Fox, Masevic, Emeakaroha, Morrison & Lynn 2019). Förtroende är en viktig faktor för de affärsmässiga relationerna mellan parterna. Studien syftar således till att undersöka molnkonsumenternas upplevda förtroende till molnleverantörernas förmåga att bibehålla säkerheten i molntjänsterna (Tabrizchi & Kuchaki 2020).

2 Bakgrundskapitel

Kapitlet beskriver den vetenskapliga bakgrunden till ämnet, begrepp, olika definitioner konkretiseras och förtydligas i kontrast till det specifika området som ämnet handlar om. Inom ramen för detta arbete faller fokus således på molntjänster, informationssäkerhet, definition av begreppet förtroende och olika typer av relaterade aspekter.

2.1 Molntjänster

Molntjänster eller molnet, bidrar till förmågan att hämta och transfereras data mellan olika servrar, som kan bygga på flertalet olika lokaliseringar, vilket innebär att molnet kan ha ett flertal geografiska områden som utgångspunkter. Data i molnet kan därför beskrivas vara flyktig i sin natur, uttryckligen grundat efter hur molndata har förmågan att transferera mellan olika platser (Kelly et al. 2020). Molnbaserade tjänster existerar således inte lokalt, utan bygger på externlösningar ofta utanför de lokala brandväggarna (Fisher 2018). Molntjänster skulle därför kunna jämföras rent funktionellt med ett nätverk, som vid behov kan ge tillgång till en uppsjö av IT-resurser (Yan et al. 2018). Molnet bidrar därmed till att IT tilldelas ökade egenskaper så som skalningsförmåga, vilket innebär, tillförseelse av resurser i korrelation till organisationens behov. Molnet kan som ett resultat bidra till att underlätta vid hanteringen av stor mängd data och arbetsbelastning (Kelly et al. 2020; Tabrizchi & Kuchaki 2020; Yan et al. 2018). Molntjänster bidrar således till att skapa en miljö där tillkopplad IT delar på systemresurser via samma molnnätverk, vilket kan beskrivas som en delad IT-miljö (Multi-tenant). Molntjänster möjliggör därför till virtualisering, vilket är en teknologisk komponent som kan användas i molnet och innebär möjligheter för flera virtuella maskiner eller applikationer att tillhandahålla resurser via en och samma underliggande infrastruktur (Yan et al. 2018; Ziani & Medouri 2018). Molntjänster kan som ett resultat av dess många fördelar konstaterats ha blivit en effektiv och sparsam miljö där en organisation kan etablera sina IT-lösningar (Kelly et al. 2020; Yan et al. 2018).

Molntjänsterna brukar kategoriseras efter tre olika typer av tjänstemodeller (Yan et al. 2018). De olika kategorierna är: *infrastrucure as a service* (IaaS), *platform as a service* (PaaS) eller *system as a Service* (SaaS) (Kelly et al. 2020; Yan et al. 2018). IaaS ger konsumenten tillgång till den underliggande infrastruktur som molnet bygger på, så som, lagringskapacitet och systemresurser (Yan et al. 2018; Ziani & Medouri 2018). Det är viktigt att poängtera att IaaS dock inte ger konsumenten den fysiska kontrollen över själva hårdvaran. Utan konsumenten tillhandahåller tjänsten via diverse styrmedel så som olika operativa system. Systemen som erbjuds i denna tjänstemodell är således indirekt skapade för att kunna hantera den underliggande infrastrukturen (Ziani & Medouri 2018). PaaS erbjuder användaren tillgång till en plattform baserad i molnet, vilket oavsett underliggande infrastruktur, så som servrar och olika operativsystem ger användaren förmågan att kontrollera och distribuera olika typer av applikationer på den erbjudna plattformen (Yan et al. 2018). Skillnaden mellan tjänstemodellerna PaaS och IaaS definieras i att PaaS inte tillåter konsumenten att hantera den underliggande infrastrukturen. Utan molnet brukas med hjälp av plattformen, som tillhandahålls via

leverantören, vilket istället körs på infrastrukturen (Ziani & Medouri 2018). SaaS innebär att en applikation distribueras och körs direkt via molnet, vilket betyder att applikationen inte behöver installeras lokalt. Tillgänglighet till SaaS applikationer tillhandahålls via olika typer av gränssnitt, ett exempel kan vara via en webbläsare (Yan et al. 2018). Leverantören av molntjänsten erbjuder SaaS lösningen direkt till konsumenten, som därför inte behöver hantera några specifika delar i molnet, till exempel, infrastruktur, operativa system eller datalagring (Ziani & Medouri 2018).

Molnnätverk kan kategoriseras som publikt eller privat vilket avgörs beroende på om molnlösningen använder sig av ett företags externa eller interna infrastruktur (Kelly et al. 2020). Publika moln tillhandahålls oftast via leverantörer som konstruerat och underhåller IT-infrastrukturen och via denna erbjuder olika molnbaserade tjänster till konsumenterna. Publika moln nyttjas som ett resultat gemensamt av alla användare som betalar för tillgången till tjänsten, därmed delas IT-miljön mellan flertalet aktörer. Privata moln har till skillnad från publika moln bara en aktör som äger rätten att bruka tjänsten, inga externa aktörer finns med i bilden. Molnet konstrueras i dessa fall antingen av ett företags IT-avdelning eller i kontrakt med en leverantör. Privata moln ger den brukande aktören genom resultatet av sitt ägande fullständig kontroll över data och arbetet med säkerhet (Ziani & Medouri 2018). Denna studie lägger fokus på molntjänster erbjudna via externa aktörer, fokus är därmed placerat på det som benämnts som publika molnet.

Publika moln erbjuds oftast via molnleverantörer, vilka kan beskrivas som aktörer som erbjuder olika typer av molnbaserade tjänstemodeller för konsumtion. Tjänster som tidigare har diskuterats, vilka oftast är: IaaS, PaaS eller SaaS (Tabrizchi & Kuchaki 2020). Molntjänster som erbjuds av en leverantör kan bidra till att den brukande konsumenten blir beroende av leverantören, i den mån att leverantören oftast står för hanteringen av IT-infrastrukturen. En stor del av säkerhetsarbetet tillfaller därför till den levererande parten av tjänstemodellen. Ett exempel på detta skulle kunna vara vid ett tillfälle då molntjänsten blir utsatt för ett belastningsangrepp, vilket skapar en situation då konsumenten behöver förlita sig på leverantörens säkerhetsförmåga för bibehållen tillgänglighet av konsumerad tjänst (Coppolino, D'Antonia, Mazzeo & Romano 2017). Molnkonsumenten definieras i denna studie som den brukande parten av en tillhandahållen molntjänst erbjuden av en molnleverantör. En molnkonsument kan vara en individ, ett företag eller en organisation. Denna studie fokuserar på molnkonsument i den mån av ett företag eller en organisation. Fokus ligger därmed på att undersöka upplevelserna ur molnkonsumentens perspektiv gentemot molnleverantören (Tabrizchi & Kuchaki 2020).

Molntjänster erbjuds oftast genom ett leveransavtal, ett så kallat *service-level-agreement*, även känt som ett SLA. Specifikationer och krav för den levererade tjänsten dikteras genom SLA, där styrs relationen mellan molnkonsumenten och molnleverantören (Tabrizchi & Kuchaki 2020; Subramanian & Jeyaraj 2018). Innehållet i ett SLA kan styra olika krav så som exempelvis prestanda, tillgänglighet och säkerhet för den brukade molntjänsten (Tabrizchi & Kuchaki 2020; Subramanian & Jeyaraj 2018). Leverantören ska

erbjuda molntjänsten till konsumenten efter de krav som dikterats i SLA, vilket dock inte betyder per automatik, att tjänsten är säker eller effektiv. Ett SLA beskriver de situationer då leverantören har ett ansvar och även därmed vid vilka tillfällen leverantören inte bär ansvaret. Därför kan ett SLA bidra till situationer då en leverantör kan avsäga sig skyldigheten för eventuell uppkommen problematik (Tabrizchi & Kuchaki 2020).

2.2 Lokal IT eller etablera IT i molnet

Företag som använder molnbaserade lösningar brukar sin IT utanför de egna brandväggarna, till skillnad från användande av lokalt baserad IT (Fisher 2018). IT som baseras lokalt innebär att den fysiska kontrollen oftast innehas av konstruktören, vilket vanligen är företaget eller organisationen som besitter ägandet över själva infrastrukturen (Winkler & Brown 2013). Att implementera en lokal IT-lösning kan i en del sammanhang fungera bättre än att vända sig till en molnleverantör, vilket hade inneburit att IT-lösningar istället baserats i form av olika molntjänster. För att möjliggöra till en lokal IT-lösning bör dock ett företag se till att säkerställa möjligheten att tillhandahålla en god IT-kapacitet, strategi och god förmåga att leverera resultat för att lyckas vid implementering. I de sammanhang då dessa faktorer finns tillgängliga kan en lokalt baserad IT-lösning leda till möjligheter att bespara en organisation kostnader. Organisationer som inte besitter denna grad av IT-kompetens, tjänar i de flesta fall mer på att tillförskaffa IT genom en flexibel molnbaserad lösning, vilket oftast genomföras genom kontraktering via en molnleverantör (Fisher 2018).

En av de främsta anledningarna att många organisationer väljer att etablera sin IT i molnet är på grund av kostnadseffektivitet. Organisationer gör ofta antagandet att en övergång till molnbaserad IT kommer leda till reducerade kostnader genom möjliga besparingar på IT-avdelningen, främst genom att kunna reducera personalkostnader (Al-Nassar, Al-Nsour & Rababah 2021). Organisationens antagande, gällande reducering av kostnader stämmer ofta överens med det faktiska resultatet vid implementering. Övergång till molnet kan i många fall resultera i frigörandet av IT-resurser och därmed bespara ett företag onödiga utgifter. Värt att konstatera är att det finns fall då interna IT-lösningar faktiskt kan briljera. En organisation som överväger att etablera sin egen IT kräver dock som tidigare benämnt tillgången till en hög kapacitet, vilket långt i från alla organisationer besitter och är något som därför inte alltid kan förverkligas, då är molntjänster ofta en bättre lösning (Fisher 2018).

2.3 Informationssäkerhet i molnet

Flertalet av de säkerhetsutmaningar som identifierats i molntjänster kan på olika sätt beskrivas ha en indirekt påverkan på tre av aspekterna i CIA triaden: *Confidentiality*, *Integrity* och *Availability* (Tabrizchi & Kuchaki 2020). *Confidentiality*, (sekretess) är förmågan hemlighålla data från obehöriga. *Integrity*, (integritet) handlar om att kunna säkerställa att data inte förändrats utan att den information som faktiskt presenteras är korrekt och inte har modifierats. *Availability*, (tillgänglighet) syftar till förmågan att säkerställa att inte tillgången till system och servrar begränsas (Sherman, DeLatte, Neary,

Oliva, Dhananjay, Scheponik, Herman & Thompson 2018). CIA triaden bör tas i beaktande när säkerhet och molntjänster diskuteras triaden fungerar som en god utgångspunkt för att kategorisera säkerhetsproblematiken (Díaz de León Guillén, Morales-Rocha & Fernández Martínez 2020). Generellt finns ett stort intresse bland konsumenter för att migrera till molntjänster, de som avvaktar med att ta steget väljer ofta att vänta på grund av säkerhetsaspekter och integritetsfrågor (Wagemann, Siemen, Seeger & Bendix 2021).

En av faktorerna som berör olika typer av säkerhetsaspekter är specifikationer i SLA som tecknats mellan molnleverantören och molnkonsumenten. Ett SLA förtydligar hur de olika parterna ska arbeta för att bibehålla säkerhet och även inom vilka områden respektive part är ansvarig. Specifika områden som bör uppmärksammas i SLA är bandbredd, driftstörningar och geografisk plats för datalagring. Vilka beroende på tillfället samtliga är faktorer som skulle kunna påverka tillgängligheten och integriteten av den data som brukas i molntjänsten (Subramanian & Jeyaraj 2018). Noterbart är att ett SLA endast beskriver specifikt vad den levererade molntjänsten ska innehålla och därför inte bör tolkas som en faktisk garanti för den levererade tjänstens kvalité. Molnleverantören klarar inte att i alla sammanhang upprätthålla det faktorer som garanterats i ett SLA. Därför är det viktigt att poängtera att ett SLA inte skyddar mot ett dåligt val som resulterar i leverans av en dålig tjänst (Tabrizchi & Kuchaki 2020). Ett SLA bör därför ses som ett avtal som ger en juridisk garanti mellan molnkonsumenten och molnleverantören. Vilket bidrar till att diktera och specificera respektive parts åtaganden. Därmed ger ett SLA avtalsenliga garantier för vilka olika typer av krav tjänsten måste innehålla, vilket indirekt skulle kunna påverka olika säkerhetsaspekter (Carvalho, Andrade, Castro, Coutinho, & Agoulmine 2017).

Säkerhetsrisker kan även uppkomma som ett resultat av delad IT-miljö, även känt som multi-tenancy. Infrastrukturen som molnet bygger på brukas mellan flera användare vilket kan ha en påverkan på säkerheten. Delad IT-miljö är ur många perspektiv fördelaktig och bidrar till möjligheter för funktionalitet så som skalning och delning av systemresurser, vilket kan ses som en viktig kompentent i molnet. Genom delad infrastruktur möjliggörs att flertalet virtuella maskiner får tillgång till systemresurser och kan köras parallellt (Yan et al. 2018; Ziani & Medouri 2018). Molntjänster kan därför genom denna metod bidra till att lösa problematik som uppkommer vid brist på tillgång av resurser vid en hög arbetsbelastning. Vilket i molntjänsten då kan justeras genom förmågan att distribuera resurser och datakraft efter behov, parallellt mellan flertalet olika användare (Tabrizchi & Kuchaki 2020). Förmågan till en delad IT-miljö, utöver att vara en viktig komponent, blir även genom sin funktionalitet också ett av molnet svagheter ur ett säkerhetsperspektiv. Utöver att möjliggöra för virtuella maskiner att samexistera på samma underliggande infrastruktur bidrar tekniken till en rad olika säkerhetsrisker (Yan et al. 2018). Delad resurstillgång kan användas i syfte att angripa andra virtuella maskiner som existerar inom ramen av samma infrastruktur. Vilket resulterar i att en delad IT-miljö bör ses som både en styrka och svaghet i molnet (Coppolino et al. 2017). Resultatet blir att de virtuella maskinerna grundat i den faktor att de delar på samma IT infrastruktur, kan användas för att angripa underliggande

kommunikationslänkar i molnet (Subramanian & Jeyaraj 2018). Vilket leder till att en angripare kan komma över andra isolerade delar i molnet genom att nyttja att de virtuella maskinerna hämtar sin datakraft från samma källa (Yan et al. 2018).

Ännu ett säkerhetsperspektiv som bör diskuteras, är graden av den påverkan som molnleverantören har på säkerheten. Främst i den mån att leverantören indirekt är i kontroll över hur data rent funktionellt lagras och hanteras. Molnleverantören blir därför den part som står för den faktiska kontrollen över bruk av underliggande infrastruktur, så som själva hårdvaran. Molnkonsumenten måste exempelvis, till en viss grad, förlita sig på att molnleverantören kan bemöta angrepp för att bevara tillgänglighet av konsumerad tjänst (Coppolino et al. 2017). Data som baseras i molnet kan ofta förflyttas och speglas mellan flertalet olika platser. Servrar med koppling till molnet kan vara baserade via flertalet olika geografiska lokaliseringar som sina utgångspunkter (Kelly et al. 2020). Kombinationen av de två benämnda faktorerna leder till att konsumenten tilldelas en bristande förmåga till kontroll över datalagring och drift, vilket kan leda till en rad olika typer av säkerhetsrisker (Yan et al. 2020). Så som kontostöld, bristande tillgänglighet på grund av överbelastningsattacker och minskad förmåga att skydda sig mot elaksinnade individer på grund av att driften är externt. Exempelvis en anställd som får tillgång till data utan egentligt tillstånd, alltså en obehörig användare. Skyddsförmågan mot säkerhetsriskerna tillfaller till stor del molnleverantören. Resultatet blir att molnkonsumenten får brist på kontroll över flera säkerhetsaspekter som tillförs till molnleverantören. Fenomenet är en av de större nackdelarna med molnbaserade tjänster och även en av de största och mest betydande säkerhetsriskerna vid konsumtion av molntjänst (Coppolino et al. 2017). Organisationer måste också ta i beaktande vart data lagras, EU domar som Schrems II har en ytterligare påverkan på denna aspekt och hur data får överlämnas till tredje part. Geografiska aspekter har därmed fått en betydligt större påverkan och ställer höga krav på att data säkras upp och inte felaktigt hamnar i händerna på exempelvis externa aktörer som inte kan säkerställa att EU medborgares datasekretess bibehålls enligt GDPR, eller rimlig nivå (Tracol 2020; Rotenberg 2020).

2.4 Förtroende och molntjänster

Säkerhet är en faktor som användare i molntjänster tar i beaktande när ett SLA ska tecknas mellan molnkonsumenten och molnleverantören, transparens är viktigt i detta avseende för att bygga förtroende mellan parterna (Carvalho et al. 2017). Förtroendet är en affärsmässig viktig faktor, brist på förtroende kan skapa många utmaningar för molnbaserade tjänster och dess leverantörer (Tabrizchi & Kuchaki 2020). Molnkonsumentens förtroende viktigt av den anledning, att konsumenten troligen kommer bearbeta och ta i beaktande de förtroendepåverkande faktorerna i sitt beslut vid val av molnleverantör (Yan et al. 2018).

Organisationer har ofta kunnat konstateras vara oroliga över hur deras data hanteras vid extern lagring lokaliserat hos ett annat företag (Tabrizchi & Kuchaki 2020). Ägaren av data räds alltså den egna förlusten av kontroll över datahanteringen, som istället tillförs till molnleverantören (Díaz de León Guillén et al. 2020). För att molnkonsumenten ska

känna förtoende till en leverantör och dess tjänst, måste molnkonsumenten kunna acceptera, ha förståelse, medvetenhet om både företaget och tjänstens eventuella brister. Molnbaserade tjänster har förändrat uppfattningen och synen på användarens rättigheter, vem som äger data och uppfattningen kring online baserade miljöer (Van der Werff et al. 2019). Valet av leverantör kan därför vara svårt, ofta erbjuder leverantörerna snarlika tjänster, konsumenten kan därför finna en utmaning i att välja rätt leverantör för att tillfredsställa funktionalitet och rätt krav (Muralidharan & Anitha 2021). Utifrån de förändrade förutsättningarna och riskerna som påtagligen bevisats existerar i molnbaserade miljöer, definieras förtroende i denna studie i mån av molnkonsumentens uppfattning av förtroendet till molnleverantören i relation till dess förmåga att erbjuda en trygg säkerhetslösning (Tabrizchi & Kuchaki 2020; Yan et al. 2018).

3 Problemområde

Kapitlet beskriver arbetets problemformulering, vilket mynnar ut i ett syfte och frågeställning, därefter beskrivs avgränsningar och hypotetiska antaganden.

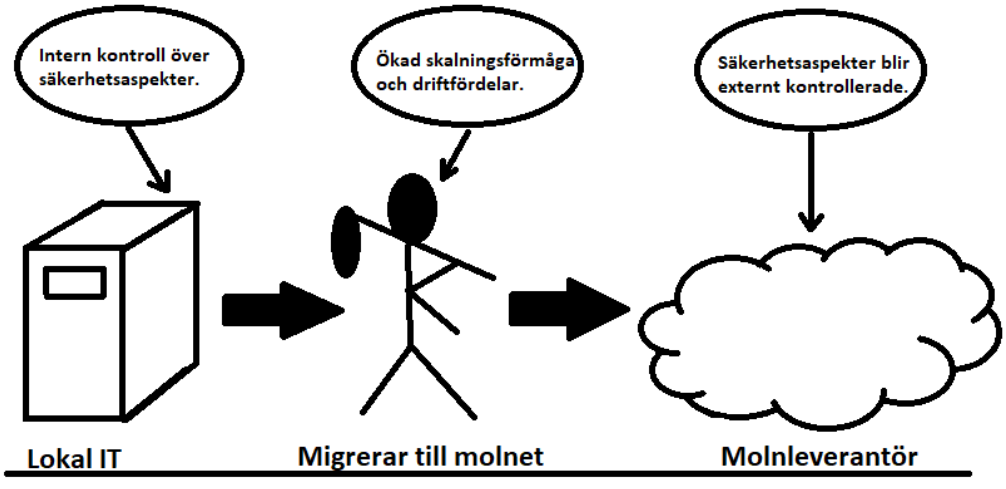
3.1 Problemformulering

Molntjänster har fått en större roll för IT-driften inom många organisationer (Kelly et al. 2021). Lokala IT lösningar som bygger på eget intranät är fortfarande ett väl fungerande alternativ om organisationen har en god intern IT-kapacitet. Molntjänster ger dock förmåga till en hög grad av flexibilitet, vilket möjliggör frigörandet av IT-resurser som kan läggas på annat än att implementera lokal IT (Fisher 2018). IT etablerad i molnet ger ofta en ökad skalningsförmåga, alltså egenskapen att kunna tillföra dataresurser till systemet efter organisationens behov (Tabrizchi & Kuchaki 2020). Därför kan molntjänster bidra till ökad tillgänglighet och möjlighet till bättre prestanda, data kan enkelt delas mellan olika användare som ges förmåga att skapa kopior av data oberoende plats, så länge den dator som brukas har tillgång till molnet (Yan et al. 2018). Molnbaserade lösningar blir således ofta ett kostnadseffektivt alternativ till att implementera egen IT, vilket även som ett resultat medför en hög grad av flexibilitet. Molntjänsters allt vanligare förekomst väcker dock ett antal frågor gällande säkerhet i samband med att IT succesivt flyttas och etableras i molnet. Säkerhetsrisker i molnet har på olika sätt effekt på alla tre aspekter inom CIA triaden. Molntjänster skapar en osäker IT-miljö byggd på multi-tenancy, att miljön delas är en risk som påverkar integritet och sekretess. Molnkonsumenten har en begränsad kontroll och tillgång över den underliggande infrastrukturen, vilket konsekvent skulle kunna resultera i en bidragande faktor som gör att molntjänster kan påverka tillgänglighet till ett system negativt (Tabrizchi & Kuchaki 2020).

Kelly et al. (2020) kartlagde frekvensen för olika typer av angrepp mot molnbaserade tjänster genom en undersökning riktad mot några av de större molnleverantörerna på marknaden. Resultatet visade på en frekvens av cirka 55 000 registrerade angrepp per dag. Molnkonsumenterna kan inte helt lägga sitt förtroende till att leverantören av tjänsten ska stå för säkerheten och äger därmed själva en del av ansvaret. Många av molntjänsterna som utsattes för angrepp i undersökningen hade kända säkerhetsluckor, vilka inte var nytillkomna, utan hade förekommit under en längre tid. Vissa av de identifierade säkerhetsluckorna hade existerat sedan år 2001. Säkerhetsluckornas primära förekomst identifierades hos IP-telefoni och skrivbordsdelning. IT-tjänster som också brukades i en högre utsträckning i samband med Covid-19 pandemins effekter.

Molntjänster kan således konstateras dras med säkerhet och angreppsproblematik vilket öppnar för frågor kring informationssäkerhet, det ökade bruket av molntjänster står som ett resultat inför många utmaningar relaterade till en rad olika säkerhetsaspekter (Kelly et al. 2020; Tabrizchi & Kuchaki 2020; Yan et al. 2018). En av utmaningarna som uppkommer kan relateras till den data som flyttas till molnet. Orsaken är att datalagring sker via molnleverantören som tillhandahåller tjänsten genom ett system av servrar, vilka beroende på situation kan ha utgångspunkt från flera olika geografiska platser. Resultat

blir att molnkonsumenten inte har kontroll över den faktiska lokaliseringen eller hårdvaran vid datalagring (Subramanian & Jeyaraj 2018). Brist på kontroll över hårdvara kombinerat med bristande insikt för hur arbetsbelastning och datalagring hanteras i molnet gör det svårt att bemöta angrepp (Tabrizchi & Kuchaki 2020). Ett annat faktum är att molnet skapar en miljö där dataresurser delas och flera virtuella maskiner och applikationer körs parallellt, en delad IT-miljö (Multi-tenant), grundat i samma infrastruktur, resultatet blir en potential för olika säkerhetsrisker (Yan et al. 2018; Ziani & Medouri 2018). Virtuella maskiner kan till exempel användas i en delad IT miljö för att angripa andra virtuella maskiner som körs parallellt (Subramanian & Jeyaraj 2018). Beroende på situation, har molnkonsumenten och molnleverantören även olika ansvarsområden för att bibehålla säkerhet (Yan et al. 2018). Molntjänsten erbjuds till molnkonsumenten via ett SLA, där regleras vad som ingår i tjänsten och vilket ansvar molnleverantören innehar till konsument (Tabrizchi & Kuchaki 2020; Subramanian & Jeyaraj 2018). En av utmaningarna med molntjänster kan därför relateras direkt till SLA där många av specifikationer för tjänsten dikteras. Inom ramen för ett SLA regleras tjänstemodellen, där specificeras alla leverantörens skyldigheter till kund och även vilket ansvar som leverantören har för att bibehålla integriteten, tillgänglighet och prestanda (Subramanian & Jeyaraj 2018). Ett SLA förhindrar dock inte risken att molntjänsten levereras på ett felaktigt sätt och kan därför inte ses som en garanti för en säker systemlösning (Tabrizchi & Kuchaki 2020). Under början av pandemiutbrottet kopplat till Covid-19 kunde en ökad förekomst av angrepp riktade mot olika typer av molntjänster identifieras. Anledning tros vara att tjänsternas relevans ökade i korrelation med olika åtgärder vidtagna för att hantera pandemin (Kelly et al. 2020). Covid-19 pandemin kan ha förändrat hur människor arbetar, vilket resulterat i ett ökat behov och ett påskyndande av införandet tjänstemodeller baserade på SaaS och PaaS, ofta i form av olika typer av kommunikationsmedel som konstruerats i molnet (Alashhab et al. 2021).



Figur 1: Lokal IT till publika molnet.

Figur 1 sammanfattar illustrativt det övergripande sambandet som diskuterats i kapitlet, IT flyttas och etableras i molnlösningar främst på grund av diverse fördelar som förenklar

organisationers IT-drift. Resultatet blir uppkomsten av olika typer av säkerhetsrisker som ofta direkt kan kopplas till molntjänsten. Molnkonsumenten får därmed en minskad kontroll över säkerhetsaspekter relaterade till molnet och ett stort förtroende placeras som resultat till molnleverantören (Tabrizchi & Kuchaki 2020; Subramanian & Jeyaraj 2018). Molntjänsternas allt större relevans och operativa vikt inom många organisationer har lett till uppkomsten av en ökad hotbild mot denna typ av tjänster (Kelly et al. 2020). Vilket sammantaget pekar på relevansen att undersöka förtroendet och relationen mellan molnkonsument och molnleverantör. Förtroende är en viktig kompentent i en affärsrelation, många organisationer oroas över hur sin data hanteras av andra företag. Molnkonsumentens brist på kontroll, förståelse och hur konsumentdata hanteras kan leda till utmaningar på denna front (Tabrizchi & Kuchaki 2020). Konsumentens uppfattning kring leverantörens pålitlighet, säkerhetslösningar och kvalité kommer troligen vara avgörande faktorer när konsumenten väljer vilken molnleverantör som ska få leverera den efterfrågade lösningen (Yan et al. 2018).

Syftet med studien är således att undersöka hur de diskuterade säkerhetsriskerna, som vanligen kan relateras till publika molntjänster, påverkar molnkonsumetens förtroende till molnleverantören. Konsumenten representeras i denna studie av individer aktiva inom IT-branschen, fokus är därför placerat på de som troligen antas indirekt jobba med denna typ av frågor. Tidigare forskning pekar på svårigheter att som konsument hitta rätt molnleverantör för att ge förtroendet att leverera och säkerställa organisationens behov (Muralidharan & Anitha 2021). Denna studie bygger därför vidare på ämnet och undersöker molnkonsumentens upplevelda förtroende till molnleverantören när molnresan redan är etablerad, därmed lyder studiens forskningsfråga enligt följande:

Hur upplever molnkonsumenterna förtroendet till molnleverantören att bibehålla säkerheten i molnet?

3.2 Avgränsningar

Denna studie avgränsas till att undersöka molnkonsumentens förtroende till molnleverantören. Undersökning av konsumentens uppfattning kring leverantören avgränsas ytterligare genom att fokusera på säkerhetsrisker och därmed konsumentens uppfattning av leverantörens förmåga att värja sig mot angrepp och säkra kvalitén av den levererade tjänsten. Konsumentens roll har i denna studie avgränsats till att fokusera på erfarenheter från IT-avdelningar hos företag eller organisation.

3.3 Förväntat resultat

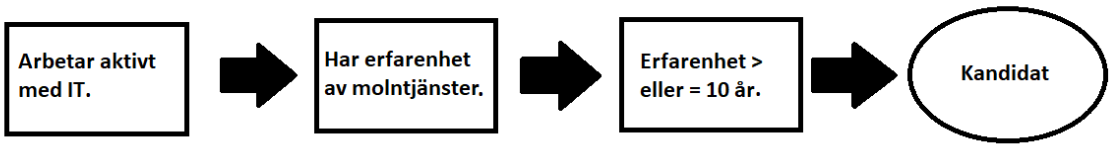
Hypotetiska antagandet är att arbetet kan bidra till insikter gällande uppfattning kring molnleverantörens förmåga att leverera en effektiv och säker tjänst. Därmed skapa en bild för hur konsumenten uppfattar den levererade tjänsten, ifall tjänsten uppfattas som förtroendeingivande och trygg att bruka samt vilka områden det kan råda tveksamheter kring.

4 Metod

Kapitlet beskriver det metodologiska valet för att besvara arbetets frågeställning, varför valet av metod lämpar sig för denna typ av studie och även vilket tillvägagångsätt som användes vid datainsamlingen. Undersökningen utfördes i denna studie genom en fallstudie och valet av datainsamlingsmetodik föll på semistrukturerade intervjuer.

4.1 Fallstudie

Undersökningen i denna studie utfördes genom en fallstudie, valet av metod grundade sig i det faktum att en fallstudie kan utföras via kontakt med människor där de vedertagna observationerna i fallet analyseras ur flera olika aspekter som därefter studeras på djupet (Eriksson & Wiederheim-Paul 2014). Resultatet av metodvalet ledde till djupare insikter kring det inringade området som fokuserats på i denna undersökning.



Figur 2: Urval och kategorisering.

Figur 2 visade hur fallstudien kategoriserades, samtliga kategorier skulle uppfyllas för att en deltagare skulle kvala in i avgränsningen av fallet som studerats. Följande scenarion för deltagande kandidater har därmed varit obligatoriska: *Arbetar aktivt inom IT, har erfarenhet i sitt arbete med molntjänster och en sammantagen tid i branschen på minst tio år eller längre.* Tanken var att deltagare som uppfyllde samtliga kategorier som illustrerats i Figur 2, förhoppningsvis kunde bidra till en tydligare och mer nyanserad bild genom sina gedigna erfarenheter av båda arbeten med lokal och molnbaserad IT. Avgränsning och urvalet av kandidater bidrog därmed till att kategorisera studiens undersökningsområde till ett mer inringat specifikt fall, vilket är av vikt för genomförandet av en fallstudie (Bryman 2018).

I egenskap av denna studie eftersöktes primärt djupgående insikter kring molntjänster kopplat till erfarenheter som talade för hur relaterade säkerhetsrisker påverkade upplevelsen av förtroendet till molnleverantörerna. Metodvalet lämpar sig primärt för att tillföra kvalitativ data, vilket var den typ av data som antogs bäst lämpad för att besvara syftet och forskningsfrågan inom ramen av denna studie (Eriksson & Wiederheim-Paul 2014). Fokus placerades därmed på att identifiera meningar och innebörder av konsumentens uppfattning kring säkerhet och förtroendet i det publika molnet. Förhoppningen var att valet av metod kunde bidra till att besvara hur molnleverantörens förmåga att bibehålla säkerhet påverkade molnkonsumetens förtroende. Genom att dokumentera, undersöka erfarenheter och upplevelser inom ramen av fallstudien kunde förhoppningsvis metodvalet bidra till att bygga större förståelse för fenomenet som undersöktes i denna studie (Alvehus 2019). Metodvalet har därför förhoppningsvis

bidragit till en rättvis och mer djupgående bild och därmed förbättra förståelsen för hur de identifierade säkerhetsriskerna i molnet påverkar förtroendet till molnleverantörens säkerhetsarbete.

I en fallstudie väljs ett undersökningsområde ut, selektering av område kan utföras genom inriktat fokus mot ett specifikt företag eller bransch. Efter val av undersökningsområde, analyseras området på djupet. Inom ramen av denna studie fokuserade studien på branschområde och erfarenheter, se Figur 2 för en tydligare kategorisering. Genom att titta specifikt på observationer inom IT-branschen var förhoppningen att tillföra adekvat kvalitativ data lämpad i förhållande till arbetets frågeställning. Kvantitativ data var fortfarande relevant i sammanhanget och möjliggjorde för en viss beskrivning av undersökningsobjekten i studien, så som år av erfarenhet i branschen. Kvantitativ data kunde alltså oftast kopplas direkt i relation till den observation som undersöktes. Kvantitativ data, kan således hjälpa att beskriva och bygga förståelse för ett specifikt fall. Kvantitativ data som kunde vara relevant för denna studie är sådant som berörde information gällande observationerna, framförallt för att kunna kategorisera dem inom ramen av det undersökta fallet. Så som, information för att beskriva arbetslivserfarenhet, antal år inom yrket. Denna data kunde indirekt kopplas till de individer som deltog i studien och därmed bidra till bättre förståelse i sammanhanget (Eriksson & Wiederheim-Paul 2014).

Sammanfattningsvis, en fallstudie analyserar ett specifikt fall, denna studie avgränsade undersökningsområdet efter bransch, profession och erfarenhet, se Figur 2. Fokus i detta arbete föll således på individer med erfarenhet av mjukvaruutveckling och IT-drift i molnet. Kvantitativ data kommer till viss del att användas, i den mån för att beskriva egenskaperna hos deltagare som kategoriseras inom ramen av det avgränsade fallet (Eriksson & Wiederheim-Paul 2014). Således är förhoppningen att valet av metod primärt kan tillföra kvalitativ data via de medverkande och som ett resultat bidra till djupare insikter och förståelse för hur förtroendet till leverantören påverkas av säkerhetsrisker relaterade till publika molntjänster (Alvehus 2019).

4.2 Datainsamling

Studiens datainsamling utfördes med hjälp av intervjuer där valet av struktur landade på ett semistrukturerat tillvägagångssätt (Alvehus 2019). Tillskaffandet av primärdata i denna studie var således tänkt att samlas in genom att ställa frågor till individer i den specifikt inringade gruppen som kategoriserats inom ramen för fallstudien. För att kunna genomföra denna typ av datainsamling brukar vanligen två olika tekniker lämpa sig, antingen insamlas information via intervjuer eller med hjälp av enkäter. I denna studie föll valet av datainsamlingsmetod på att utföra intervjuer kopplade till de människor som arbetar i den utvalda branschen som fallstudien fokuserar på, anledning är att detta antogs öka chansen att tillförskaffa djupare kunskaper kring ämnet än en enkätstudie (Eriksson & Wiederheim-Paul 2014). Intervjuer insamlar nämligen data via berättelse och erfarenheter från människor, resultatet blir information om hur olika fenomen uppfattas, alltså hur individen tänker, agerar i och kring olika situationer. Tekniken kan

därför vara väl lämpad för att eftersöka upplevelserna kring konsumentens förtroende till leverantören (Alvehus 2019). Upplevelser och erfarenheter är just den typ data som primärt eftersöktes i denna studies syfte.

Intervjuer kan anpassas i val efter hur strukturerat utförandet ska vara, en ostrukturerad intervju kräver ett skickligare utförande men kan däremot leda till djupare insikter kring ämnet. Eftersom denna studie lade fokus på att identifiera upplevelser och erfarenheter från IT-branschen relaterat till molntjänster kunde ett någorlunda ostrukturerat tillvägångsätt lämpa sig vid intervjutillfällena och därmed möjliggöra för en djupare förståelse (Eriksson & Wiederheim-Paul 2014). Trots de eventuella fördelarna med ett ostrukturerat tillvägagångsätt ansågs det inte lämpligt och vägde inte upp för risken att råka sträva ut och tappa fokus från de faktiskt identifierade säkerhetsriskerna som diskuterats. Därför beslutades det att bibehålla en viss grad av struktur vid utförandet och därför föll valet på en semistrukturerad intervjuteknik. Denna typ av struktur möjliggör för en låg grad av kontroll genom ett antal öppna frågor och kan förhoppningsvis bidra till att bibehålla fokus kring området som ska diskuteras. Därför ansågs datainsamling genom semistrukturerade interjuver vara den bäst lämpade datainsamlingsmetod i detta arbete (Alvehus 2019).

4.3 Etiska principer

När det kommer till etiska principer inom forskning så fanns ett antal områden som har varit viktiga att ta i beaktande. Dessa områden berör deltagande individers rättigheter till bevarande av integritet, konfidentialitet, rätt till anonymitet och att deltagande i forskningen måste ske på frivillig basis. I denna studie har de benämnda områdena berörts via valet av metod. För att samla in data i studien användes intervjuer, detta ledde till indirekt kontakt med berörda människor, därför blev det viktigt att ta de etiska perspektiven i beaktande som berörde individer som påverkats vid metodutförandet (Bryman 2018).

Några av de övergripande forskningsetiska principer som varit viktiga att ta hänsyn till är Informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet. Vilka i en sammanfattad beskrivning skulle kunna summeras likt följande: Deltagande individer i forskning har rätt att veta arbetets syfte och ska delta på frivillig basis, det ska även finnas ett samtycke till att delta. Uppgifter gällande deltagare ska bevaras i sekretess så att inte deras anonymitet ofrivilligt röjs eller tilldelas obehöriga. Nyttan av data som tillkommit genom undersökningen ska enbart användas i det arbetets syfte. Enskilda institution har i många fall också etiska riktlinjer, det är därför viktigt att följa de styrdokument som finns tillgängliga på Högskolan i Skövde (Bryman 2018). Enligt ett styrdokument från berörd institution gällande behandling av personuppgifter beskrivs ett examensarbete på grundnivå som exkluderat enligt lag ur processen av etiskprövning av forskning. Däremot lyder fortfarande students arbete under dataskyddförordningen och personuppgifter bör därför hanteras varsamt (Högskolan i Skövde 2020).

Sammanfattningsvis har denna studie följt de benämnda etiska principer som diskuterats samt enligt dataskyddsförordning hanterat data från person på ett varsamt och säkert sätt så att inte obehöriga kunnat äga tillgång. Detta har inneburit att studien utförts enligt följande: Samtliga medverkande intervjudeltagande har givits möjlighet att ge sitt samtycke före och efter en intervju. Transkriberad data har delats med respondenten så att denna fått möjlighet att återkomma med eventuella åsikter om materialet. Insamlade data från respondenter anonymiserades för att bibehålla integritet hos respektive deltagande. För att säkerställa deltagandes rätt till sekretess har även uppgifter som tillhandahålls i utförandets syfte hanteras skyndsamt med främsta anledning att undvika att obehöriga har kunnat äga tillträde till bakgrundsmaterial, så som kontaktuppgifter till berörda individer.

4.4 Genomförande

I denna studie genomfördes sammantaget åtta intervjuer med individer som kunnat placeras inom ramen av fallstudien, dessa hade som gemensam nämnare relation till branschspecifika områden, grad av erfarenhet och arbete relaterat till molntjänster. Att kategorisera kandidaterna underlättade i uppgiften att ringa in korrekt deltagare till det specifika området, därför avgränsades undersökningen via ett antal faktorer vilket bidrar till att skildra studien som ett specifikt fall (Bryman 2018). Det genomsnittligt intervjuutförande landade avrundat, till cirka 40 minuter och samtliga deltagare informerades om de etiska principerna som vidtogs i denna studie, se tdigiare kapitel 4.3 för ytterligare information. Under utförandet spelades intervjuerna in och resulterande ljudmaterial har transkriberats för underlättande vid analyssyfte. Inspelning och transkribering är ett säkert alternativ för att bibehålla en god kvalité av datamaterialet från intervjuer (Alvehus 2019). Slutligen har samtliga deltagare har också erbjudits chansen att granska sitt transkriberade material.

Tabell 1: Deltagare.

Deltagare:	**Arbetsområden:**	**Erfarenhet(år):**
R1.	IT-konsult, Projektledare, Molnutveckling, Utvecklare.	24
R2.	Chef, Webbutvecklare, Molndelar, Produktutvecklare.	20
R3.	Utvecklare, Digitaliseringschef, IT-Chef.	26
R4.	IT-utveckling, IT-Drift.	20
R5.	IT-chef och Digitalisering.	24
R6.	Backendutvecklare, Webmaster, Fintech.	23
R7.	IT-chef, IT-samordnare.	11
R8.	IT-arkitekt, tekniker, informationssäkerhet.	22

Tabellen illustrerar deltagare som kvalificerades inom ramen för fallstudien. Detaljer kring arbetsområde och sammanfattning av erfarenhet i branschen kan utläsas ur

tabellen. Uppgifterna i tabellen är hämtat och baserade på sammanställning direkt från det transkriberat material.

Vid genomförandet av datainsamlingen ställdes huvudsakligen frågor till respondenterna relaterat till sammantaget fyra kategorier som baserades på studiens förarbete och byggde således på data från kapitel 2 och 3. En övervägande del av diskussionen med respondenterna kretsade som ett resultat kring de huvudområdena som identifierade i förarbetet, frågor i intervjuerna ställdes därför kring följande områden:

- Förtroendet till molnleverantören.
- Leveransavtal och förhandling.
- Externdatalagring, hårdvara och drift.
- Delad IT-miljö.

Genom de listade kategorierna möjliggjordes för en relativt öppen diskussion om ämnet och samtidigt bibehållandet av en underliggande struktur för att undvika att diskussionen svävade ut från de områden som ansågs viktiga att undersöka.

5 ANALYS

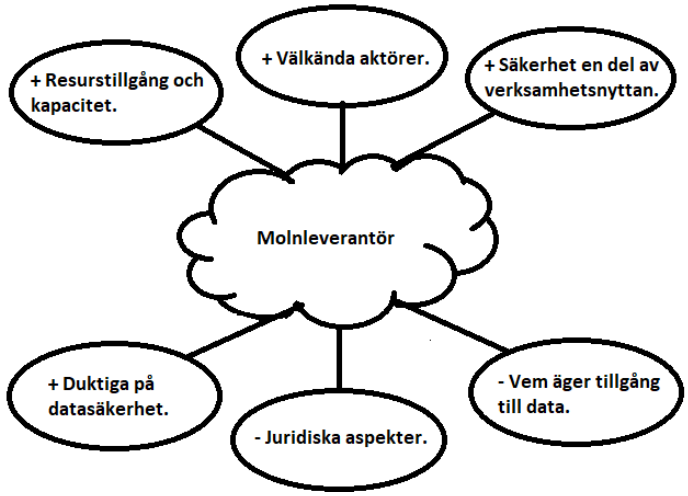
Kapitlet redoviserar analysprocessen av data som samlats in vid genomförandet, transkriberat material analyserades genom att selektera ut data efter fyra olika kategorier som byggde på nyckelbegrepp och termer identifierade i litteraturen. Använda kategorier kunde kopplas synonymt till de fyra huvudområden som diskuterades med respondenterna, se genomförande kapitel 4.4 och lämpade sig därför till att selektera ut data för analys kring respektive diskuterat område. Samtliga kategorier representeras som delkapitel i analysen och beskrivs i större detalj i följande kapitel, 5.1 till 5.4 och sammanfattas i 5.5.

Tabell 2: Kategorier.

Kategori:	**Område:**
1.	Förtroendet till molnleverantören.
2.	Leveransavtal och förhandling.
3.	Externdatalagring, hårdvara och drift.
4.	Delad IT-miljö.

Första kategorin förtroendet till molnleverantören, baserades på förlusten av kontroll som molnkonsumenten får över olika aspekter i molnet, som istället per automatik hanteras av molnleverantören (Subramanian & Jeyaraj 2018; Tabrizchi & Kuchaki 2020). Vid angrepp på molnbaserade tjänster tillfaller en stor del av försvarsförmågan till leverantören, konsumenten tillför därför automatiskt ett stort förtroende till leverantören och dess säkerhetslösningar (Coppolino et al. 2017). Kategori ett syftade således till att bearbeta och bygga en första sammantagen bild av molnkonsumentens förtroende ur perspektiv till de tidigare diskuterade riskerna som kunnat kopplas till molnet. Kategori två leverans avtal och förhandling, berör SLA, leveransavtalet som tecknas mellan molnkonsumenten och molnleverantören. Ett SLA styr vilka specifikationer en tjänst ska innehålla och även de olika parternas skyldigheter. Kategorin användes därför för att utläsa data som talade för hur respondenterna uppfattade sin förmåga att förhandla och påverka avtalet efter sina behov och säkerhetskrav (Subramanian & Jeyaraj 2018; Tabrizchi & Kuchaki 2020). Kategori tre externdatalagringar, hårdvara och drift, uppkom som ett resultat av de aspekter som kunde kopplas till förlust av kontroll över hårdvara, datalagring och geografiska aspekter när IT etableras i molnet (Subramanian & Jeyaraj 2018; Tabrizchi & Kuchaki 2020). Kategori fyra delad IT-miljö, berör respondenternas erfarenheter av multi-tenancy uppsättning och eventuella risker med att spinna upp virtuella maskiner och dela system/dataresurser med andra parallella processer i molnet (Yan et al. 2018; Ziani & Medouri 2018). Delad IT-miljö innebär uppkomsten av risker likt hypervisor angrepp och påverkar därmed molnkonsumentens datasäkerhet. Kategorin ämnar bygga en förståelse för hur respondenterna såg på förtroendet till molnleverantörens förmåga att säkra upp en delad miljö (Subramanian & Jeyaraj 2018).

5.1 Förtroendet till molnleverantören



Figur 3: Fördelar och nackdelar molnleverantör

Figur 3 visar de sammanställda faktorer som gemensamt på ett övergripande plan kunde konstateras ha en inverkan på molnkonsumentens förtroende till molnleverantören. Fördelarna och nackdelarna är sammanställda från de svar givna av respondenterna kopplat till litteratur och tidigare forskning som bygger studiens bakgrund och problemformulering. Delresultatet som presenteras i detta analyskapitel pekade på att de förtroendeingivande faktorerna övervägde nackdelarna. Primärt identifierades förtroende bygga på molnleverantörernas storlek, rykte och kapacitet, vilket respondenterna angav som förtroendeingivande faktorer. Trots det faktum att dessa faktorer inte har en bevisad påverkan på frekvensen eller angreppen mot en molnleverantör (Kelly et al. 2020). Säkerhet i sig, påpekades även vara en del av molnleverantörernas nytta som därför ansågs som ytterligare förtroendeingivande. Förtroendet mellan parterna är viktigt, leverantörens rykte relaterat till säkerhet kan möjligen, som antytt av respondenterna ha en påverkande effekt (Tabrizchi & Kuchaki 2020). Förtroendet brast snarare på punkter som av leverantören är svårpåverkade, juridiska aspekter och vem som äger tillgång till den data som lagras i molntjänsten. Dessa faktorer påverkade respondenternas förtroende negativt i större utsträckning än eventuell teknisk och intrångsproblematik (Tracol 2020).

Molntjänster kan skapa driftfördelar, så som skalningsförmåga och dataresurser efter behov, vilket inneburit att molnet blivit ett effektivt IT-alternativ för många organisationer. Trots diverse driftfördelar finns olika typer av säkerhetsutmaningar som kan relateras direkt till det publika molnet (Kelly et al. 2020; Tabrizchi & Kuchaki 2020; Yan et al. 2018). När IT etableras som molntjänst tilldelas molnleverantören per automatik en stor del av förtroende för molnkonsumentens datasäkerheten. Konsumenten måste således förlita sig på att leverantören kan bibehålla säkerhet för den levererade tjänsten. Ifall molntjänsten utsätts för ett angrepp, ligger en stor del av försvarsförmågan hos molnleverantören. Tillgänglighet till konsumentdata hanteras således i förtroende av molnleverantören som därmed måste säkerställa dess säkerhet

och tillgänglighet (Coppolino et al. 2017). Förtroende mellan parterna är en viktig komponent för att molntjänstmarknaden ska fungera (Tabrizchi & Kuchaki 2020). Denna studies primära syfte var därför att undersöka hur förtroendebilden till molnleverantören påverkades av negativa aspekter relaterade till säkerhetsrisker som kunnat kopplas till det publika molnet.

Samtliga respondenter gav svar som pekade på att deras övergripande förtroende och inställning till molnleverantörer var positiv. Förtroendebilden ur ett helhetsperspektiv kunde konstateras vara mycket hög. R1 beskriver på ett tydligt och koncist sätt varför förtroendet till leverantörerna ser ut som det gör, med ett resonemang som speglade svaren från många av de övriga respondenterna. *”Generellt tycker jag nog att utgångspunkten är att vi har ett stort förtroende för leverantören och deras säkerhetslösningar. Ofta handlar det om stora kända leverantörer som man köper tjänster från, till exempel Amazon.”, R1.* Förtroendet enligt R1 grundar sig således i det faktum att många av molnleverantörerna är kända och stora, man vet vilka dessa aktörer är och litar på deras förmåga att hantera de risker som finns. Respondenternas svar pekar alltså på att storleken och kännedom kring aktören talar för ett starkare förtroende att bibehålla säkerhet. Aktörens storlek kan dock inte konstateras vara en påverkande faktor när det kommer till frekvensen av angreppförsök mot en molntjänst, valet av en mindre aktör påverkar inte heller frekvensen av eventuella angrepp (Kelly et al. 2020).

R1 fann även stöd i sitt resonemang givet R2 som framförde liknande argument, men även uppgav ytterligare ett perspektiv gällande molnleverantören och datahantering. *”Det jag har mest erfarenhet av är den moderna varianten, de tre stora saas leverantörerna och där är förtroende gällande datasäkerhet väldigt högt och när det kommer till intrång. Lite mindre högt när det kommer till vilka leverantören delar med sig data av.”, R2.* I svaret hänvisade R2 till tre större molnleverantörer, som vid intrångsförsök och datasäkerhetssammanhang, enligt R2 ansågs vara förtroendeingivande. Trots det faktum som pekar på att frekvensen av angrepp egentligen inte går att relatera till leverantörens storlek (Kelly et al. 2020). R2 poängterade att problematiken snarare identifierades i olika aspekter relaterade till hur molnleverantören delar konsumentens data. Resonemanget kan troligen kopplas till juridiska aspekter, som resulterar i situationer då ett företag under vissa förutsättningar kan tvingas dela data, till exempel på en begäran av en stat (Tracol 2020).

R4 gav ännu ett konkret exempel på hur leverantörernas storlek kan ha en påverkan på konsumentens förtroende. *”Om man tittar på ett företag som omsätter 2-miljader och ett som omsätter 70-miljarder eller ännu mer. Amazon kontra någon europeisk molnleverantör. Så är det klart de har mycket mer resurser att lägga på att hålla en högre säkerhet och vara noga med information eller datasäkerhet.”, R4.* Resonemanget framfört av R4 tyder på ett högt förtroende för molnleverantörer och bygger på en liknande grund som argumentationen framförd av R1 och R2. R4 pekar således på att storleken talar för kapacitet hos aktören, vilket resulterar i ett ökat förtroende för aktörens säkerhetslösningar. Kapacitet talar alltså enligt R4 för ett övertag när det kommer till

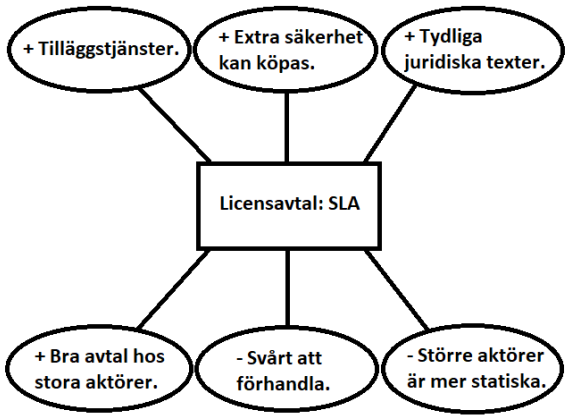
resurser att lägga på IT och informationssäkerhet. Att implementera en egen lokal IT-infrastruktur kräver en god IT-kapacitet, vilket inte alla bolag eller organisationer besitter, därför gjorde troligen många av respondenterna denna koppling, då erfarenheter kanske talade för komplikationer med att implementera egen IT (Fisher 2018).

En hög grad av konsensus har kunnat utläsas ur respondenternas svar, som även antytts från exempel av R1, R2 och R4, vilket tyder på att det övergripande förtroendet för molnleverantörerna är högt. Speciellt större leverantörerna uppfattas som mer förtroende ingivande på grund av kapacitet och resurstillgång. Uppfattningen bland respondenterna synkroniserade således inte med det faktum som pekar på den existerande angreppsproblematik som finns även hos stora molnleverantörer, vilket kan konstateras vara ett aktuellt problem och en utmaning för molnbaserade tjänster (Kelly et al. 2020). Respondenterna hade således en hög grad av konsensus i sitt förtroende för molnleverantörer, framförallt de större aktörerna, dock påpekade R2 tillsammans med andra respondenter att förtroendet snarare brister i tilliten för hur molnleverantören delar konsumentens data. R6 är inne på ett liknande spår som R2, förtroendet är högt, snarare ligger bristerna i geografiska och juridiska aspekter. R6 framförde ett resonemang som gav stöd till den problematik R2 diskuterade. *”Det skulle jag nog säga att man har, de jag har erfarenhet av är AWS. Jag har även kollegor som jobbat i Google Cloud. Jag har själv experimenterat lite med Google Cloud, men AWS är nog det jag har haft mest erfarenhet av sedan tidigare. Säkerhetsmässigt har jag inte hört några direkta dubier kring dem. Det handlar övergripande om vart man lägger sin data och vilka lagar som gäller då i landet.”, R6.* Enligt R6 som tidigare poängterat, ansågs förtroendet för säkerheten vara hög. Däremot pekade respondenten på att problematiken snarare baseras på geografiska aspekter och juridik, vilka är faktorer som kan ha en påverkan på hur ett företag hanterar data (Tracol 2020). När data migreras till molnet förvinner en del av konsumentens kontroll vilket kan vara en av anledningarna till betydelsen var data placeras som antytt av R6 (Yan et al. 2018).

En annan faktor som ansågs göra leverantören förtroendeingivande i frågor relaterade till säkerhet är den funktionella vikten för deras organisatoriska existens, R6 gav svar som pekade på detta perspektiv. *”De är väldigt beroende av att de är säkert och att man använder standarder, att de tillhandahåller tillvägagångssätt för att säkra data och säkra trafik. De skulle inte ha råd att misslyckas med det. Därför känns det både stabilt och pålitligt. Det är en del av deras affärsnytta.”, R6.* Säkerhet är en del av nyttan och av största vikt för molnleverantörerna, enligt R6, därför en faktor som ökar förtroende. Det är enligt R6 funktionellt av högsta vikt att leverantören inte fallerar på denna punkt. Bristande säkerhet skulle kunna spekuleras påverka molnleverantörens rykte, därmed leda till förlorade marknadsandelar, eftersom förtroende är viktiga komponenter när konsumenten väljer leverantör (Yan et al. 2018). Förtroendet mellan parterna är en viktig komponent och den faktor som R6 anger skulle kunna vara betydelsefull för att bibehålla en förtroendeingivande relation (Tabrizchi & Kuchaki 2020).

Sammanfattningsvis framfördes flertalet faktorer som talade för en positiv upplevelse av förtroendet till molnleverantörerna och säkerheten i deras tjänster. Leverantörens storlek ökade respondenternas upplevda förtroende, en faktor som ofta sammankopplades till en hög kapacitet och god resurstillgång. Respondenterna hade således ett högt förtroende till större aktörer trots att angreppsfrekvens troligen inte påverkas i beroende av leverantörens marknadsandelar (Kelly et al. 2020). Bygge av egen infrastruktur är dock ofta krävande och något som inte alla organisationer kan tillgodose, att vända sig till en leverantör skulle kunna tolkas som ett tryggt alternativ (Fisher 2018). Säkerhet beskrevs som en del av leverantörens nytta, därför ansågs de trovärdiga. Ett dåligt säkerhetsrykte skulle kunna leda till förlust av potentiella avtal med kunder (Yan et al. 2018). En faktor där leverantörerna ansågs mindre pålitliga var enligt respondenterna risken för att data skulle hamna hos tredje part. Juridiska aspekter skulle i detta fall kunna tolkas vara en påverkande faktor som leder till att leverantörerna tvingas dela data (Tracol 2020).

5.2 Leveransavtal och förhandling



Figur 4: Fördelar och nackdelar SLA.

Den sammantagna bilden beskrivs i Figur 4, respondenternas svar tyder på ett resultat där de förtroendeingivande faktorerna som framförts överväger nackdelarna. Respondenterna upplever dock komplikationer i förmågan att kunna påverka ett SLA innehållsmässigt, vilka ofta kunde tolkas vara statiskt strukturerade standardavtal. Ett SLA styrker molntjänstens innehåll på ett antal parametrar som berör aspekter så som, prestanda, tillgänglighet och säkerhet för den levererade tjänst (Subramanian & Jeyaraj 2018). Att kunna påverka dessa faktorer skulle kunna tolkas vara av vikt ur konsumentens perspektiv för att uppleva ett förtroende gentemot leverantören. Avtalet mellan parterna kan vara viktigt i arbetet för att motverka osäkerhet hos konsumenten och på så sätt öka förtroendet, därav skulle dess statiska karaktär kunna tolkas som en negativ aspekt i sammanhanget (Carvalho et al. 2017). Respondenterna påpekade även att det var svårt att förhandla med större aktörer, dock erbjöd dessa ofta i grund och botten troligen bättre avtal trots begränsade förhandlingsmöjligheter. Ett SLA styr specifikationerna inkluderade i en tjänst, fördelar tycks enligt respondenterna finnas i att vända sig till en större aktör då dessa kan erbjuda ett bättre avtal, dock ansågs det svårt

att förhandla i denna typ av förhållande (Subramanian & Jeyaraj 2018). Trots att ett SLA påpekades vara svårförhandlade, pekade respondenterna på att avtalen ofta hade en tydligt juridisk formulering, säkerhet och extra tjänster kan ofta inköpas som komplement för den redan befintliga tjänsten efter behov. Avtalets juridiska format skulle kunna tolkas som styrkande i förståelsen för respektive parts skyldigheter och därmed öka förtroendet mellan aktörerna. Tilläggstjänster kan ses som ett komplement till den statiska strukturen i grundavtalet, därmed ge molnkonsumenten större möjlighet att påverka innehållet i tjänsten (Tabrizchi & Kuchaki 2020).

SLA styrker genom specifikationer hur en molnleverantör är skyldigt att leverera en molntjänst till konsumenten (Subramanian & Jeyaraj 2018). Ett avtal bör dock inte ses som en garanti för en tillgänglig och säker tjänst och kan därför inte tolkas som en enhetlig säkerställare för kvalitén av levererad tjänst. Avtalet mellan konsumenten och leverantören skyddar således inte mot en dålig tjänst (Tabrizchi & Kuchaki 2020). Ett SLA dikterar dock faktorer som berör tjänstens innehåll och är ett affärskontrakt som styr konsumentens inköp, frågan är därför hur molnkonsumenten ser på avtalet och förmågan att förhandla och tillägga specifikationer efter behov (Subramanian & Jeyaraj 2018). Genom ett SLA kan förhoppningsvis molnkonsumtens osäkerhet kring risker i molnet motarbetas, därför är det intressant att se hur avtalet påverkar förtroendet till molnleverantören (Carvalho et al. 2017).

Konsumentens förhandlingsutrymme i ett SLA ansågs i stora drag av respondenterna vara begränsat. När ett SLA ska tecknas mellan de olika parterna finns oftast ingen möjlighet att påverka specifikationer för den levererade tjänsten, R2 poängterade just detta, vilket till en viss grad speglade de övriga respondenternas syn. *”Om du signar ett konto så får du acceptera deras kriterier. Och det är per definition det som blir avtalet med dig. Mellan dig och leverantören.”*, *R2*. När du skriver på menar R2, accepterar du ett SLA eller så blir det ingen levererad tjänst. Möjligheten att påverka relationen mellan leverantör och kund var enligt respondenten således något begränsad. Ett SLA styr specifikationerna som dikterar förhållandet mellan parterna, aspekter som tillgänglighet och skyldigheter mellan molnleverantören och molnkonsument. Det fanns alltså inget större utrymme enligt R4 att styra och påverka dessa aspekter efter eget behov (Subramanian & Jeyaraj 2018).

R1 styrker övergripande R2 ytterligare och pekar på att avtalen ofta skrivs i juridisk kontext. *”Jag tror att de flesta stora tjänsteleverantörerna inom Cloud i de flesta fallen har ganska vattentät och juridiska texter, där de garanterar men också friskriver sig vissa saker. Till exempel när det gäller skador åsamkat av mig. Som alla avtalen mellan köparen och säljaren så är de ju väldigt vattentät då det ofta rör sig om väldigt stora belopp.”, R1.* Avtalen var således, enligt R1, svårförhandlade av den anledning att det rör sig om juridiska texter och ofta involverar ekonomiska faktorer. R5 gav i sitt resonemang ytterligare stöd till R2 och styrker att det finns svårigheter att förhandla med de större aktörerna. *”De stora drakarna dikterar ganska mycket, det är inte så att en kommun kan komma in och säga, Microsoft nu får ni ge teamsleveransen till oss på det här viset. Det ligger väl i sakens natur att man får ta det lite som det kommer.”, R5*. Möjligheten att påverka ett SLA var

sammantaget enligt respondenternas något begränsad, så som antytts av R1, R2 och R5. Eftersom säkerhet är en viktig parameter, så skulle avtalens statiska karaktär kunna vara en negativ faktor för molnkonsument förtroende till molnleverantör säkerhetslösningar (Carvalho et al. 2017). Svårigheter att påverka innehållet i ett SLA kan få effekter på säkerhet, tillgänglighet och många andra specifikationer, så som vart respektive parts ansvar ligger (Tabrizchi & Kuchaki 2020).

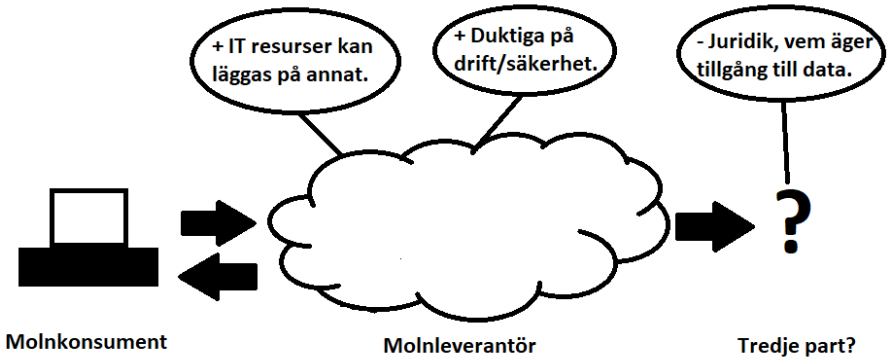
R4 var inne på ett liknande spår som de övriga respondenterna men utvecklade sitt resonemang ytterligare. *”Någon med mycket pengar kan prata med någon med mycket pengar. Om jag har en budget på 30-tusen i månaden, då kanske jag kan prata och förhandla med medium svensk leverantör eller europeisk leverantör och få igenom saker som är viktiga för mig. Men att gå till Amazon med min budget, de vill inte ens prata med mig men jag får ett bättre erbjudande by default. Det där får man utvärdera själv vad som är viktigt.”, R4*. Enligt R4 har molnleverantörens storlek i förhållande till konsumenten en effekt som leder till att förhandlingsutrymmet begränsas. SLA från en större molnleverantör hade trots dess statiska karaktär enligt R4 vissa fördelar. Anledningen var att större aktörerna ofta hade bättre erbjudanden till grund och botten. Standarder är ett viktigt verktyg för att bygga förtroende mellan molnkonsumenten och molnleverantören, transparens och ett väl formulerat avtal som pekar på vad som faktiskt levereras är viktigt för konsumentens förtroende. Trots att SLA från större aktörer inte gick att påverka, antydes av respondenten att de var väl formulerade till grunden, vilket kan tolkas som ett komplement till dess statiska karaktär (Carvalho et al. 2017).

Trots den begränsade förmågan till förhandlingsutrymme poängtera R6 att vissa leverantörer erbjuder tilläggstjänster efter behov. *”Tar vi AWS, så vet jag att de har infrastruktur som följer visa krav. Jag jobbade på det här företag som hade kortbetalningar. Då är det väldigt hårt reglerat av VISA och Mastercard, de har en väldigt hård standard, Payment Card Industry Data Security Standard.”, R6*. Tilläggstjänster kan enligt R6 adderas till en redan befintlig tjänst. Vilket möjligen kan öka flexibilitet till de områden som respondenterna konstaterade vara statiska. R5 styrker R6 resonemang ytterligare. *”Det finns säkerhetsmekanismer som man kan välja till om man vill ha ökad säkerhet. Men nyttjande avtalen eller SLA avtalet som är knutna till de här tjänsterna föreställer jag mig är ganska opåverkningsbara.”, R5*. Vid behov av extra säkerhet kan enligt R5 likt R6 olika tjänster tilläggas, men grundavtalet, SLA är svårt att påverka. Styrning av säkerhetsparametrar är viktigt vid val av molnleverantör, tilläggstjänsternas alternativ skulle således kunna tolkas ha positiv inverkan på förtroendet (Carvalho et al. 2017). Ekonomi var också en påverkande faktor vid förhandling enligt respondenterna, så som antytt av R3. *”Det kan man jämföra med långt tillbaka i tiden, då hade man ful och fin disk kallades det. Fin disk var snabbt då fick man svar direkt, när det var något som var lite ointressant la man det på lite långsammare och sämre disk längre bak i datahallen. Det kanske till och med kunde ta 10-20 sekunder att få fram något. Men det spelade ingen roll för man behövde bara få fram det någon gång ibland. Lite så är det på molntjänst sidan också att man kan betala för ökad säkerhet, ökad tillgänglighet.”, R3*. Säkerhet och tillgänglighet kan enligt R3 alltså med rätt ekonomiska incitament tillförskaffas. Vilket

innebär att tillgänglighet, datakraft och olika säkerhetsaspekter, vilka dikteras i ett SLA, enligt R3 kan påverkas av molnkonsumentens ekonomi och vilja att betala för extra tillägg (Subramanian & Jeyaraj 2018).

Summerat kunde ett SLA enligt respondenterna konstateras vara statiskt strukturerat och svårt att förhandla kring. Förhandlingsutrymmet är en faktor som därför skulle kunna tolkas som negativa i den mån att de begränsar konsumentens förmåga att få igenom specifikationer som skulle kunna anses viktiga för verksamheten (Subramanian & Jeyaraj 2018). Resultatet blir att konsumentens upplevda förtroende till tjänsten påverkas på grund av den begränsade förmågan att påverka respektive parts ansvar, så som säkerhetsaspekter och tillgänglighet (Tabrizchi & Kuchaki 2020). Att förhandla med större aktörer ansågs generellt enligt respondenterna som ännu svårare, dock bör det poängteras att dessa aktörer ofta erbjuder bra avtal till grunden, vilket skulle kunna tolkas som ett komplement till att vara mer komplicerade att förhandla kring (Carvalho et al. 2017). Extra tillägg och säkerhet kunde konstateras vara möjligt att köpa som ett komplement till den befintliga tjänsten. Säkerhetsaspekter och andra specifikationer som bör inkluderas skulle därmed möjligen kunna adderas (Subramanian & Jeyaraj 2018).

5.3 Externdatalagring, hårdvara och drift



Figur 5: Fördelar och nackdelar molndrift.

Figur 5 illustrerar fördelarna och nackdelarna som angivits av respondenterna, molnleverantören har ett högt förtroende i datasäkerhetsammanhang och är duktiga på drift. Nackdelar identifieras snarare kring juridiska aspekter och frågor som berör vem som äger tillgång till data. Införandet av egen IT infrastruktur är något som kräver en hög resurskapacitet, molntjänster och därmed extern drift kan ge organisationer flexibilitet och möjliggör för dessa resurser att frigöras (Fisher 2018). Molnleverantörerna ansågs generellt vara väldigt duktiga på sitt område och ansågs arbeta på ett effektivare och bättre sätt med drift och säkerhetsfrågor. Molntjänster dras med konstaterade brister men respondenterna ansåg sig troligen inte ha kapacitet att leverera ett bättre resultat (Coppolino et al. 2017). Molntjänster tillför dessutom många fördelar som leder till en ökad flexibilitet genom bland annat skalningsförmåga, vilket leder till en ökad kapacitet att hantera arbetsbelastning och möjliggöra tillgänglighet (Tabrizchi & Kuchaki 2020).

När data migreras till molnet tappar molnkonsumenten kontroll och placerar en stor del av sitt förtroende för datasäkerhet och hantering av datalagring i molnleverantörens händer (Yan et al. 2020). Till skillnad från lokal IT, vilket ofta innebär att konstruktören besitter den faktiska kontrollen över infrastrukturen (Winkler & Brown 2013). Konsumenten måste därför förlita sig på att molnleverantören hanterar många av utmaningar kopplade till säkerhet och drift, vilka konsument inte längre råder över (Coppolino et al. 2017). Frågan är således hur molnkonsumentens förtroende till leverantören påverkas av säkerhetsrisker i det publika molnet, ifall konsumenten faktiskt känner trygghet i molnleverantörens förmåga att hantera och lagra data, trots den faktiskt påvisade säkerhetsproblematiken (Kelly et al. 2020). En annan aspekt är konsumentens brist på kontroll och hur det geografiska perspektivet påverkar förtroendet till leverantören (Carvalho et al. 2017).

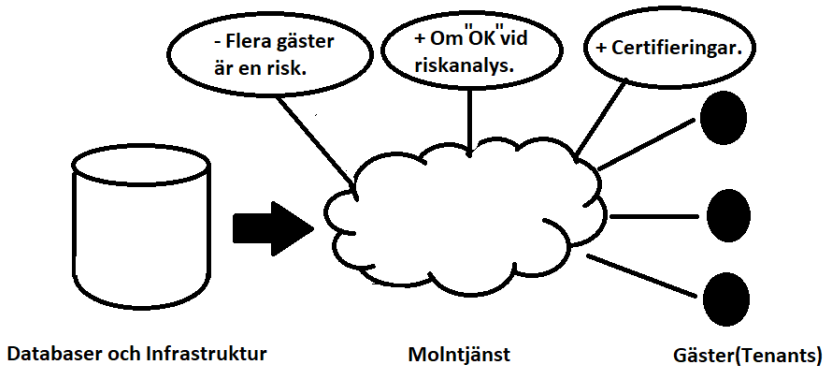
Respondenterna definierade molnleverantörens förmåga att hantera data som mindre trovärdig, detta oftast inte grundat i tekniska komplikationer, bristande kompetens eller resurser. Snarare brast förtroendet av det faktum att respondenterna inte fann en tydlig bild av till vem molnkonsumenten valde eller tvingades dela data med. R5 påpekade just detta i ett av sina resonemang. *”Nej egentligen inte, det beror på vad man menar med molnet. vi har dataskyddsförordningar att förhålla oss till. Utifrån Schrems II domen, så är det uppenbart att det finns molntjänster där vi inte får lagra, eller att vi behöver ställa högre krav på vår lagring.”, R5*. Juridiska aspekter så som dataskyddsförordningar och Schrems II domarna påverkade enligt R5 valet av vilken data som kunde överföras i förtroendet till molnleverantör. Schrems II domarna har inneburit ytterligare en komplikation i den mån att data som delats till en aktör utanför EU måste kunna säkerställa eller skyddas enligt GDPR (Tracol 2020). R8 framförde ett liknande resonemang som till viss del speglade R5, datalagring hos en molnleverantör kan vara problematiskt beroende på typ av data. *”Vi har en oerhört stor mängd typer av information och det kanske är så att vissa typer av information inte hör hemma där och de kanske får hanteras på ett annat sätt. Ett vårdsystem av något slag, geografisk dokumentation av elnät, sådant som påverkas av en säkerhetsgrad som gör att Office 365 kanske inte är olämpligt.”, R8*. Data kan beroende på situation, så som R8 resonerade inte vara lämpad för att lagra i molnet, vilket styrker det resonemang som R5 framförde. Det finns två möjliga anledningar till detta, konsumenten förlorar kontrollen och ger förtroendet till leverantören att hantera och säkerställa den data som överförs (Yan et al. 2020). Eller som tidigare diskuterat, den juridiska problematiken, vem äger tillgång till den data som lagras. Frågor som skulle kunna ställa är, kan tredje part komma över känslig information utan konsumentens medgivande, följer molnleverantören de lagar och regler som krävs (Tracol 2020; Rotenberg 2020). Förtroendet brister troligen på denna punkt av anledning att datahantering är ett problemen med molntjänster, data riskerar att hamna i händerna tredje part utan konsumentens godkännande (Tabrizchi & Kuchaki 2020). Effekterna grundat i de legala aspekterna som uppkommer mellan Europa och Amerika leder till att många europiska konsumenter har visat sig tveksamma i sitt förtroende till kommersiella tjänster och skulle istället föredra ett offentligt alternativ (Wagemann et al. 2021).

Respondenterna hade i större drag ett förtroende för molnleverantörens förmåga till drift och tillgänglighet av erbjuden tjänst. R2 sammanfattade på ett tydligt sätt fördelarna med att tilldela leverantören denna typ av förtroende. *”Man slipper att ens funder på om det finns en tekniker som sköter det här. Det är därför du väljer att betala för att någon annan ska hantera det. Om det är viktigt för dig att din tjänst har stor tillgänglighet är det viktigt att hårdvara är tillförlitligt. Att du inte får strömspikar att ramminnet är tillförlitligt, hårddiskarna inte dör, internet inte går ner.”, R2.* Uppfattningen enligt R2 är att det var fördelaktigt att kunna lämna driften till en annan aktör och istället fokusera på det som var viktigt. Trots konstaterade brister på en rad punkter inom IT-säkerhet, så hade respondenterna ett större förtroende till molnleverantörens förmåga att bygga en stabil tjänst, än att etablera egna IT-lösningar (Coppolino et al. 2017). När det kommer till tillgänglighet, skapar ofta molntjänster stordriftsfördelar, så som ökad skalningsförmåga, något som pekar på att molnbaserade tjänster kan erbjuda en högre grad av tillgänglighet (Tabrizchi & Kuchaki 2020). R2 förtydligar också ytterligare varför det är fördelaktigt att ge leverantören förtroende för driften. *”Ja, därför att de här storleverantörerna har anställda som är bättre på det här än du är. Det går inte komma ifrån det, de är inte bara en anställd som är bättre än du på alla punkter utan det finns en pol av människor som var och en är bättre på varje enskild punkt. Tillsammans bildar de en supermänniska som är otroligt mycket bättre på att hantera data än du är.”, R2.* Kompetens och kapacitet hos molnleverantörerna talade enligt R2 till deras favör, speciellt de större aktörerna. Resonemanget framfört av R2 går i linje med de komplikationer mindre organisationer ofta kan erfara vid införandet av egen IT. Vilket leder till att molntjänster blir ett kostnadseffektivt och flexibelt alternativ som även kan frigöra IT resurser till annat än egen implementation och drift (Fisher 2018). R7 gav ytterligare stöd för detta och poängterade att en organisation bör lägga sina IT-resurser på sådant som är av större vikt och ger ett värde. *”Den största fördelen som jag ser är att man kan använde sina resurser, de mänskliga resurserna på annat som är bättre än att hålla på och skruva i socket. Att lägga ut massa pengar på färskvara om man ska ha det själv. Nu kan vi bara koppla upp oss och vi har allt vi behöver.”, R7.* Bilden framförd av många av respondenterna pekar på fördelar med att ge leverantören förtroendet för drift, så som poängterat av R7, kan resurser frigöras och läggas på annat. Något som troligen inte hade varit en möjlighet vid bygge av egen IT-infrastruktur och drift (Fisher 2018).

Till större del upplevde respondenterna stora fördelar med att tilldela förtroende för drift, datahantering och infrastruktur till en extern aktör. Detta går i linje med det faktum att molntjänster ofta kan erbjuda organisationer många olika driftfördelar (Tabrizchi & Kuchaki 2020). Molnleverantörerna ansågs duktiga på sitt arbete och upplevdes ofta ha tillgång till en högre grad av kapacitet än konsumenten vid IT-drift. Möjligen kopplat till komplikationer och de krav som hade uppkommit för att införa en egen IT-lösning som hade varit jämförbar molnet (Fisher 2018). Nackdelarna identifierades snarare kring de juridiska aspekterna, respondenterna upplevde att problematiken uppkom i frågor om vem som äger tillgång till data. I detta anseende upplevdes leverantörerna vara mindre tillförlitliga. Lagar och regler skulle kunna leda till att data kan hamnar i fel händer eller

att data lokaliserar och lagras på ett sätt som inte är juridiskt korrekt (Tracol 2020; Rotenberg 2020). Generellt med Europa som utgångspunkt skulle många av konsumenterna kunna konstateras föredra offentligt erbjudna molntjänster istället för kommersiella. Troligen grundat i de legala aspekterna som uppkommer mellan Europa och Amerika, juridiska aspekter kan därmed konstateras vara ett problem (Wagemann et al. 2021).

5.4 Delad IT-miljö



Figur 5: Fördelar och nackdelar delad IT-miljö.

Respondenternas uppfattning kring effekterna av en delad IT-miljö illustreras i Figur 5. Övergripande svaren från respondenterna tyder på att molnkonsumenten har förståelse och en medvetenhet kring de eventuella riskerna med en delad IT-miljö. Effekterna av multi-tenancy och de risker som finns med en delad IT-infrastruktur och det eventuella resultatet ifall någon av användarna i molnet angrips, var således något respondenterna till en viss del hade förståelse för (Yan et al. 2018; Ziani & Medouri 2018; Díaz de León Guillén et al. 2020). Trots risker med multi-tenancy, så som hypervisor angrepp, påpekade respondenterna att etablering i moln ofta föregås av en riskanalys där man får utvärdera situationen och avgör ifall tjänsten är lämplig (Subramanian & Jeyaraj 2018). Standarder, certifieringar och analyser kan leda till förståelse och transparens i molnleverantörens säkerhetsarbetet. Därmed bidra till att konsumenten känner ett ökat förtroende till tjänsten (Carvalho et al. 2017). Faktorerna som framförts av respondenterna pekar på att förtroendet inte påverkas negativt av riskerna ifall molnkonsumenten kunnat bilda sig en uppfattning kring tjänsten och dess risker. Detta speglar det faktum att transparens och förståelse för en tjänst och dess eventuella risker är viktiga för att bygga tillit och förståelse (Van der Werff et al. 2019).

Molntjänster bygger ofta på en delad IT-miljö, vilket innebär att flera virtuella maskiner exekverar parallellt i molnet även känt som multi-tenant. Att kunna spinna upp virtuella maskiner är en teknologiskt viktig komponent, men också en faktor som medför ett antal säkerhetsrisker. (Yan et al. 2018; Ziani & Medouri 2018). Angripare kan utnyttja multi-tenancy miljöer genom hypervisor angrepp och därmed dra nytta av den delade IT-miljön i elakartat syfte (Subramanian & Jeyaraj 2018). Frågan är hur molnkonsumenten ser på molnleverantören förmåga att värja sig mot denna typ av angreppsmetodik, känner

konsumenten ett förtroende att etablera sin IT i en delad miljö, hur påverkar denna angreppsfaktor konsumenten och dennes förståelse för riskerna. För att bygga ett starkt förtroende måste konsumenten ha en förstå vad riskerna med den tjänst som brukas innebär (Van der Werff et al. 2019).

Generellt ansåg respondenterna att problematiken gällande risker som uppkommer ur ett resultat av en delad IT-miljö inte påverkade förtroenden för molnleverantören och dess säkerhetslösningar. R4 gav ett konkret exempel som gick i linje med hur många av de övriga respondenternas resonerade. *”Det är egentligen på alla nivåer, har du en certifiering för det som molnleverantör, då förutsätter man att sådana saker inte ska hända. Men sårbarheten finns på alla nivåer. Det är omöjligt att garantera, att skydda sig, så länge du har en multi-tenancy set up.”, R4.* Respondenterna kunde alltså konstateras vara medvetna om riskerna med multi-tenancy och de effekter som kan uppkomma av en delad IT-miljö byggd i samma grundläggande infrastruktur, denna dimension av angreppsproblematik relaterad till molnet övervägs av respondenterna vid val av molnleverantör (Yan et al. 2018; Ziani & Medouri 2018; Subramanian & Jeyaraj 2018). För att molnkonsumenten ska kunna känna förtroende gentemot molnleverantören måste förståelse finnas för de risker som bruk av tjänsten eventuellt medför, något som antyddes finnas hos respondenterna (Van der Werff et al. 2019). R4 menade också att molnleverantör kan erhålla certifiering för denna typ av problematik. Standarder och certifieringar är något som kan användas för att bygga förtroende mellan en konsument och leverantör (Carvalho et al. 2017).

R4 utvecklade sitt resonemang ytterligare och poängterar att det snarare handlade om att göra ett avvägande gällande säkerhet och risker. *”Har du något som är så pass viktigt får du väga fördelarna mot nackdelarna, kostnad versus säkerhet. Det motsattsförhållandet finns ju alltid. Jag har inte upplevt detta som något man tänker på.”, R4.* R5 Styrker bilden given av R4 och beskriver på i sitt resonemang på ett sätt som speglar R4. *”Nej det är självklart, tittar man generellt på stora molnleverantörer och leverantörer av iaas eller paas tjänster är det absolut intressant för en illasinnad att attackera. För man kan få stor påverkan om man kommer in där. Och andra sidan har den här typen av företag en helt annan nivå av resurser för att arbete med IT-säkerhetsfrågor. Lite som jag var inne på från början, man får välja att ha förtroende för de här företagen och blir man motbevisad får man omvärdera de beslutet. ”, R5.* Beskrivningen från R5 korrelerar i stort med resonemanget givet av R4, det finns en medvetenhet kring riskerna men R5 poängterar att det handlar om att välja att ge sitt förtroende till molnleverantören. R1 bygger vidare på samma resonemang som R4, R5 och styrker att man väljer att placera tilliten hos molnleverantören, riskerna finns men fördelarna är större. *”Man får göra en bedömning tänker jag från fall till fall om det är lämpligt att dela IT-miljö. Många små Start up och high tech företag skulle inte existera om det inte fanns Cloudleverantörer för att tillgodose IT-miljö. Hela deras miljö bygger på att det finns datorkraft att köpa, att det finns någon annan som tar hand om service, support och underhåll.”, R1.* R1, R4 och R5 menar på att det handlar om att göra ett avvägande, förståelse för risker med tjänsten underlättar möjligen i denna mån och möjliggör för molnkonsumenten att ge förtroende till molnleverantören

(Carvalho et al. 2017). Certifieringar och standarder kan styrka förtroendet i denna mån att det talar för en transparens i hur molnleverantören arbetar, något som också är viktigt för att molnkonsumenten ska kunna känna ett förtroende till leverantören (Van der Werff et al. 2019).

R2 bidrar med något mer nyanserad bild och poängterar att risken möjligen kan relateras till vilken typ av tjänstemodell som konsumeras. *"Det beror på vilken nivå vi landar på. SaaS nivå nej, paas nivå nej. Men på de lägre nivåerna måste du tänka på sådana saker. Om det är delade resurser.", R2.* Enligt R2 ökar risken beroende vad det för typ av tjänst, iaas, paas eller saas, vilket korrelerar till de tre vanligen kategoriserade tjänstemodellerna i molnet (Ziani & Medouri 2018). R2 tillägger att hotbilden finns på samtliga nivåer men varierar *"Det är klart att de är möjligt på de andra också. Men då har du väldigt duktiga människor som har designat sitt nätverk för att minimera den vektorn. Chansen är mindre ju längre ner att detta är gjort på ett bra sätt.", R2.* Risken kan således enligt R2 variera mellan olika nivåer i molnet, vilket skulle kunna påverka konsumenten beroende på vilken modellnivå som ska nyttjas. R2 menar således att hypervisor skyddet och andra tekniker för att motarbeta denna typ av angreppsvektor möjligen är konstruerad på ett bättre sätt desto högre tjänstemodell som brukas (Ziani & Medouri 2018).

R8 likt de övriga respondenterna var medveten om riskerna och summerade sitt resonemang på ett sätt som speglade helheten. *"Det finns många anledningar att ha kunskap om de aktuella sårbarheter som påverkar sin driftsmiljö. I en multi-tenantlösning dras detta till sin spets då det potentiella läckaget kan ske över kundgränserna.", R8.* Framförande pekar på vikten av att veta vad som är påverkar driftsmiljön vilket är av största vikt, R8 tillägger. *"Att ha kunskap om sårbarheterna är avgörande för en bra risk- och sårbarhetsanalys som i sin tur kan påverka vilken information som man väljer att behandla i molntjänsten. Alternativ vilken typ av molntjänst, delad vs. dedikerad server man väljer att konsumera.", R8.* Respondenterna var i stora drag medvetna om riskerna med en multi-tenancy baserad miljö. Virtuella maskiner och delad infrastruktur leder till brister som kan nyttjas av elaksinnade, för att bryta hypervisor skydd och angripa molntjänsten (Subramanian & Jeyaraj 2018; Ziani & Medouri 2018). Många av respondenterna pekade på att det är viktigt att göra ett avvägande vid bruk av denna typ av tjänster. Förståelse för riskerna med tjänsten kan vara en bidragande faktor för att molnkonsumenten ska kunna uppleva ett högt förtroende till leverantören (Van der Werff et al. 2019).

Respondenterna konstateras i stora drag vara medvetna om säkerhetsriskerna med effekterna av en multi-tenancy uppsättning. Risker med att bruka en delad IT-miljö var således en negativ aspekt på konsumentens förtroende till molntjänsten och leverantörens förmåga att bibehålla säkerhet (Yan et al. 2018; Ziani & Medouri 2018; Subramanian & Jeyaraj 2018). Molnleverantörer som kan uppvisa certifiering som pekar på att de har förmågan att säkerställa tjänsten mot denna typ av problematik uppfattades som mer förtroendeingivande. Certifiering tillsammans med möjligheten att utföra en riskanalys kan leda till ökad förståelse för tjänsten, vilket skulle kunna leda till upplevelsen av ett ökat förtroende till leverantören (Van der Werff et al. 2019).

5.5 Sammanfattning av analys

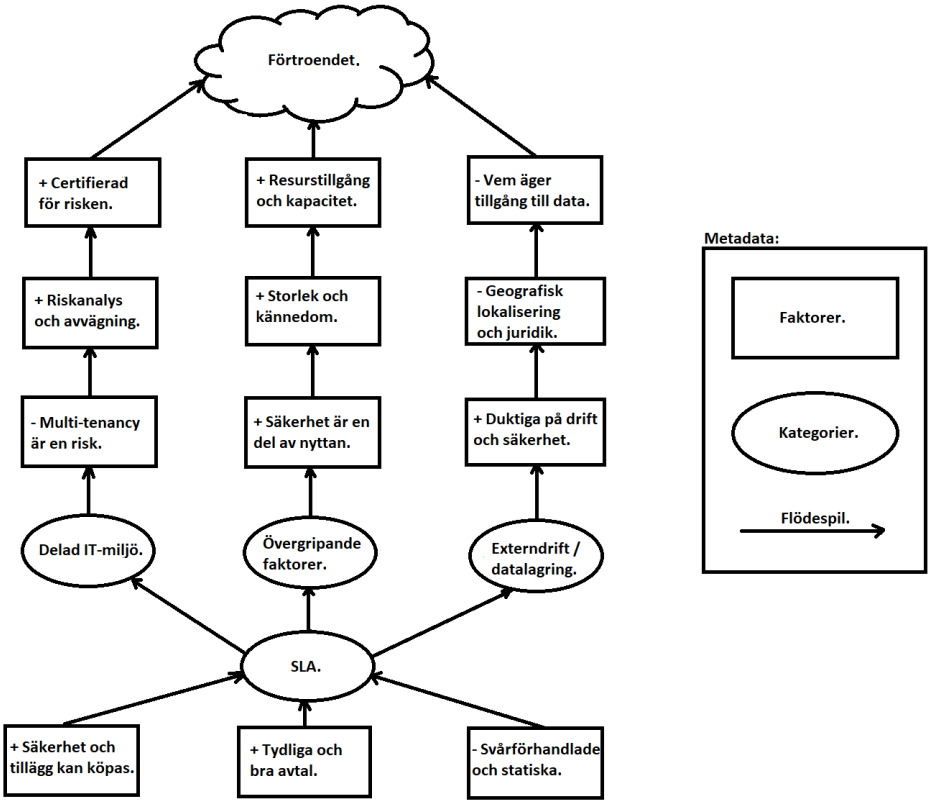
Den sammantagna analysen pekade på att det upplevda förtroendet till molnleverantörerna var högt. Faktorer som hade en positiv påverkan på respondenternas förtroende identifierades primärt i erfarenheter som visade på att leverantörens storlek talade för kapacitet och god resurstillgång att värja sig mot angrepp. Konsumentens upplevelser stämmer således inte med det faktum att även molnmiljöer som etableras av större aktörer är mål för frekventa angrepp (Kelly et al. 2020). Införandet av lokal IT är dyrt och kräver en god kapacitet, molnet uppfattades av respondenterna som ett trovärdigt alternativ när dessa faktorer inte fanns tillgängliga. Respondenterna upplevde även att molnleverantörerna var duktiga på drift, konsumentens kunde som ett resultat av molntjänsterna frigöra resurser till annat istället för egen IT-drift (Fisher 2018). Säkerheten i molnet upplevdes även som trovärdig eftersom det uppfattades som en del av molnleverantörens nytta, att bibehålla säkerheten skulle kunna tolkas vara mycket viktigt konkurrensmässigt eftersom säkerhetsbrister kan vara en påverkande faktor som avgör konsumentens val av leverantör (Yan et al. 2018). De SLA som erbjuder tjänsterna kunde enligt respondenterna kompletteras med tilläggstjänster, större aktörer erbjöd även bra avtal till grunden. Standarder och certifieringar upplevdes även som något som kunde betrygga konsumentens förtroende, möjligen på grund av ökad transparens i hur leverantören arbetar (Carvalho et al. 2017). Möjligheten att kunna göra ett avvägande och riskanalys kring en leverantör ansågs även vara en viktig parameter, något som skulle kunna kopplas till vikten av förståelse för att kunna bygga förtroende till tjänsten (Van der Werff et al. 2019).

Nackdelarna som påverkade respondenternas upplevelse av förtroendet negativt, identifierades primärt kring juridiska aspekter. Lokalisering av data kombinerat med lagar och regler risker att leda till att konsumentens data skulle kunna hamna hos en tredje part (Tracol 2020). Infrastrukturen och effekterna av en delad IT-miljö upplevdes även som problematiskt, trots det faktum att respondenterna uppgav faktorer som skulle kunna komplettera eller säkra för risken. Faktum kvarstår att molnbaserade tjänster med multi-tenant uppsättning kan nyttjas i elakartat syfte (Yan et al. 2018). SLA ansågs även vara av statisk karaktär och det påpekades svårt att förhandla med större aktörer, detta skulle indirekt kunna ha en påverkan på konsumentens förmåga att styra innehållet i tjänsten (Subramanian & Jeyaraj 2018).

6 Resultat

Denna studie syftade till att undersöka vilka faktorer som var avgörande för molnkonsumentens upplevda förtroende till molnleverantören. Relaterat till leverantören och dess hanteringen av diverse säkerhetsrisker och problem som kunnat identifieras kopplat till molnet, således lydde arbetets forskningsfråga enligt följande:

Hur upplever molnkonsumenterna förtroendet till molnleverantören att bibehålla säkerheten i molnet?



Figur 6: Förtroende träd.

Figur 6 visar en sammanfattning av de faktorer som identifierats i kapitel 5 och har kategoriserats i tre olika grenar: delad IT-miljö, externdrift/datalagring, övergripande faktorer och en stam ett SLA eller leveransavtal. Ett SLA är den grundläggande faktorn som specificerar hur en molntjänst ska levereras, vilket indirekt leder till en påverkan på samtliga faktorer i molnet. De tre kategorierna tillsammans med SLA kunde konstateras ge upphov till ett antal positiva och negativa faktorer som påverkade molnkonsumtentens upplevelse av förtroendet till molnleverantörens förmåga att bibehålla en säker tjänst. Kategorierna och dess olika faktorerna skulle kunna sammanfattas likt följande:

Sammanfattning av identifierade faktorer som påverkade förtroendet positivt.

+ Molnleverantörens storlek och kapacitet, större aktörer ansågs bättre.

+ Säkerhet är en del av nyttan.

+ Certifieringar och möjlighet till riskanalyser.

+ Leverantörerna anses vara duktiga på säkerhet och drift.

+ Tillägg och extra säkerhet kan ofta köpas efter behov.

Sammanfattning av identifierade faktorer som påverkade förtroendet negativt.

- Effekterna av en delad IT-miljö (multi-tenancy).

- Juridiska aspekter.

- Geografisk lokalisering.

- SLA ansågs ofta vara statiska och svårförhandlade.

Molnkonsumenternas upplevda förtroende till molnleverantören kunde konstateras vara högt, åtta av åtta respondenter poängterade en rad olika faktorer som pekade på detta förhållande. Således litar konsumenten på leverantörens säkerhetslösningar, förmågan att bibehålla datasäkerhet och kvalité för den levererade tjänsten. Mycket tyder på att konsument ofta uppfattade införandet av egen IT som komplext och svårt, detta troligen för att det kräver en hög grad av kapacitet att faktiskt bygga något som skulle kunna spegla det som molnleverantörerna erbjuder. Just kapacitet och kännedom var faktorer som talade för förtroende, egenskaper som många av molnleverantörerna på marknaden innehar. De kunde alltså, när det handlar om molntjänster, enligt respondenterna konstateras ofta röra sig om stora välkända aktörer. IT-säkerhet konstaterades även vara en del av molnleverantörernas marknadsnytta, därför uppfattades de som trygga och trovärdiga alternativ, det påpekades att det skulle vara förödande för en aktör ur ett konkurrensperspektiv med en större säkerhetsmiss. Säkerhetsrisker relaterade till det publika molnet, kunde således inte på ett övergripande plan konstateras påverka molnkonsumenternas förtroende till molnleverantören negativt.

Leveransavtalet eller SLA styr vilka specifikationer som gäller för den konsumerade tjänsten, avtalen kunde ur konsumenternas perspektiv konstateras vara av statisk karaktär. vilket skulle kunna tolkas som negativt och försvåra möjligheten att få igenom viktiga aspekter i avtalet. Specifikt nämndes förhandlingsutrymmet med de större aktörerna på marknaden som uppfattades som begränsat. Det bör dock konstateras att konsumentens uppfattning pekar på att det finns kompletterande möjligheter för att väga upp för den statiska karaktären av ett SLA. Tilläggstjänster och ekonomiska förutsättningar kan användas som komplement för att få igenom extra säkerhet vilket därmed kan tolkas som en styrkande faktor för förtroendet till att tjänsten hanterar organisationens data och behov på ett tryggt sätt.

Förtroendet påverkades inte heller negativt av det faktum att IT-drift och datalagring hanterades externt. Molnleverantörerna ansågs vara duktiga på drift, att hantera data och kunde ofta konstateras enligt respondenterna vara bättre lämpad än konsumenten i detta avseende. Återigen troligen kopplat till komplexiteten som kan identifieras vid

implementation av egen IT tillsammans med det behov av kapacitet som krävs vid drift. Som ett resultat kan det därför konstateras att molnkonsument i hög grad såg fördelarna med att tilldela förtroendet för drift och datahantering till en extern aktör. Resultatet leder ofta till möjligheten att kunna frigöra IT-resurser till annat, vilket ansågs mer fördelaktigt än att lägga resurserna på förmågan på till egen infrastruktur och IT-drift. Dessutom som tidigare benämnt, ansågs molnleverantören som väl rustad för att bemöta eventuella hot och risker. Komplexiteten i frågan uppkom snarare kring juridik och frågor som berörde geografisk lokalisering. Molnkonsumenternas förtroende brast snarare till molnleverantörerna när det kommer till frågor om vem som äger tillgången till data som lagrats i molnet. Lagar och regler varierar från land till land och det anses därför svårt att ha förtroende till molnleverantörerna ur detta perspektiv. Risken finns att leverantören tvingas eller delar data, med tredje part, utan berörd organisation vetskap eller mot deras vilja. Problematiken gör att konsumenten inte alltid kan förlita sig på att bruka en molntjänst i de sammanhang då säkerhetsgraden för data inte tillåter risken. Juridik kan även leda till komplexitet då konsumenten trots tillit och ett högt förtroende inte kan etablera IT i molnet på grund av legala risker.

Vid etablering av IT i publika molntjänster utsätter även konsumenten sig för de risker som uppkommer av en delad IT-miljö. Molnkonsumenterna var ofta medvetna om riskerna med att etablera IT i en delad miljö och de eventuellt negativa konsekvenser som kan bli ett resultat. När IT ska etableras i denna typ av miljöer föregås ofta implementationen av en riskanalys, där gör konsumenten ett avvägande huruvida molntjänsten är lämplig, trots de eventuella riskerna. Ifall avvägandet tyder på ett ja, så kan konsumenten med den ökade kunskapen känna ett starkare förtroende för tjänsten. Standarder och certifikat som visar på molnleverantörens förmåga att hantera denna typ av problematik är också faktorer som ökar förtroende och inger trygghet hos konsumenten.

6.1 Sammanfattning av resultat

Sammantaget kan det konstateras att molnkonsumentens förtroende till molnleverantören är högt. Det är svårt att som konsument införa egen IT, så till vida inte stor kapacitet och tillgång till resurser finns tillgängligt för att utföra IT-drift på ett sätt som är mätbart med leverantörerna. Datasäkerhet och skydd mot intrång är en del av leverantörens marknadsnytta och de är enligt konsumenten duktiga på det de gör. Aktörernas storlek är därför en påverkande faktor till förtroendet, mindre aktörer konstaterades ha mer att bevisa än större aktörer. Således räds inte molnkonsumenten vid bruk av tjänster från större molnleverantörer att bristande säkerhet skulle uppkomma som ett resultat av ett angrepp, intrångsförsök eller svagheter som uppkommer på grund av en multi-tenancy uppsättning. Däremot finns en rädsla och osäkerhet hos konsumenten vilket primärt uppkommer på grund av juridiska och geografiska aspekter. Problematik identifieras ofta i frågan om vem som äger rätt till data, en anledning till detta kan vara på grund av lagar och regler som varierar mellan olika länder. Molnleverantören kan som resultat tvingas dela data till tredje part, ibland kanske

möjligen utan konsumerande organisations vetskap. Juridiken i sig kan även uppkomma som ett hinder, vilket leder till att konsumenten tvingas avvakta med att etablera viss IT i molnet. Främst på grund av osäkerhet ifall lagar och regler tillåter att data lagras externt hos en molnleverantör.

6.2 Resultatet i relation till tidigare forskning

Etablering i molnet har visat sig föregås av ett SLA, där dikteras tjänstens specifikationer (Subramanian & Jeyaraj 2018). Molnkonsument uppfattade SLA som svårförhandlade, ofta rör det sig om större aktörer med stående erbjudanden av statisk karaktär. Att som konsument påverka tjänstens innehåll kunde konstateras begränsat, som komplement för att påverka innehållet inhandlas oftast tilläggstjänster.

Molnkonsumentens övergripande förtroende till molnleverantören kunde konstateras vara högt, en av de huvudsakligen faktorerna som identifierades i denna studie är leverantörens storlek vilket talade för kapacitet och resurstillgång något som ansågs förtroendeingivande. Tidigare forskning har uppmärksammat vikten av kapacitet och resurstillgång för att en organisation ska klara utmaningen att implementera en egen lokal IT-lösning (Fisher 2018). Detta kan vara en trolig anledning till att konsumenten kände ett förtroende till leverantörerna, då det ofta antydes röra sig om större aktörer som därmed hade tillgång till dessa faktorer.

Molntjänster har tidigare kunnat påvisas vara mål för frekventa angrepp och storleken hos aktören är ingen garant för en säker tjänst (Kelly et al. 2020). Trots detta hade konsumenten förtroende för leverantörens IT-drift och ansåg även i många fall att leverantören gjorde ett bättre jobb. Molntjänster har också kunnat konstateras erbjuder konsumenten driftfördelar i form av skalning och ökad tillgänglighet (Yan et al. 2018; Tabrizchi & Kuchaki 2020). Dessa faktorer som påvisat av tidigare forskning skulle kunna vara en trolig anledning till att konsumentens övergripande förtroende är så högt. Multi-tenancy uppsättning som molntjänster dras med har i tidigare forskning kunnat konstateras bidra till ett antal säkerhetsrisker (Yan et al. 2018). Molnkonsumenterna var medvetna om denna risk, men ansåg att vetskap om molnleverantören i form av riskanalyser och bevis på certifieringar kunde styrka förtroendet till tjänsten. Ökad förståelse har i tidigare forskning kunnat påvisa resultera i ett ökad förtroende till en tjänst (Van der Werff et al. 2019). Certifieringar kan även påpekats skapa transparens, vilket ytterligare skulle kunna bidra till denna faktor (Carvalho et al. 2017).

Tidigare forskning pekar på problematik som uppkommer när data transfereras mellan exempelvis EU och Amerika. Juridiken varierar mellan olika länder och leder till att en organisation måste förhålla sig till risker som kan uppkomma om data hamnar utanför EU (Tracol 2020; Rotenberg 2020). Molnkonsumenten upplevde detta faktum som problematiskt i relationen till molnleverantören och oroades att data skulle kunna delas till en tredje part. Juridik var således en faktor som frekvent återkom i ett negativt sammanhang.

6.3 Resultatets påverkan och nytta

Studiens resultat pekade på att molnkonsumentens förtroendet till molnleverantören i generell bemärkelse är högt, konsumenten litar ofta på leverantörens säkerhetslösningar. Resultat visade dock på att ett antal faktorer som undersöktes vilka hade en negativ effekt på konsumentens uppfattning om leverantören. Faktorerna berörde juridiska aspekter och tyder på att molnkonsumenten upplever en oro över hur molnleverantören delar data till tredje part. Denna faktor kan ha en stor betydelse för hur en konsument väljer molnleverantör, den leverantör som kan påvisa att möjligheten finns för konsumenten att säkra sin data på ett sådant sätt som gör att den inte riskerar att hamna i fel händer. Kan också dra stor vinning då många konsumenter, kan spekuleras välja just den aktör som kan påvisa detta. Studien ger således uppkomsten till data som kan användas i marknadsmässigt syfte för att bilda uppfattning kring faktorer som är viktigt för att vinna förtroendet till de aktörer som konsumerar molntjänster. Förtroende skulle kunna tolkas vara en viktig faktor i en affärsmässig relation och bör därför vara aktuellt i samband med kommersiella intressen och molntjänster.

Resultatet från studien skulle även kunna användas i forskningssyfte, konsumentens upplevelser kring olika säkerhetsrisker och molntjänster skulle kunna användas till grund för att undersöka hur och ifall riskerna bemöts på ett lämpligt sätt av konsumenten i förhållande till utmaningarna de skapar. Vetskapen om att förtroendet till leverantörerna är högt, skulle också kunna användas till grund i en studie som vidgar vyn ytterligare och tittar på eventuella konsekvenser av ett högt förtroende till externt baserad IT, mer om framtida forskning diskuteras i kapitel 7.5.

7 Diskussion

Kapitlet tar upp och diskuterar arbetet ur ett samhällsperspektiv, vetenskapligt perspektiv, etiska aspekter kring resultat/utförandet, kritik av arbetet och slutligen förslag på eventuella framtida forskningsområden.

7.1 Molnet ur ett samhällsperspektiv

Implementation av egen IT är ofta komplext och kostsamt, detta leder till att organisationer i högre grad vänder sig till större aktörer och brukar deras infrastruktur eller tjänster. Således vänder sig ofta organisationer till molnleverantörer som via sin infrastruktur erbjuder diverse IT-lösningar i form av molntjänster. Molntjänster har därför fått en alltmer betydande roll i samhället, en större del av IT etableras alltmer succesivt i molnet. Molntjänster tilldelar ofta konsumenten diverse fördelar som är svåra att implementera på egen hand, så som en ökad skalningsförmåga för att hantera inkommande arbetsbelastningar i systemet. Molnleverantörer har som ett resultat fått en allt större roll i samhället i korrelation med en högre grad av digitalisering och fler organisationer som förlitar sig på deras tjänster. Resultatet när en organisation brukar molntjänster blir ett överförande av kontroll till leverantören över aspekter så som säkerhet och tillgänglighet av IT. Organisationer räds som ett resultat ofta hur deras data hanteras och vilka aktörer som äger rätten av tillgång till den data som lagrats i molnet.

Denna studie undersökte hur molnkonsumentens förtroendet till molnleverantören påverkades av eventuella säkerhetsrisker, vilka ofta kunnat relateras direkt till publika molnet. Förtroendet är en viktig och avgörande faktor, att bruka molntjänster från en leverantör innebär att ge aktören förtroende för drift, data och IT-säkerhet. Transparens och förståelse för hur leverantörer hanterar konsumentdata och säkerställer kvalité för tjänsten är viktigt när konsumenten ska fatta ett beslut om vilken leverantör som ska få uppdraget att leverera tjänsten. Resultatet av studien pekar på att organisationer faktiskt har ett högt förtroende till olika leverantörer, snarare är det juridiska och geografiska begräsningar som lägger krokben på vad som får etableras i molnet. En del av debatten skulle kunna kopplas till GDPR och Schrems II domarna som skapat svårigheter för organisationer att etablera IT i molnet med risk att data hamna utanför EU. Exempelvis är många av de större molnaktörerna på marknaden amerikanska, vilket innebär att molnkonsumenten måste ta i beaktande att lagring av data via dessa kan hamna i händerna på amerikanska staten. Molntjänster väcker således etiska och samhällsviktiga frågor, personuppgifter riskerar att hanteras av tredje part utan organisationen eller individens vetskap, detta skulle kunna argumenteras för att vara en av de större utmaningar i framtiden för molnbaserade tjänster. Över lag pekar dock flera faktorer på att fördelarna överväger nackdelarna, molntjänster möjliggör ofta sådant som mindre eller medelstora organisationer inte skulle klara bygga på egen hand. Studien pekar på ett högt förtroende till molnleverantörens säkerhetslösningar och driftförmåga. Juridiken skulle ur en positiv synvinkel kunna tolkas viktig för att säkerställa vad som gäller kring aspekter så som skydd av konsumenten, individens rättigheter och säkerställande av hur molnleverantörerna får och inte får agera. Faktum är dock att de juridiska aspekterna är

värda att diskutera, förhindrar de en utveckling inom IT som hade kunnat förbättra samhället i sin helhet som ett resultat av fördelarna med molntjänster. Eller säkerställer de juridiska aspekterna individer och organisationers rättigheter.

7.2 Metodval

Denna studie undersökte ämnesområdet genom att intervjua individer med kunskap och erfarenhet kring molnet. Arbetet utfördes som en fallstudie med semistrukturerade intervjuer och kvalitativ data eftersöktes. Inringandet av fallet hade kunnat utföras bättre och på ett tydligare sätt, fallet som studien bygger på konstruerades på ett antal faktorer. Ett förslag hade legat mer i linje med ett tydligt område hade varit att fokusera på en avgränsad grupp, exempelvis ur ett organisatoriskt eller dylikt sammanhang. Det hade varit intressant att möjligen undersöka kontraster mellan den privata och offentliga sektorn, då tolkningen kring hur restriktiva aktörerna är med data möjligen hade kunnat skilja sig. Ett annat scenario hade varit att fokusera på en valfri organisation och utgå från dess storlek för att se om IT-kapacitet hade haft en påverkan på viljan och förtroende att etablera IT i molnet eller snarare hade resulterat i införandet av egen lokal IT.

7.3 Etiska aspekter

Resultat vid sammanställning av inhämtade data från respondenterna pekade på olika aspekter som kan bidra till att förtydliga hur konsumentens förtroende upplevs i relation till leverantörens förmåga att bibehålla säkerhet. Således skulle denna data kunna tolkas vara känslig i den mån att denna studie sammanställer informationen, vilket bidrar till att bygga en bild av hur konsumenten egentligen förlitar sig till en molnleverantören. Detta är en faktor som skulle kunna leda till uppkomsten av en bild, som riskerar att missgynna de aktörer som inte möter de kriterier som listats i denna studie. Exempelvis har många av respondenterna uttryckt sig på ett sätt som leder till att mindre aktörer skulle kunna tolkas vara sämre ur ett säkerhetsperspektiv, studien skulle därför indirekt genom sitt resultat kunna missgynna mindre leverantörer, vilka troligen redan har det problematiskt konkurrensmässigt i jämförelse med de amerikanska jättarna på marknaden.

Vid det metodologiska utförande har även andra typer etiska aspekter behövts hanteras relaterat närmare till själva studien. Primärdata hämtats från respondenter som kvalificerats inom ramen av de kritiker som kategoriserat denna fallstudie. Syftet att besvara arbetets forskningsfråga har framförallt lett till att kvalitativ data eftersökts, denna information har insamlats genom semistrukturerade intervjuer. Resultat har blivit mängder med data som skulle kunna kvalificeras som personuppgifter. Därför har den inhämtade information behövts hanteras varsam och konfidentiellt, uppgifter som kunnat kopplas till individer som deltagit i studien har anonymiserats och har hanterats med försiktighet vid denna undersökning.

Samtliga deltagare har informerats om de etiska principer som efterföljts under detta arbete, de har därmed garanterats anonymitet, fått vetskap om fritt deltagande och har haft rätt till en insyn av den data som samlats ihop från den egna intervjun. Deltagarna

informerades om de etiska faktorerna som arbetet stödjer sig på innan intervjuerna utfördes, vilket bland annat handlade om att säkerställa rätten till inspelning, transkribering och att använda data till arbetets syfte. Intervjudeltagare informerades även om bakgrunden till arbetet för att kunna ge respondenterna transparens för vad den faktiska studien ämnade undersöka. Efter intervjuerna har det inspelade materialet transkriberats, därefter skickades resultatet till respondenterna som därmed fått chans att återkomma med eventuella synpunkter. Data har efter denna process lagrats på ett säkert sätt, när arbetet färdigställts kommer de sista kontaktuppgifterna att avlägsnas för att säkerställa att inte några personuppgifter kommer att felbehandlas.

7.4 Kritik

Förtroende är ett återkommande uttryck som uppkommer i relation till forskning om molntjänster och är relativt diffust att specificera. Ett ytligt försök att kategorisera termen gjordes i denna studie och syftade till att definiera förtroende i den mån av IT-säkerhet, vilket innebär skydd mot angrepp och bevarad tillgänglighet av levererade tjänster. Säkerhetsproblematiken och olika angreppsvektorer som lyfts upp har försökt kategoriseras efter CIA triaden och tillsammans ur ett förtroendeperspektiv undersöka uppfattning av molnkonsumtens upplevda relation till molnleverantören. Studien skulle således kunna kritiseras för att undersöka ett relativt brett område i väldigt generella termer. Ett starkare argument hade kunnat byggas genom att möjligen kategorisera begreppet förtroende ytterliga och därmed försöka rama in den problematik eller den faktor som ämnas undersökas ytterligare. Som tidigare diskuterat i kapitel 7.2 skulle även en annan metodologiskt ansats kunnat vara intressant och också bidragit till att bättre kategorisera studien till en specifikare avgränsning.

Slutligen bör det konstateras att de finns studier som undersöker förtroende och molntjänster, ofta försöker dessa att bygga Förtroendemodeller för hur konsumentens ska kunna lita på tjänsten, förtroende och molnet är alltså inget nytt forskningsområde. Till studiens försvar kan möjligen frågans relevans strykas i grunden av den utveckling som kunnat konstateras, bruket av molntjänster ökar stadigt. Därmed blir frågan relevant då molntjänster, juridik och IT är fenomen som ständigt förändras, vilket bidrar till att nya frågor uppkommer kring området.

7.5 Förslag på framtida forskningsområden

Molnkonsumentens förtroende till molnleverantören är av största vikt och skulle kunna ses som en del av den affärsmässiga relationen mellan de båda parterna. Därför bör de faktorer som molnkonsumenterna tar i beaktande tolkas som viktiga argument ur ett konkurrensperspektiv, det aspekter som diskuterats i denna studie kan möjligen vara påverkande vid konsumentens val av molnleverantör. Framtida forskning skulle kunna undersöka hur denna relation ser ut på ett djupare plan, är de förtroendeingivande faktorerna viktiga vid valet av leverantör eller ser konsumenten snarare till prestanda än säkerhet. En annan kategori som diskuterats i denna studie är de juridiska aspekter som ofta pekade på diverse komplikationer med molntjänster. Problematik identifierades

alltså inte kring tekniska eller funktionella aspekter, de största problemen som identifierades i denna studie hade med lokalisering, lagar och regler att göra. Molnkonsumenten är i högre grad orolig för vem som äger tillgång till data än att en elaksinnad aktör skulle göra ett intrång hos en molnleverantör. Därför finns en möjlighet för framtida forskning att fokusera på juridik och frågor som berör tillgång till data av tredje part, då dessa faktorer är sådant som molnkonsumenten och organisationer oroar sig för. Slutligen bör det konstateras att denna studie fokuserat på molntjänster i sin helhet, förtroendet skulle kunna variera mellan olika typer av tjänstemodeller, vid studiens analys identifierades små indikationer på detta. SaaS tjänster upplevdes som mer säkrade mot multi-tenancy svagheter än andra typer av tjänstemodeller. Således skulle framtida arbeten inom områden kunna fokusera på en viss typ av tjänstemodell.

8 Slutsats

I denna studie undersöktes molnkonsumtens förtroende till molnleverantören. Förtroende är en viktig del mellan de olika parterna, konsumenten tilldelar per automatik en stor del av tidigare egen kontroll till leverantören som ett resultat vid etablering av IT i molnet. Därför är det viktigt att bygga en förståelse för hur förtroendet påverkas i molnmiljöer av olika faktorer relaterade till diverse säkerhetsrisker relaterade till molnet. För att bygga en uppfattning om förtroendet ur ett säkerhetsperspektiv så intervjuades individer med erfarenhet inom IT-branschen som besatt kunskap kopplad till molntjänster. Resultatet pekade på att konsumenten trots de påtagliga riskerna med molntjänster hade ett högt förtroende till att etablera IT via en molnleverantör. Konsumenten hade en förståelse för de eventuella riskerna med molntjänster, men ansåg i stora drag att komplikationerna med att konstruera ett eget alternativ ofta övervägdes av fördelarna med att kunna vända sig till en leverantör. Molntjänster uppfattades således som ett förtroendeingivande alternativ till en egen lokal IT speciellt i de fall då inte egen kapacitet fanns. Större molnleverantörer hade ett starkare förtroende, eftersom storlek ansågs tala för ökad kapacitet, dessa aktörer erbjöd även enligt konsumenten bra leveransavtal till grunden, vilket konstaterades fördelaktigt. Problematik i frågan identifierades snarare vara kopplat till juridiska och geografiska aspekter. Användaren av en molntjänst oroar sig ofta för hur molnleverantören delar dess data, juridik kan tvinga molnleverantören att lämna ut konsumentdata till tredje part. Resultatet visade alltså på att organisationer trots upplevelsen av ett högt förtroende och god uppfattning kring eventuella fördelar med molntjänsten, kan tvingas att välja andra IT alternativ än molnet på grund av lagar och regler.

Referenser

Alashhab, Z. R., Anbar M., Singh, M. M., Leau, Y., Al-Sai, Z. A. & Alhayja'a, S. A. (2021). Impact of coronavirus pandemic crisis on technologies and cloud computing applications. *Journal of Electronic Science and Technology*, 19(1), ss. 1-12. https://doi.org/10.1016/j.jnlest.2020.100059

Alvehus, J. (2019). *Skriva uppsats med kvalitativ metod: en handbok*. 2. Uppl., Stockholm:Liber

Al-Nassar, B. A., Al-Nsour, S. N. & Rababah, K. A. (2021). Advantages and Factors Affecting the Adoption of Cloud Computing. *ICSIE 2021: 10th International Conference on Software and Information Engineering.* Kairo, Egypten 12-14 November 2021, ss. 55-56. https://doi-org.libraryproxy.his.se/10.1145/3512716.3512726

Bryman, A. (2018). *Samhällsvetenskapliga metoder*. 3. Uppl., Stockholm:Liber

Carvalho, C. A. B. d., Andrade, R. M. d. C., Castro, M. F. d., Coutinho, E. M. & Agoulmine, N. (2017). State of the art and challenges of security SLA for cloud computing. *Computers and Electrical Engineering*, 59, ss. 141-152. http://dx.doi.org/10.1016/j.compeleceng.2016.12.030

Coppolino, L., D'Antonia, S., Mazzeo, G. & Romano, L. (2017). Cloud security: Emerging threats and current Solutions. *Computer and Electrical Engineering*, 59, ss. 126-140. https://doi.org/10.1016/j.compeleceng.2016.03.004

Díaz de León Guillén, M. Á., Morales-Rocha V. & Fernández Martínez, L. F. (2020). A systematic review of security threats and countermeasures in SaaS*. Journal of Computer Security*, 28(6), ss. 635-653. https://doi.org/10.3233/JCS-200002

Eriksson, L. T. & Wiedersheim-Paul, F. (2014) *Att utreda, forska och rapportera*. 10. uppl., Stockholm:Liber.

Fisher, C. (2018). Cloud versus On-Premise Computing. *American Journal of Industrial and Business Management*, 8(9), ss. 1996-2006. https://doi.org/10.4236/ajibm.2018.89133

Högskolan i Skövde. (2020). *Riktlinjer för behandling av personuppgifter i forskningsprojekt och examens- och studentarbeten.* ss. 1-5.

Kelly, C., Pitropakis, N., Mylonas, A., McKeown, S. & Buchanan, W. J. (2021). A Comparative Analysis of Honeypots on Different Cloud Platforms. *Sensors,* 21(7), s. 2433. https://doi.org/10.3390/s21072433

Muralidharan, C. & Anitha, R. (2021). Risk analysis of cloud service providers by analyzing the frequency of occurrence of problems using E-Eclat algorithm. *Wireless Networks: The Journal of Mobile Communication, Computation and Information,* 27(8), ss. 5587-5595. https://doi.org/10.1007/s11276-019-02191-4

Rotenberg, M. (2020). Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection. *European Law journal*, 25(1-2), ss. 141-152. https://doi.org/10.1111/eulj.12370

Sherman, A. T., DeLatte, D., Neary, M., Oliva, L., Dhananjay, P., Scheponik, T., Herman, G. L. & Thompson, J. (2018). Cybersecurity: Exploring core concepts through six scenarios. *Cryptologia*, 42(4), ss. 337-377. https://doi.org/10.1080/01611194.2017.1362063

Subramanian, N & Jeyaraj A. (2018). Recent security challenges in cloud computing. *Computers and Electrical Engineering*, 71, ss. 28-42. https://doi.org/10.1016/j.compeleceng.2018.06.006

Tabrizchi, H & Kuchaki, M. R. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *Journal of Supercomputing*, 76(12), ss. 9493-9532. https://doi.org/10.1007/s11227-020-03213-1

Tracol, X. (2020). "Schrems II": The return of the Privacy Shield. *Computer Law & Security Review*, 39, ss. 1-11. https://doi.org/10.1016/j.clsr.2020.105484

Van der Werff, L., Fox, G., Masevic, I., Emeakaroha, C, V., Morrison, P, J. & Lynn, T. (2019). Building consumer trust in the cloud: an experimental analysis of the cloud trust label approach. *Journal of Cloud Computing: Advances, Systems and Applications*, 8(6), ss. 1-17. https://doi.org/10.1186/s13677-019-0129-8

Yan, L., Hao, X., Cheng, Z. & Zhou, R. (2018). Cloud Computing Security and Privacy. *ICBDC '18 Proceedings of the 2018 International Conference on Big Data and Computing*, Shenzhen, Kina 28-30 April 2018, ss. 119-123. https://doi.org/10.1145/3220199.3220217

Wagemann, J., Siemen, S., Seeger, B. & Bendix, J. (2021). A user perspective on future cloud-based services for Big Earth data. *International Journal of Digital Earth*, 14(12), ss. 1758-1774. https://doi.org/10.1080/17538947.2021.1982031

Winkler, J. T. & Brown, V. C. (2013). Horizontal Allocation of Decision Rights for On-Premise Applications and Software-as-a-Service. *Journal of Management Information Systems*, 30(3), ss. 13-48. http://doi.org/10.2753/MIS0742-1222300302

Ziani, A. & Medouri, A. (2018). Risks and Security Requirements for Cloud Environments. *SCA '18: Proceedings of the 3rd International Conference on Smart City Applications*, Tetouan, Marocko 10-11 Oktober 2018, ss. 1-6. https://doi.org/10.1145/3286606.3286865