LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Huvudet bland molnen eller fötterna på jorden?

En studie om användares säkerhetsmedvetenhet gällande molnlagring

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Evelina Larzon
Cecilia Nilsson

Handledare: Miranda Kajtazi

Examinatorer: Anders Svensson
Nicklas Holmberg

Huvudet bland molnen eller fötterna på jorden: En studie om användares säkerhetsmedvetenhet gällande molnlagring

Författare: Evelina Larzon, Cecilia Nilsson

Utgivare: Inst. för informatik, Ekonomihögskolan, Lunds universitet

Framlagd: Vårterminen 2018

Dokumenttyp: Kandidatuppsats

Antal sidor: 48

Nyckelord: cloud computing, molnlagring, informationssäkerhet, dataintrång, säkerhetsmedvetenhet

Sammanfattning (Max. 200 ord):
Med molnlagring kommer många fördelar såsom möjligheten till back-up och att användaren kan komma åt sina filer oberoende av plats. Det finns även flertalet säkerhetsrisker med molnlagringstjänster vilket kan äventyra informationssäkerheten. På senare tid har flera attacker mot molnlagringstjänster ägt rum, samtidigt som antalet användare ökar. I denna uppsats har det genom en enkätundersökning studerats hur medvetna användarna är om dessa säkerhetsrisker och om de på något sätt tagit dessa i beaktande i sin användning. I resultatet framkom att många använder molnlagringstjänster och nästan alla känner till minst en risk. Få användare känner till många risker och endast en liten andel vidtar motåtgärder mot riskerna. Slutsatserna blir att användare väljer att använda molnlagringstjänster trots att de känner till riskerna. De användare som vidtar motåtgärder känner också till fler risker än de som inte vidtar motåtgärder. Det finns heller inget samband mellan ett högt säkerhetsmedvetande och valet att inte använda molnlagringstjänster, utan det beror snarare på ointresse.

Innehåll

Figurer

Tabeller

1 Introduktion

I detta kapitel ges en bakgrund till uppsatsämnet och vilket problemområde som finns. Detta resulterar i en forskningsfråga samt syftet med att undersöka denna. Slutligen presenteras de avgränsningar som har gjorts.

1.1 Bakgrund

De senaste fem åren har antalet användare av molntjänster ökat med ungefär 50 procent (Juniper Research, 2018). En molntjänst är en service som erbjuder till exempel datalagring och körning av program. Framförallt syftar molntjänster till att ersätta tjänster som tidigare skulle ha utförts på en lokal dator eller i ett lokalt nätverk (Mell & Grance, 2011). Enligt Junipers (2018) uppskattningar var antalet konsumenter av molnbaserade tjänster i världen 2013 2.4 miljarder. I år beräknas det antalet ha stigit till 3.6 miljarder (Juniper Research, 2018). Även de resurser som läggs på att utveckla cloud computing har ökat och enligt IDC (2017) utgör molntjänster en tredjedel av alla investeringar som läggs på IT globalt.

För privatpersoner är ett vanligt användningsområde för molntjänster lagring av filer och information. Några av de mest använda molnlagringstjänsterna är Dropbox, Google Drive samt iCloud. 2016 hade Dropbox en halv miljard användare (Dropbox, 2016) medan Google Drive samt iCloud hade cirka 800 miljoner användare i mars 2017 (AppleInsider, 2016; Popper, 2017). Det finns många fördelar med att lagra filer och information i molnet såsom automatisk synkronisering, backup samt att informationen kan nås från olika enheter, oberoende av plats. Men att lagra information i molnet medför vissa säkerhetsrisker.

Risker med molnlagring kan till exempel vara att tjänsten utsätts för attacker av olika slag. Det kan vara attacker som minskar tillgängligheten för tjänsten genom att den blir långsam eller går ner av överbelastning. Det kan också vara känslig data som användaren har laddat upp som läcker vilket gör att konfidentialiteten försämras. Det kan även finnas problem med integriteten vilket kan yttra sig genom att en angripare kommer åt tjänsten och manipulerar användarens data.

Därmed hamnar informationssäkerhet i fokus även för användare. De senaste åren har flera tjänster online blivit hackade eller attackerade på annat sätt. Till exempel utsattes Gmail för en omfattande phishing-attack i maj 2017 som gick ut till en miljard användare (Johnson, 2017). Angriparna skickade ut ett mail från en användare som liknade användare som brukade skicka mail till dem (Johnson, 2017). Mailet innehöll en falsk inbjudan till ett Google Docs dokument, vilket lurade användarna att klicka på en skadlig länk. Därmed fick angriparna tillgång till användarnas konton (Johnson, 2017). Dropbox utsattes 2016 för en dataläcka där ett stort antal lösenord från 2012 hade kommit ut (Campanello, 2016). Dropbox skickade då ut ett mail till sina användare och uppmanade dem att byta lösenord (Campanello, 2016). Även

Apples molnlagringstjänst iCloud har blivit utsatt, 2017 kom en hackergrupp över inloggningsuppgifter till cirka 250 miljoner konton via tredjepartsprogram (Whittaker, 2017). Angriparna hotade med att radera all data på kontona om inte Apple betalade ut en lösensumma till hackergruppen (Whittaker, 2017).

Trots riskerna ökar användandet vilket gör att man ställer sig frågan om användare ens är medvetna om dem. Det kan även vara så att användare tycker sig vara bekymrade över sin privata data online men genom observationer har det fastställts att de inte efterlever detta (Coopamootoo & Groß, 2014). En möjlig anledning till detta är att internet gör gränsen mellan vad som är publikt och privat suddig, vilket i sin tur medför att det blir svårt för användare att fatta beslut angående sin privata data (Coopamootoo & Groß, 2014).

Vid användandet av en molnlagringstjänst krävs det att användaren tillgodogör sig information om vilken data som delas till vem och på vilket sätt, vem som äger informationen samt förstår vad det innebär att dela med sig av personlig information (Coopamootoo & Groß, 2014). Även om detta krävs är det tveksamt om detta sker vid användning av molnlagringstjänster då det är en komplex miljö som kan vara ovan för många användare.

I denna uppsats har molnlagring och dess aspekter lett oss till att definiera problemområdet som i sin tur mynnat ut i en forskningsfråga. I avsnittet syfte presenteras varför denna studie är viktig att genomföra. Resultatet av dessa delar har sedan lett oss till de avgränsningar vi valt att göra för att definiera uppsatsens ramar. Följande delar är därmed presenterade i denna ordning.

1.2 Problemområde

Cloud computing har studerats tidigare, framförallt med ett tekniskt fokus på hur molnet fungerar och hur arkitekturen är uppbyggd (Aguiar, Zhang, & Blanton, 2014; Ahmad, 2017; Alani, 2016; Ali, Khan, & Vasilakos, 2015; Fernandes, Soares, Gomes, Freire, & Inácio, 2014; Galibus, Krasnoproshin, Oliveira Albuquerque, & Freitas, 2016; Kulkarni et al., 2012; Singh & Chatterjee, 2017).

Det finns även forskning på vilka säkerhetsrisker och utmaningar som molntjänster medför (Aguiar et al., 2014; Ahmad, 2017; Ahuja & Komathukattil, 2012; Fernandes et al., 2014; Galibus et al., 2016; Jathanna & Jagli, 2017; Kumar Sharma et al., 2017; Patil, Pandey, & Bhole, 2017; Singh & Chatterjee, 2017; Zhou, Zhang, Xie, Qian, & Zhou, 2010). Exempelvis ger en sökning i LUBSearch på “Cloud computing security” över 45 000 träffar.

En typ av molntjänst som framförallt är relevant för användare är lagring för filer och information. Men för att kunna använda sig av molnlagringstjänster krävs en uppkoppling mot internet vilket för användare kan innebära en otrygg miljö med ett ökat antal säkerhetsrisker. Allt från vilken fysisk enhet som används till tjänsteleverantörens arkitektur påverkar vilka risker som finns närvarande. Trots detta ökar antalet användare av molntjänster vilket kan leda till ett ifrågasättande om användare är medvetna om dessa säkerhetsrisker.

Att välja en molnlagringstjänst kan vara komplicerat för användare på grund av att det finns ett stort urval av tjänster. De kanske heller inte förstår fullt ut vad användandet av molnlagring innebär, hur applikationen i sig fungerar samt att det finns säkerhetsrisker att ta hänsyn till.

För att addera till tidigare forskning skulle användares säkerhetsmedvetande specifikt för molnlagringtjänster vara intressant att studera, då det täcker in ytterligare ett användningsområde som blir allt vanligare i samhället.

1.3 Forskningsfråga

Vilka risker med molnlagringstjänster påverkar säkerhetsmedvetandet hos användare?

1.4 Syfte

Vår uppsats syftar till att fastställa användares kunskap om säkerhetsrisker med molnlagring samt få förståelse för hur de resonerar genom en kvantitativ enkätundersökning. Därmed vill vi studera privata användares nyttjande av molnlagringstjänster, hur medvetna de är om säkerhetsrisker med molnlagring samt huruvida de vidtar motåtgärder mot dessa risker. Detta innefattar hur användare ställer sig till tjänster som hanterar personlig information och om de tar eget ansvar över sin data online.

1.5 Avgränsningar

Vi har valt att avgränsa studien till privatpersoners användande av molnlagringstjänster och utesluter därmed organisationers användande av nämnda tjänster. Vi tar ej upp konsekvenser av risker eller lösningar på säkerhetsproblem då detta inte faller inom ramen för studien.

Med molnlagringstjänst menar vi en tjänst som används för att ladda upp filer eller information för fillagring, fildelning och säkerhetskopiering som kan kommas åt oberoende av plats. Exempel på sådana tjänster är Google Drive och Dropbox. Alltså ingår inte mailtjänster i denna definition eftersom dessa tjänsters primära användningsområde är kommunikation och inte fillagring.

Gällande säkerhetsrisker har vissa avgränsningar gjorts, framförallt diskuteras inte nätverksspecifika risker. Användares val av webbläsare samt fysiska enheter kan också medföra säkerhetsrisker men inte heller dessa står i fokus i denna studie och har därför uteslutits.

Trots att denna uppsats endast fokuserar på molnlagringstjänster finns konkurrerande infrastrukturer såsom Internet of Things (IoT) som också ger möjligheter för datalagring i olika format och genom olika arkitekturer (Gubbi, Buyya, Marusic, & Palaniswami, 2013; Khan, Khan, Zaheer, & Khan, 2012). Eftersom denna studie går bortom dessa infrastrukturer har de blivit exkluderade från denna uppsats.

2 Teoretiskt ramverk

I detta kapitel ges en genomgång av tidigare forskning som är relevant för att besvara forskningsfrågan. Kapitlet är uppdelat i underrubrikerna Vad är cloud computing, Molnlagring, Informationssäkerhet, Risker med molntjänster samt Medvetenhet.

Cloud computing är en teknologi som möjliggör för användarna att nyttja tjänster som tidigare varit lokala, kan nu användas oberoende av plats. Cloud computing består av olika typer av tjänster där en typ av tjänst är molnlagring. Molnlagring används både av organisationer och privata användare för att lagra filer eller information på ett lättillgängligt sätt. I och med att data lagras virtuellt istället för fysiskt och att ansvaret läggs på en tjänsteleverantör medför det säkerhetsrisker. Dessa risker kan uppstå på grund av att molntjänstens arkitektur delas mellan olika tjänsteleverantörer som lagrar användares data i samma moln, vilket kallas multitenancy. Andra risker inkluderar dataintrång och attacker på molntjänster. Därmed blir informationssäkerhet ett relevant område för molnlagring. Framförallt äventyras de tre grundstenarna inom informationssäkerhet (konfidentialitet, integritet och tillgänglighet) genom användandet av cloud computing som teknologi.

Inom tidigare forskning har cloud computing i flera fall studerats från ett informationssäkerhetsperspektiv. Ahmad (2017) har undersökt den underliggande teknologin till cloud computing, de nuvarande säkerhetshoten inom området samt lösningar på dem. Aguiar et al. (2014) har beskrivit attacker som drabbat tjänsteleverantörer, motåtgärder och skyddsmekanismer för att förbättra integriteten för användare. Ahuja och Komathukattil (2012) har också beskrivit säkerhetshot och risker med molnet samt hur dessa kan hanteras.

Eftersom den data som riskeras, i och med användandet av molnlagringstjänster, tillhör användare kan deras medvetenhet om dessa risker analyseras. Till exempel skriver Coopamootoo och Groß (2014) i en artikel att användare har svårare att fatta beslut online eftersom det kräver ett mer komplext beslutsfattande.

Sammanfattningsvis presenteras nedan i teorin en definition samt förklaring till cloud computing, molnlagring samt säkerhetsrisker klassas enligt informationssäkerhet för att sedan beskrivas. Avslutningsvis presenteras även tidigare forskning gällande användares medvetenhet inom närliggande informationssäkerhetsområden.

2.1 Vad är cloud computing?

Enligt National Institute of Standards and Technology (NIST) definieras cloud computing som en modell för att ge tillgång till en delad pool av konfigurerbara datoriserade resurser, såsom nätverk, server, lagring, applikationer och tjänster, via ett nätverk som alltid finns tillgängliga när behovet för användande av dem uppstår (Mell & Grance, 2011).

Visionen om cloud computing uppstod på 1960-talet då J.C.R Licklider presenterade ett koncept om *intergalactic computer network* som har likheter med dagens internet (Mohamed, 2009). Även John McCarthy var inne på samma spår när han i ett tal på MIT förespråkade att man i framtiden skulle kunna sälja “computer power” genom en utility business model (Alani, 2016).

Begreppet som sådant nämndes för första gången 1996 i ett internt dokument hos företaget Compaq när man gjorde en vision för hur framtidens internet business skulle se ut (Regalado, 2011). Detta följdes av Amazon som 2006 marknadsförde en tjänst som cloud computing (Mohamed, 2009). 2009 introducerade Google sitt koncept Google Apps, numera kallat G Suite, med tjänster som Gmail och Google Calendar som sedan utökades efter hand (Alani, 2016). 2012 lades tjänsten Google Drive till som är deras plattform för att lagra filer och dela dem mellan användare (Johnston, 2012).

För att möjliggöra cloud computing används teknologin för virtuell arkitektur och följer strukturen för en virtuell servermodell (Alani, 2016). Den virtuella servermodellen inkluderar en fysisk server som har ett server-operativsystem som är värd åt ett flertal virtual machines (VM). Varje VM har i sin tur ett gäst-operativsystem samt en eller flera applikationer (Alani, 2016).

Arkitekturen för cloud computing kan delas in i flera lager. Det nedersta lagret är hårdvaran för servrarna, sedan finns ett abstraktionslager som sträcker sig över flera fysiska enheter och hanterar alla VM dynamiskt (Alani, 2016). Över abstraktionslagret finns tre olika servicemodeller, nämligen Infrastructure as a Service (IaaS), Platform as a Service (PaaS) samt Software as a Service (SaaS) (Alani, 2016).

2.1.1 Servicemodeller

Infrastructure as a Service innebär att kunder får tillgång till hela infrastrukturen via internet genom tjänsten (Sinjilawi, Al-Nabhan, & Abu-Shanab, 2014) där kunden själv kan installera operativsystem samt applikationer (Alani, 2016). Detta är den miniminivå av service som ges till kunden, då den endast betalar för tillhandahållandet av fysisk hårdvara (Alani, 2016). Vidare innebär detta att kunden själv ansvarar för all säkerhet från operativsystemet och uppåt (Alani, 2016). Exempel på tjänster som IaaS-leverantörer erbjuder är messaging queues och databaser (Jathanna & Jagli, 2017).

Platform as a Service innebär att kunden får tillgång till en plattform för utveckling, testning och implementering (Sinjilawi et al., 2014) och att verktyg som krävs för detta, exempelvis en kompilator, redan finns installerat på plattformen (Alani, 2016). Tjänsteleverantören ansvarar för att tillhandahålla och underhålla infrastrukturen samt hanterar all säkerhet gällande detta (Alani, 2016). PaaS-tjänster kan användas till att utveckla applikationer med samma egenskaper som finns i molnet, såsom skalbarhet, tillgänglighet samt möjliggör implementering av SaaS (Jathanna & Jagli, 2017).

Software as a Service lägger all kontroll på tjänsteleverantören som får ansvara för säkerhet, uppdatering och underhåll av tjänsten (Sinjilawi et al., 2014) och användaren har endast tillgång till tjänsten via en tunn klients gränssnitt (Alani, 2016). Detta medför att kunden endast behöver fokusera på att använda tjänsten och hantera den tillgängliga funktionaliteten i gränssnittet (Alani, 2016). Exempel på SaaS-tjänster är mailapplikationer eller applikationer för samarbete, oftast via ett webbläsarbaserat gränssnitt (Jathanna & Jagli, 2017).

Utöver att klassificera en molntjänst efter servicemodell finns det flera olika deployment-modeller som kan användas för att kategorisera molntjänsten. De fyra vanligaste är public, private, community och hybrid cloud (Alani, 2016).

2.1.2 Deployment-modeller

Public cloud kan definieras som en molntjänst som är tillgänglig för allmänheten (Alani, 2016). Det ägs och hanteras av en molntjänstleverantör såsom Microsoft eller Google. Publikt moln är den vanligaste deployment-modellen och det är tjänsteleverantören som ansvarar för infrastruktur och säkerhet (Jathanna & Jagli, 2017).

Private cloud är en molntjänst som används av en enskild organisation och enbart tillåter auktoriserade användare (Alani, 2016). Många företag föredrar att använda sig av ett privat moln för att de har bättre kontroll över tjänsteleveranssystemet. Det är vanligt bland till exempel banker och myndigheter att använda sig av ett privat moln (Alani, 2016).

Community cloud är ett delat moln mellan olika organisationer som har gemensamma intressen (Jathanna & Jagli, 2017). Det ägs vanligen av en eller flera av organisationerna eller ibland av en tredje part.

Hybrid cloud är en kombination av publikt, privat och community moln. Syftet med att blanda deployment-modeller är att öka portabiliteten (Alani, 2016).

Sammanfattningsvis är cloud computing en modell för tillgängliga tjänster som tillhandahålls via internet och ger användaren möjlighet att till exempel lagra data eller maila. En molntjänst kan delas upp i två olika kategorier, enligt servicemodell där nivån av service från tjänsteleverantören avgör och enligt deployment-modell där den som äger molnet avgör.

2.2 Molnlagring

Molnlagring innefattar lagringstjänster som tillhandahålls via ett moln online. Det kan innehålla fillagring i form av arkivering samt back-up men även webbaserade operativsystem eller databaser (Aguiar et al., 2014). Lagring av data i molnet tillhandahålls genom tjänster där en användare eller organisation kan köpa lagringsutrymme för sin data. Detta gör att användaren inte själv behöver ha arkitekturen för lagring lokalt utan får tillgång till lagringsutrymme via internet genom en molnlagringstjänst (Aguiar et al., 2014). Molnlagringstjänster presenteras för användaren genom ett grafiskt gränssnitt, låter tjänsteleverantören ansvara för tillgång till och underhåll av infrastruktur samt hårdvara (Aguiar et al., 2014). Därmed kan en molnlagringstjänst som den erbjuds till privata användare ses som en SaaS.

Ett exempel på en molnlagringstjänst är Google Drive som kan användas till att lagra filer i flera format, såsom textfiler, foton samt PDF (Johnston, 2012). Drive inkluderar också Google Docs som är ett ordbehandlingsprogram online. Google Drive underhålls av Google och medföljande säkerhet är kryptering av dataöverföring mellan servrar samt webbläsare. Data replikeras på olika datacenter vilket innebär att det finns minst en back-up, tillgänglighet till tjänsten garanteras till 99.9% av tiden samt support finns tillgänglig dygnet runt. Om lagringsutrymmet tar slut kan man köpa mer (Johnston, 2012). Exempel på andra molnlagringstjänster är Amazon Drive, Dropbox, OneDrive samt Apple iCloud.

Tidigare har all lagring skett lokalt men det pågår en övergång just nu där organisationer flyttar sina tjänster och sin datalagring till molnet. Denna övergång bromsas av att organisationer och användare inte litar på det publika molnet samt hanteringen av personlig data (Aguiar et

al., 2014). Ur ett säkerhetsperspektiv innebär användandet av en molnlagringstjänst förlorad kontroll över data eftersom den är outsourcad vilket riskerar användarens dataintegritet (Aguiar et al., 2014).

2.3 Informationssäkerhet

Grundstenarna inom informationssäkerhet kan sammanfattas enligt akronymen CIA som står för Confidentiality (konfidentialitet), Integrity (integritet) och Availability (tillgänglighet) (Galibus et al., 2016; Gollmann, 2011; Singh & Chatterjee, 2017; Sinjilawi et al., 2014).

Konfidentialitet innebär att data och information enbart kan tillgängliggöras av auktoriserade användare (Sinjilawi et al., 2014). Obehöriga ska alltså inte ha tillgång till känslig eller privat data. Konfidentialitet inom organisationer benämns som *secrecy* och för privatpersoner som *privacy* (Gollmann, 2011).

Integritet ser till att data bibehåller sin fullständighet och exakthet (Gollmann, 2011). Data ska alltså skyddas från att ändras obehörigt. Inom begreppet ingår det även att möjliggöra total återställning när en auktoriserad användare har gjort ett misstag som riskerar att förstöra data (Gollmann, 2011).

Tillgänglighet innebär att tjänsten som tillhandahåller data ska finnas tillgänglig (Gollmann, 2011). Det innebär att systemet ska skyddas från skadliga attacker, DoS-attack (Denial of Service), som skulle medföra att auktoriserade användare nekas tillgång till tjänsten.

2.4 Risker med molntjänster

Nedan presenteras de säkerhetsrisker för molntjänster vi har funnit i litteraturgenomgången. För varje risk klassificerar vi vilken eller vilka av de tre grundstenarna inom informationssäkerhet som risken är relevant för. Nedanför tabellen finns det även en beskrivning av varje säkerhetsrisk.

Tabell 2.1 Sammanställning av risker

	Konfidentialitet	Integritet	Tillgänglighet	Referenser
Dataintrång	x	x		Ahmad (2017), Alani (2016), CSA (2016), Galibus et al. (2016), Jathanna & Jagli (2017), Kumar Sharma et al. (2017), Patil, Pandey & Bhole (2017), Singh & Chatterjee (2017), Sinjilawi et al. (2014), Tari et al. (2015)
DoS-attack			x	Ahmad (2017), Ahuja & Komathukattil (2012), Alani (2016), CSA (2016), Galibus et al. (2016), Jathanna & Jagli (2017), Kumar Sharma et al. (2017), Singh & Chatterjee (2017), Sinjilawi et al. (2014),
Exponerade sårbarheter pga multi-tenancy	x	x		Ahuja & Komathukattil (2012), Alani (2016), Ali et al. (2015), CSA (2016), Galibus et al. (2016), Jathanna & Jagli (2017), Kumar Sharma et al. (2017), Patil et al. (2017), Singh & Chatterjee (2017), Sinjilawi et al. (2014)
Hackade gränssnitt och APIer	x	x	x	Ahmad (2017), Ahuja & Komathukattil (2012), Alani (2016), Ali et al. (2015), CSA (2016), Galibus et al. (2016), Jathanna & Jagli (2017), Singh & Chatterjee (2017)
Svag eller okrypterad data	x			Kumar Sharma et al. (2017), Sinjilawi et al. (2014)
Minskad kontroll samt inkomplett radering av data	x			Aguiar et al. (2014), Ahmad (2017), Ahuja & Komathukattil (2012), Alani (2016), Ali et al. (2015), Fernandes et al. (2015), Galibus et al. (2016), Kumar Sharma et al. (2017), Singh & Chatterjee (2017), Sinjilawi et al. (2014), Tari et al. (2015)
SQL-injektioner	x	x		Ali et al. (2015), Jathanna & Jagli (2017), Kumar Sharma et al. (2017), Sinjilawi et al. (2014)
Malicious insiders	x	x	x	Ahuja & Komathukattil (2012), Alani (2016), CSA (2016), Galibus et al. (2016), Singh & Chatterjee (2017)
Stulen identitet genom phishing	x	x		Alani (2016), James, Nottingham & Kim (2013), Singh & Chatterjee (2017)

2.4.1 Beskrivningar av risker

Dataintrång

Risken för dataintrång hos tjänsteleverantörer finns på grund av att data sparas på molnservrar och att de anses som attraktiva mål (CSA, 2016; Galibus et al., 2016; Jathanna & Jagli, 2017). Dataläckor uppstår som en följd av dataintrång eller attacker (Galibus et al., 2016; Jathanna & Jagli, 2017) vilket innebär att personlig data hamnar i olaga händer som därefter kan förvrängas eller raderas (Alani, 2016; Singh & Chatterjee, 2017). Även enskilda konton eller hela molntjänsten riskerar att kapas av obehöriga vilket medför att angriparna kan se alla aktiviteter, manipulera transaktioner och ändra data (Alani, 2016; Galibus et al., 2016; Jathanna & Jagli, 2017; Singh & Chatterjee, 2017). Därmed riskeras både konfidentialitet samt integritet.

DoS-attack

Genom en överbelastningsattack av resurser påverkas tillgängligheten till molntjänsten. Systemet kan då gå långsamt eller resultera i att användarna inte kommer åt tjänsten alls (Galibus et al., 2016; Jathanna & Jagli, 2017; Sinjilawi et al., 2014). Om arkitekturen för molnet dessutom delas mellan flera klienter kan en attack mot en klient orsaka att molnet blir otillgängligt för alla (Alani, 2016).

Exponerade sårbarheter pga multi-tenancy

Multi-tenancy är när organisationer eller användare delar på samma moln, dess minne, databaser och resurser vilket ökar antalet sårbarheter som kan utsättas för attacker (Ali et al., 2015; Galibus et al., 2016; Jathanna & Jagli, 2017; Patil et al., 2017; Singh & Chatterjee, 2017). Detta kan leda till dataintrång samt förlorad eller stulen information (Galibus et al., 2016) vilket därmed riskerar konfidentialiteten (Kumar Sharma et al., 2017). Eftersom det är en delad miljö finns risken att användare kommer åt varandras data vilket riskerar integriteten (Ali et al., 2015; Singh & Chatterjee, 2017).

Hackade gränssnitt eller APIer

Det är vanligt att molntjänster tillhandahåller application programming interfaces (APIer) (Jathanna & Jagli, 2017). APIer används för att klienterna ska kunna kommunicera med molnet och är särskilt utsatta eftersom de kan kommas åt via öppna nätverk, såsom internet (Alani, 2016). Enligt Galibus et al. (2016) kan detta riskera både konfidentialitet, integritet och tillgänglighet.

Svag eller okrypterad data

Ett sätt att undvika att obehöriga kan komma åt känslig data är att kryptera den. Många molnlagringstjänster saknar dock kryptering eller har bristfällig sådan (Kumar Sharma et al., 2017). Enligt Ramel (2017) saknar 82% av alla publika moln kryptering. Därför kan konfidentialiteten riskeras om kryptering saknas eller är svag.

Minskad kontroll samt inkomplett radering av data

Ett problem med molnlagringstjänster är att användare inte har någon kontroll över hur och var deras data förvaras (Aguiar et al., 2014; Ahuja & Komathukattil, 2012; Alani, 2016; Galibus et al., 2016; Kumar Sharma et al., 2017; Sinjilawi et al., 2014). Användare kan därför

inte själva kontrollera status på servern och se om den utsatts för intrång. Därför är det även svårt för användare att vara säker på att en fil verkligen försvinner om man väljer att radera den från molnlagringstjänsten (Alani, 2016). Detta beror på att filen tillfälligt kan ligga kvar i serverns minne tills den skrivits över av en ny fil (Alani, 2016). En angripare kan därför rikta in sig på raderad data och på så sätt komma över känslig information vilket riskerar konfidentialiteten.

SQL-injektioner

SQL-injektioner är ett sätt att hacka applikationer och kan appliceras även på molntjänster (Jathanna & Jagli, 2017). Skadlig kod läggs i SQL-queries som injiceras via inputfält i applikationen, exempelvis via ett formulär (Jathanna & Jagli, 2017). En SQL-injektion kan orsaka problem med både konfidentialitet och integritet eftersom personlig data både kan läcka och ändras obehörigt.

Malicious insiders

En malicious insider är någon som har tillgång till ett system eller en molntjänst med uppsåt att orsaka skada (Alani, 2016; Galibus et al., 2016). Det kan till exempel vara en tidigare anställd, en systemadministratör eller en affärspartner. Angriparen kan, beroende på behörighet, ändra och förstöra data eller till och med förstöra hela systemet (Alani, 2016). Detta innebär att organisationer måste se över anställdas behörigheter och anpassa dessa för att bibehålla kontroll och undvika denna risk (Galibus et al., 2016; Jathanna & Jagli, 2017). Därför påverkar risken konfidentialitet, integritet samt tillgänglighet.

Stulen identitet genom phishing

Olika typer av social manipulation (social engineering) såsom nätfiske (phishing) kan leda till att inkräktare får tillgång till användares lösenord (Alani, 2016; James et al., 2013; Singh & Chatterjee, 2017). Inkräktarna kan därmed komma åt och ändra användarens data vilket gör att konfidentialiteten och integriteten riskeras.

Därmed kan det konstateras att det finns säkerhetsrisker med molnlagring som kan relateras till grundstenarna inom informationssäkerhet och som därmed berör alla som väljer att använda molnlagringstjänster. Vissa av riskerna kan användarna själva motverka genom att vidta motåtgärder men för att kunna göra det krävs kunskap om riskerna. I tidigare forskning har användares kunskap om säkerhetsrisker undersökts genom att utvärdera deras medvetenhet.

2.5 Medvetenhet

Medvetenhet som begrepp kan syfta på kunskapen om något men det kan också vara uppfattning eller en åsikt av något snarare än kunskap (Nationalencyklopedin, n.d.). Medvetenhet inom informationssäkerhet kan definieras som användarens kunskaper om till exempel säkerhetsrisker, säkerhetshot och potentiella motåtgärder (Hanus och Wu, 2016).

2.5.1 Tidigare forskning inom informationssäkerhet

Forskning angående medvetenhet har bland annat gjorts av Hanus och Wu (2016) som i sin studie om medvetenhet för desktop security konstaterar att det inte är tillräckligt att vara medveten om säkerhetshot utan användaren måste också kunna identifiera verktyg eller tekniker för att skydda sig mot dem. Alltså menar Hanus och Wu (2016) att användaren motiveras till att använda kunskap om informationssäkerhet för att undvika säkerhetshot.

James et al. (2013) har istället klassificerat medvetenhet i fem olika kategorier: medvetenhet gällande motåtgärder, tillit till individer, tillit till organisationer, uppfattad risksannolikhet samt uppfattad risksignifikans. I deras studie konstateras det att även om användare anser att signifikansen för att bli utsatt för en attack eller ett säkerhetshot är hög tror många att det inte kommer drabba just dem varvid de ignorerar risken (James et al., 2013). Vidare menar James et al. (2013) att användarens vilja att använda en tjänst går före användarens ansvar att vidta säkerhetsåtgärder.

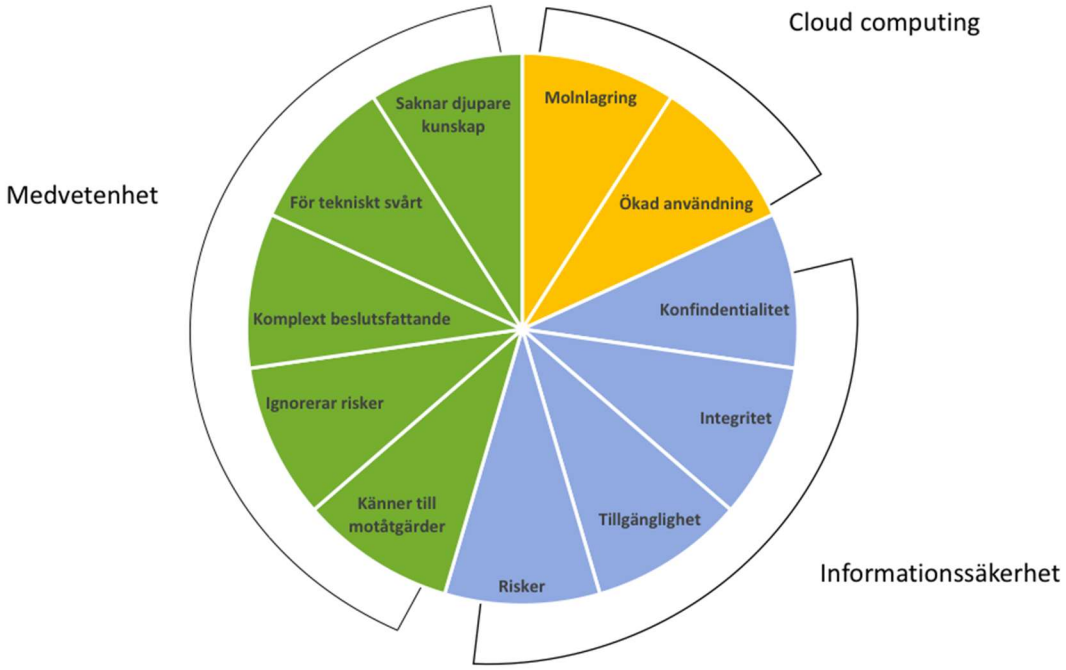
Enligt Coopamootoo och Groß (2014) är det svårare för användare att fatta beslut när det gäller privat data online, eftersom det kräver komplext beslutsfattande, vilket i sin tur kräver en hög grad av medvetenhet hos användare. De konstaterar även att användare inte är rädda för att ladda upp data online så länge data som laddats upp bibehålls inom samma tjänst. Användares uppfattning om integritet skiljer sig därför åt från tjänst till tjänst.

Andra som har forskat på hur användare uppfattar och hanterar säkerhetsrisker är Harbach, Fahl och Smith (2014) som undersökt användares säkerhetsbeteende när de använder internet. I sin artikel konstaterar de att det uppfattas som alltför tekniskt svårt att vidta motåtgärder mot säkerhetsrisker, vilket leder till att användare inte bryr sig om att agera mot riskerna utan använder internet i alla fall. De drar slutsatsen att användare är bekymrade över att få sitt konto eller lösenord stulet men förstår inte fullt ut vad det innebär utan endast på ett abstrakt plan. Harbach et al. (2014) menar därför att om användare inte förstår hur en risk skulle påverka dem själva negativt, minskar deras vilja att vidta en motåtgärd ytterligare.

Furnell, Bryant och Phippen (2007) har undersökt användares uppfattning om säkerhetsproblem och deras attityder mot att använda skyddsmekanismer mot dem. Genom en enkätundersökning konstateras att användare uppger att de är medvetna om hot och att de använder skyddsmekanismer på ett ytligt plan samtidigt som djupare analys visar att de saknar kunskap och förståelse för vad det faktiskt innebär (Furnell et al., 2007). Vidare menar Furnell et al. (2007) att användare kan vara bekanta med säkerhetstermer och veta att säkerhetshot existerar men djupare kunskap om hur man skyddar sig mot dem saknas.

2.6 Sammanfattning

Med avseende på de teoretiska aspekter som identifierats i litteraturen och presenterats i detta kapitel finns det några huvudsakliga aspekter som vår uppsats kommer bygga på. Dessa aspekter har varit viktiga i den teoretiska utvecklingen samt bidragit till utformningen av den empiriska undersökningen och utgör därmed ramverket för denna uppsats. Ramverket, i figur 2.1, ger en överblick och sammanfattar i korthet de viktigaste aspekterna.



Figur 2.1 Teoretiskt ramverk

Ramverket är uppdelat i tre huvudområden: cloud computing, informationssäkerhet samt medvetenhet. Cloud computing utgörs av molnlagring eftersom det är denna teknologi som står i fokus i studien. Även aspekten ökad användning faller under detta område. Ökad användning handlar om molnlagringstjänster som nyttjas av användare, hur frekvent deras användning är samt vilka faktorer som påverkat valet av molnlagringstjänster. Aspekten ökad användning anses självutvecklad för denna studie då dess innebörd influerats av de artiklar som behandlats under litteraturstudien. Sedan har denna information formats att passa just vår studie eftersom det anses nödvändigt för resultatet. Denna aspekt har även influerat några av frågorna i vår enkätguide.

Eftersom risker med molnlagring och användares medvetenhet gällande dessa står i fokus utgör det en aspekt. Riskerna kan alla härledas till informationssäkerhet och dess grundstenar konfidentialitet, integritet samt tillgänglighet, varvid dessa är viktiga aspekter i ramverket.

Tidigare forskning angående användares medvetenhet har lett fram till konstaterandet om vad som påverkar eller utgör medvetenhet. Dessa anses viktiga även för vår studie då de behandlat medvetenhet inom närliggande områden som eventuellt kan appliceras även i kontexten molnlagring. Därmed har dessa sammanfattats kort och utgör varsin aspekt under huvudområdet medvetenhet.

Enligt D'Arcy, Hovav och Galletta (2009) fokuserar organisationer ofta på de tekniska aspekterna som orsakar säkerhetsincidenter snarare än den mänskliga faktorn som omedvetenhet. Med avseende på detta utgörs vårt ramverk till stor del av medvetenhetsaspekter då detta borde prioriteras lika mycket som tekniska aspekter.

Ramverket representerar de centrala aspekter som vi identifierat under arbetet med litteraturstudien och som sedan ligger till grund för vår empiriska undersökning. För att bättre förstå hur vår empiriska undersökningen utformats beskriver följande kapitel denna process.

3 Metodologi

I detta kapitel ges en beskrivning av de metoder som har använts för att genomföra denna uppsats. Metodvalen diskuteras och motiveras. Även kvaliteten på enkätundersökningen diskuteras enligt kvalitetsaspekter såsom validitet, reliabilitet och etik.

3.1 Litteraturstudie

Arbetet med denna studie inleddes genom att identifiera och läsa artiklar om generella risker med cloud computing, specifika risker för molnlagring samt om medvetenhet. Detta gjordes genom sökningar i LUBSearch samt Google Scholar för att få en inblick i tidigare forskning. Vi valde att fokusera på artiklar som beskrev risker med molntjänster. I flera av artiklarna gjordes kopplingar till grundstenarna inom informationssäkerhet, därmed valde vi att definiera samt relatera riskerna till dem.

För att få en överblick över de risker vi hittat genom vår litteraturgenomgång skapades en tabell där relevanta risker för molnlagringstjänster sammanställdes. I tabellen kartläggs vilken eller vilka av grundstenarna inom informationssäkerhet som respektive risk hör till. Till en början bestod tabellen av sexton risker vilket senare omformulerades till nio risker. Dessa nio risker nämndes som minst av tre olika referenser. Omdefinieringen av risker gjordes på grund av att författare benämnt dem på olika sätt samt att de i vissa fall bröt ner riskerna till väldigt specifika risker. Vi valde att definiera förlust av data samt dataläckage som samma risk eftersom det i slutändan handlar om att användaren förlorar sin data, även om vissa författare valde att skilja på dem. Detta gjordes också för att enkätundersökningen skulle innehålla tydligt separerade risker som borde vara lättare för respondenterna att förstå. Vi valde att ha dataintrång som en egen risk även om den i viss mån täcker in vissa av de andra riskerna eftersom de artiklar som studerats haft den uppdelningen.

I litteraturstudien har vi även undersökt hur tidigare forskning kring användares medvetenhet relaterat till säkerhet har sett ut.

3.2 Enkätundersökning

I flera studier (Arpaci et al., 2014; Garrison et al., 2016; Gurung & Raja, 2016; Hanus & Wu, 2016; James et al., 2013; Yang et al., 2017) som ämnat undersöka medvetenhet har enkätundersökningar använts som undersökningsmetod, därmed ansågs det som en passande metod även för vår studie. En kvantitativ ansats har gett oss möjlighet att studera hur utbrett medvetenhet om risker med molnlagring är, samtidigt som den kritiska distansen till respondenterna bibehållits (Jacobsen, 2002).

Enkätfrågorna skickades först till vår handledare för feedback vilket resulterade i några klargöranden av otydliga begrepp. Sedan skickades enkäten till en mindre grupp respondenter som fick testa den, detta för att ge oss ytterligare en möjlighet att utföra justeringar.

Vi valde att distribuera enkäten fysiskt för att göra det enklare för respondenterna att delta i vår undersökning. Eftersom den var i fysisk form krävdes det inte att respondenten hade en dator eller smartphone tillgänglig och de behövde inte heller lägga tid på att leta upp enkäten online.

3.2.1 Urval

Vi valde att distribuera vår enkät till studenter vid Lunds universitet. För att få respondenter med olika studieinriktningar åkte vi runt till olika studieplatser och fakulteter i Lund, därmed gjordes ett bekvämlighetsurval (Jacobsen, 2002). Detta sätt valdes för att vi ville få många svar och förhoppningsvis uppnå en spridning på studenters studieinriktning. Vi strävade även efter en någorlunda jämn fördelning mellan kön.

3.2.2 Utformning av enkät

Enkäten bestod av nio huvudfrågor där en del hade följdfrågor beroende på om respondenten svarat ja eller nej samt en huvudfråga som bestod av nio underfrågor. De flesta frågor hade fasta svarsalternativ där respondenten endast behövde kryssa i ett alternativ men även öppna svarsalternativ förekom. Enkäten var indelad i tre sektioner där den första innehöll bakgrundsinformation om respondenten, nästa behandlade användningen av molnlagringstjänster och den tredje behandlade medvetenhet om risker.

I början av enkätundersökningen uppmanas respondenten att fylla i kön samt studieinriktning. Detta är för att säkerställa att vi får ungefär lika många kvinnor som män som svarar och om inte, är vi medvetna om det och kan ta hänsyn till det. Att respondenten uppmanas ange studieinriktning är för att i resultatet kunna se om det var en jämn spridning av studenter som läser olika ämnen.

I nästa sektion introduceras molnlagring med en kort beskrivning om vad det innebär vilket följs av fyra frågor om användning gällande molnlagringstjänster. Första frågan tar reda på om respondenten använder en molnlagringstjänst, om inte uppmanas respondenten hoppa till fråga sex som behandlar risker. Denna fråga har vi med för att i vår dataanalys kunna analysera huruvida det finns ett samband mellan molnlagringsanvändning och riskmedvetenhet. De efterföljande tre frågorna tar reda på vilken eller vilka molnlagringstjänster som respondenten använder, hur ofta dessa används samt vilka faktorer som påverkade valet av molnlagringstjänst. Alla tre frågor har färdiga svar men både på frågan om vilken molntjänst man använder och frågan med faktorer finns det möjlighet för respondenten att skriva en annan faktor än de som listats.

Nästa sektion i enkäten behandlar medvetenhet om risker. Den första frågan som ställs i denna sektion handlar om ifall respondenten valt att inte ladda upp en viss typ av filer eller information av säkerhetsskäl. Denna fråga kan tolkas som ledande, vilket är meningen då vi specifikt vill veta om detta sker eller ej. Svaren på denna fråga ger oss en inblick i om det finns ett säkerhetsmedvetande när det kommer till privat data och om respondenter är selektiva i sin uppfattning av vad de väljer att ladda upp i molnet. Om respondenten svarar ja på denna fråga, uppmanas den till att beskriva vilken typ av filer eller information den valt att inte ladda upp.

Den efterföljande frågan handlar specifikt om risker. Respondenten blir uppmanad att kryssa för de risker som den hört talas om. Alla risker är beskrivna i en eller två meningar på ett sådant sätt att även personer som inte är insatta i ämnet ska kunna förstå dem. Även på denna fråga finns möjligheten för respondenten att fylla i andra risker än de som listats. Med denna fråga vill vi undersöka vilken kunskap respondenterna har om specifika risker och se om det finns något samband med användning av molnlagringstjänster. Vi vill också kunna se vilka risker som flest av respondenterna har hört talas om och vilka som är nya för dem.

Nästa fråga rör huruvida respondenternas kännedom av någon eller några av riskerna i fråga sex påverkat ifall de valt att använda eller inte använda molnlagringstjänster. Om respondenten svarar ja, uppmanas den till att skriva numren på de risker som påverkat valet. Sedan ställs frågan om respondenten vidtagit några motåtgärder mot någon eller några av riskerna. Om svaret är ja, uppmanas respondenten att beskriva hur. Dessa två frågor syftar till att undersöka medvetenhet hos respondenten.

Sista frågan ställs till respondenter som fyllt i att de inte använder en molnlagringstjänst där de får uppge varför de valt att inte göra detta. Denna fråga är intressant på så sätt att vi kan kontrollera om det beror på kännedom om risker att de valt att inte använda en molnlagringstjänst eller om det finns andra skäl till att de inte valt att använda sådana tjänster.

Tabell 3.1 Enkätguide

Nr	Fråga	Motivering	Aspekter från teoretiskt ramverk	Koppling teori
1	Använder du en molnlagringstjänst?	Eftersom flera följdfrågor är beroende av att man använder en molnlagringstjänst inleds enkäten med denna fråga.	Molnlagring, ökad användning	Utvecklad för denna studie
2	Om ja, vilken eller vilka [molntjänster]?	För att kartlägga respondentens användande av molnlagringstjänster.	Molnlagring	Utvecklad för denna studie
3	Hur ofta använder du en molnlagringstjänst?	För att kartlägga hur frekvent respondenten använder molnlagringstjänster.	Molnlagring, ökad användning	Utvecklad för denna studie
4	Vilken eller vilka av följande faktorer påverkade dina val av molnlagringstjänster?	För att ta reda på vilka faktorer som påverkar val av molnlagringstjänst. Framförallt för att se om säkerhet är en av dessa faktorer.	Molnlagring, ökad användning	Coopamootoo och Groß (2014)
5	Finns det filer eller information du väljer att inte ladda upp i molnet av säkerhetsskäl?	För att se om respondenten är medveten om risken med att ladda upp eller dela privat data i molnet.	Konfidentialitet, risker, komplext beslutsfattande, för tekniskt svårt	Coopamootoo och Groß (2014), Harbach et al. (2013)
6	Nedan presenteras en lista med potentiella risker med molnlagring. Kryssa i dem som du hört talas om: [risker från tabell 2.1 räknas upp]	För att se vilka risker med molnlagring som respondenten har kännedom om.	Konfidentialitet, integritet, tillgänglighet, risker, saknar djupare kunskap	Furnell et al. (2007)

7	Påverkade din kännedom om någon/några av riskerna ovan ditt val att använda/inte använda molnlagringstjänster?	För att se om det finns ett samband mellan kännedom om risker och användning av molnlagringstjänster.	Saknar djupare kunskap, för tekniskt svårt, ignorerar risker	Furnell et al. (2007), Harbach et al. (2013), James et al. (2013)
8	Om du använder en molnlagringstjänst, har du vidtagit motåtgärder mot någon eller några av dessa risker?	För att se om respondenten har kunskap om motåtgärder.	Saknar djupare kunskap, känner till motåtgärder, ignorerar risker	Furnell et al. (2007), Hanus och Wu (2016), Harbach et al. (2014), James et al. (2013)
9	Om du inte använder en molnlagringstjänst, vad har påverkat detta val?	För att få reda på vilka faktorer som påverkat respondentens val att inte använda en molnlagringstjänst.	Molnlagring, ökad användning	Utvecklad för denna studie

3.3 Analys av empiri

I analysen av den insamlade empirin användes Excel för att sammanställa data. Excel ansågs vara ett lämpligt verktyg för att omvandla fysisk data till elektronisk på ett strukturerat sätt. Vi nyttjade också funktionaliteten i Excel för att göra tabeller och grafer vilket ger en tydlig översikt av all insamlad data.

För att effektivisera sammanställningen av data kodades svarsalternativen om till siffror. Detta gjordes för att kunna lägga in filen i SPSS där samband identifierades. I SPSS användes filtreringsfunktionen för att skilja olika svarsgrupper från varandra och för att kunna göra jämförelser mellan vad en svarsgrupp svarat på andra frågor. Sedan gjordes korstabeller där resultatet redovisades i procent eftersom det gav siffror som ansågs lättare att tolka.

Resultatet av empirin presenteras således som tabeller och grafer. Öppna frågor presenteras som citat och som tabeller där svaren blivit indelade i teman. Vi har valt att strukturera empiriresultatet enligt fyra områden: demografi, användning, informationssäkerhet och risker samt medvetenhet.

I diskussionen analyseras resultatet av empirin i förhållande till tidigare teori i enlighet med enkätguiden. Även diskussionen har samma disposition som resultat av empiri för att det ska vara tydligt att resultaten diskuteras i förhållande till teorin.

3.4 Undersökningskvalitet

Undersökningens totala giltighet beror av de tre förhållandena intern giltighet, extern giltighet samt tillförlitlighet (Jacobsen, 2002). Den interna och externa giltigheten rör validiteten och huruvida man mäter det man vill mäta medan tillförlitlighet mäter undersökningsmetodens noggrannhet (Jacobsen, 2002). Dessa aspekter har vi tagit hänsyn till när vi utformat vår metod för att uppnå högre kvalitet.

3.4.1 Validitet

Enligt Jacobsen (2002) innebär intern validitet att alla deltagare i en undersökning ska ha samma uppfattning om ett visst begrepp eller fenomen. Det är därför viktigt att utforma frågor som alla deltagare i en undersökning kan förstå. För att uppnå intern validitet i vår enkätundersökning har vi bland annat skrivit en kortare förklaring om vad en molntjänst är samt gett exempel på tjänster som vi tror att respondenterna har kännedom om sedan tidigare. Vidare var enkäten tydlig då vi justerat den efter feedback om otydlighet.

Extern validitet handlar om ifall det går att göra generaliseringar för resultatet utöver den kontext undersökningen gjorts i (Jacobsen, 2002). Ett bekvämlighetsurval gjordes, vilket medför att den externa validiteten minskar då det finns risk att det blivit ett systematiskt bortfall eftersom endast de som var på plats kunde svara på enkäten. Sedan är det osäkert att de svar som studenter vid Lunds universitet gett i denna undersökning är applicerbara i andra kontexter eftersom kunskap om molntjänster kan variera beroende på exempelvis ålder eller utbildningsnivå.

3.4.2 Reliabilitet

Eftersom studien behandlar säkerhetsrisker gällande molnlagringstjänster är enkätundersökningen ledande till en viss grad. Våra frågor kan anses gå rakt på sak vilket vi visserligen försökt tona ned i och med inledande frågor om användning samt att inte ordagrant skriva ut vår frågeställning. Exempelvis ställs frågan om kännedom av nämnda risker påverkade deras val att använda eller inte använda molnlagringstjänster direkt efter riskerna presenterats vilket i någon mån kan anses som ledande.

För att respondenterna inte skulle påverkas av tidigare frågor valde vi att ställa frågan om det fanns någon data respondenterna valde att inte ladda upp av säkerhetsskäl innan riskerna presenterades. Säkerhetsriskerna presenterades dessutom på en annan sida av enkäten vilket minskar risken att respondenterna hann se dem och blev färgade av dessa.

När vi analyserat data har vi först matat in den i Excel där vi även har skapat tabeller och diagram för att presentera resultatet av undersökningen. För att komplettera detta och kunna se samband för hur respondenterna valt att svara har vi använt oss av statistikverktyget SPSS. Båda dessa är passande verktyg för statistisk analys vilket gör vårt resultat mer tillförlitligt.

3.4.3 Etik

I inledningen till enkäten informerades respondenterna om att det var frivilligt att delta i undersökningen samt att den var helt anonym. Eftersom enkäten distribuerades fysiskt fick alla respondenter också möjlighet att ge ett muntligt samtycke. För att ge tillbaka till alla som ställde upp och genomförde undersökningen, fick de i slutet av enkäten tillgång till våra mailadresser ifall de vill läsa studien i sin helhet när den färdigställts. Vi har också varit noggranna när resultatet överförts från de fysiska formulären till en elektronisk sammanställning för att undvika att data förvrängs.

3.5 Kritik av metodval

Enligt Jacobsen (2002) finns det vissa nackdelar med en enkätundersökning såsom att svar endast ges på det som det frågas om, den som svarar måste ta hänsyn till forskarens perspektiv samt att individuella variationer missas. Därmed är vi medvetna om att denna metod kan innebära ett ytligt resultat och saknar möjligheten till djupgående analyser (Jacobsen, 2002).

En nackdel med fasta svarsalternativ är att det blir forskarens syn som testas och inte respondentens (Jacobsen, 2002). Detta blir tydligt i vår egen studie, framförallt gällande riskerna i fråga sex då det är risker som vi identifierat genom litteraturen som respondenten måste ta ställning till. Därav begränsas respondentens fria tänkande vilket kanske mynnat ut i andra risker. För att motverka detta ges respondenten möjlighet att fylla i ett annat alternativ än de fasta på vissa frågor. Därmed tillåts respondenten komma till tals och begränsningen minskas en aning.

Alla avgränsningar leder till att vi endast kan uttala oss om de som vi avgränsat oss till, nämligen studenter vid Lunds universitet (Jacobsen, 2002). Även om vi försökte få ett slumpmässigt urval är detta inte säkert, vilket innebär att de resultat vi får inte kan generaliseras direkt till populationen utan mer visar på tendenser som kan finnas inom den. Eftersom ett bekvämlighetsurval gjordes finns det också risk för ett statistiskt snett urval (Jacobsen, 2002).

Vidare utgörs vår kvantitativa data av respondentens egen uppfattning om sin medvetenhet. För att ytterligare stärka den data som inhämtats hade observationer kunnat genomföras för att se hur respondenten faktiskt agerar.

Eftersom enkätformulären distribuerades fysiskt behövdes data matas in manuellt. Därmed finns det risk att data kan ha matats in fel på grund av den mänskliga faktorn. Vi valde dock att kontrollera all data en extra gång för att se att allt hade blivit rätt.

3.6 Sammanfattning

Sammanfattningsvis utgörs vår metod av en inledande litteraturstudie med en efterföljande enkätundersökning. Den kvantitativa ansatsen som metod för empirisk undersökning valdes då vi ämnar undersöka medvetenhet och dess utbreddhet bland användare. Denna metod tillåter för en datainsamling med många enheter som sedan kan användas för att identifiera samband.

Resultat av empiri samt diskussion har samma tematiska indelning för att ge struktur och mening åt innehållet samt underlätta för läsaren att tolka sambanden som presenteras och sedan diskuteras.

4 Resultat av empiri

I detta kapitel presenteras det resultat som framkommit av enkätundersökningen. Resultatet presenteras genom tabeller, diagram och förklarande texter. Även samband som påträffats presenteras.

Totalt tillfrågades 131 personer i enkätundersökningen varav 123 valde att delta i den, vi hade alltså en svarsfrekvens på 94 %. Eftersom respondenter tillfrågades muntligt om de ville delta i undersökningen var det inga enkäter som lämnades in helt tomma. Det förekom enhetsbortfall på fråga fem, sju samt åtta där en respondent per fråga glömt eller valt att inte svara. Det var däremot inte samma respondent som stod för bortfallet på de tre frågorna.

4.1 Demografi

Av respondenterna var 82 kvinnor, 40 män samt en person som svarade annat. Flest respondenter tillhörde ekonomihögskolan och läste ekonomi eller systemvetenskap. Däremot fanns det ingen respondent som tillhörde medicinska eller konstnärliga fakulteten. Eftersom alla respondenter var studenter antar vi att åldern varierar mellan 19 och 29 år, med något enstaka undantag.

Tabell 4.1 Fördelning av respondenter enligt fakultet

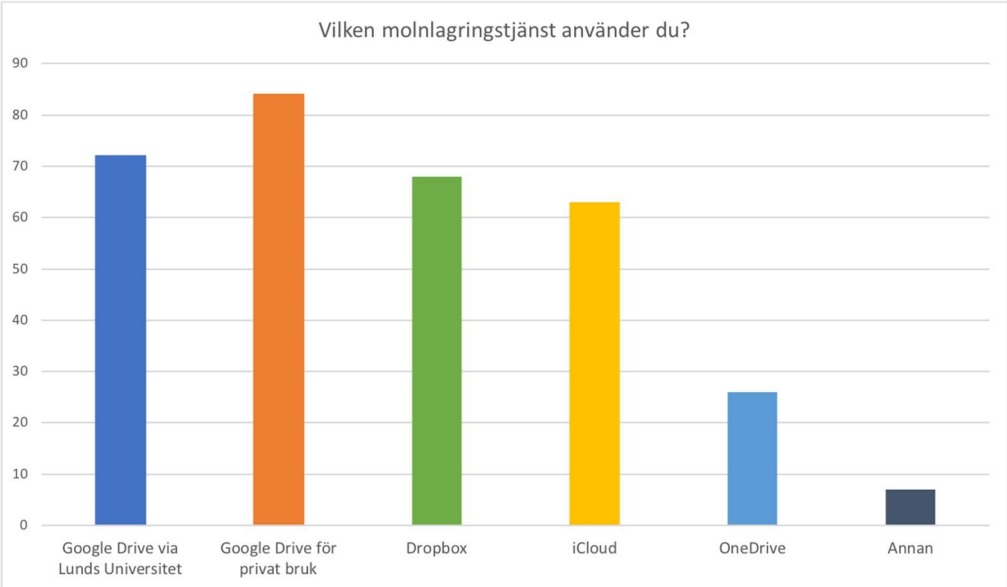
Fakultet	Antal respondenter
Ekonomihögskolan	53
Humanistiska och teologiska fakulteterna	10
Juridiska fakulteten	13
Konstnärliga fakulteten	0
LTH	16
Medicinska fakulteten	0
Naturvetenskapliga fakulteten	5

För att se om det fanns någon skillnad i män och kvinnors riskmedvetenhet jämfördes hur stor andel av männen respektive kvinnorna som valt de två mest valda riskerna, dataintrång och phishing. Resultatet visar att det är jämnt mellan de olika könen, 77 % av kvinnorna respektive 85 % av männen valde dataintrång. Även för den näst mest valda risken, phishing, är fördelningen mellan könen jämn. 50 % av kvinnorna respektive 57 % av männen känner till phishing.

Om man ser till genomsnittligt antal risker som valts, har kvinnor i snitt markerat 2,8 risker medan männen markerat 4,1 risker. Det totala genomsnittet är 3,3 valda risker.

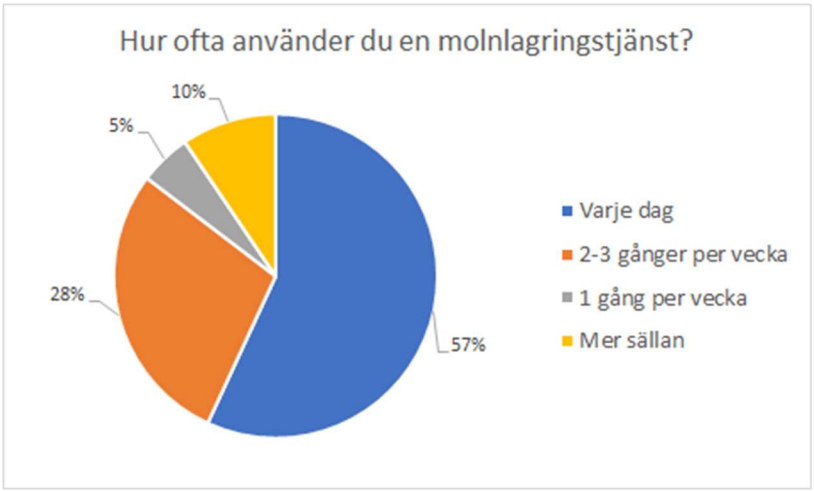
4.2 Användning

94 % av respondenterna uppgav att de använder en molnlagringstjänst och 6 % att de inte använder en molnlagringstjänst. Den molnlagringstjänst som valdes av flest respondenter (68 %) var Google Drive för privat bruk, medan OneDrive valdes av minst antal respondenter (21 %). De som angav en annan molnlagringstjänst (6 %) nämnde bland annat Google Photo samt Overleaf. 89% av respondenterna använder mer än en molnlagringstjänst.



Figur 4.1 Val av molnlagringstjänster

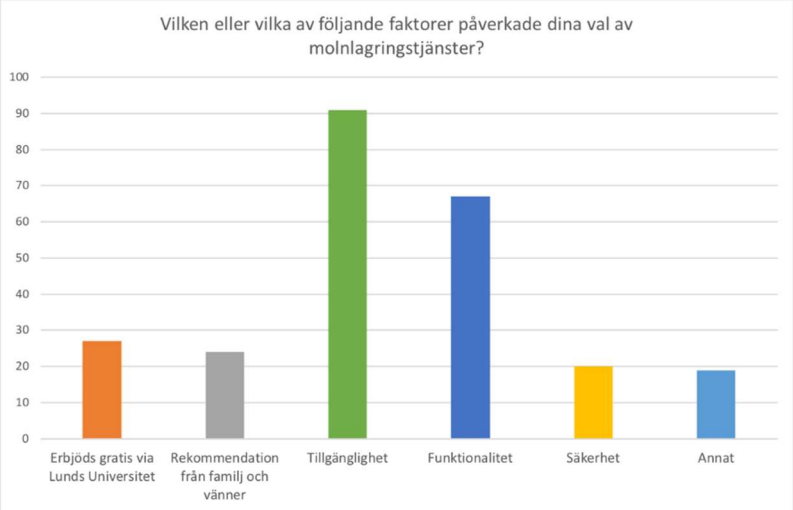
Gällande hur ofta respondenterna använde molnlagringstjänster svarade en majoritet av respondenterna (57 %) att de använder molnlagringstjänster varje dag.



Figur 4.2 Frekvent användning av molnlagringstjänster.

I en jämförelse mellan val av molntjänst och användarfrekvens upptäcktes ingen större skillnad. Fördelningen stämmer också väl överens med det generella resultatet.

De faktorer som valdes av flest respondenter som anledningar till att de valt en molnlagringstjänst var tillgänglighet samt funktionalitet. Övriga faktorer valdes av ett hyfsat jämnt antal respondenter. Endast 16 % valde faktorn säkerhet vid val av molnlagringstjänst.



Figur 4.3 Påverkande faktorer

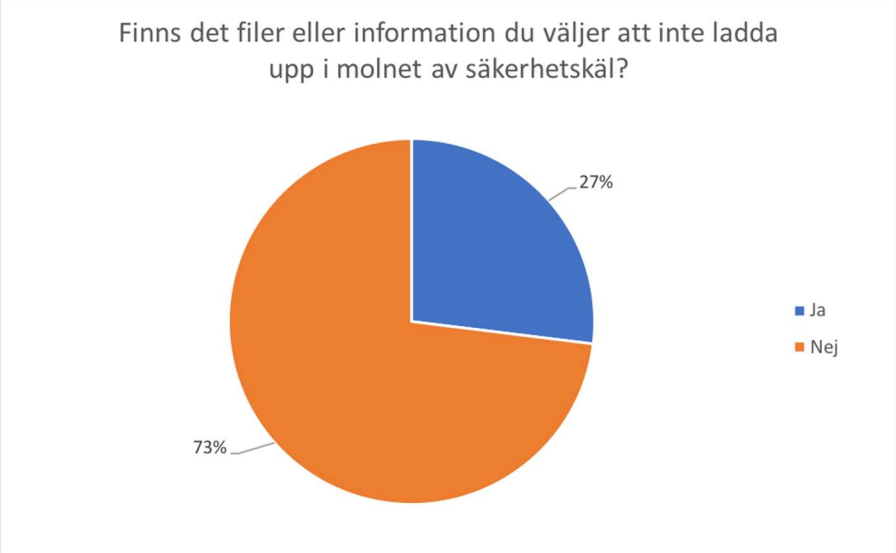
Respondenter hade också möjlighet att skriva till en annan faktor än de som listats. I huvudsak tre faktorer nämndes av respondenter: användarvänlighet, pris samt bra vid grupparbete.

Tabell 4.2 Sammanställning av andra faktorer

Anledning	**Antal**
Användarvänligt	5
Pris	5
Bra vid grupparbete	9

4.3 Informationssäkerhet och risker

Av de respondenter som använder molnlagringstjänster uppgav 27 % att det finns data de avstår från att ladda upp i molnet av säkerhetsskäl. 73 % svarade nej på frågan om det finns information som de väljer att inte ladda upp på grund av säkerhetsskäl.



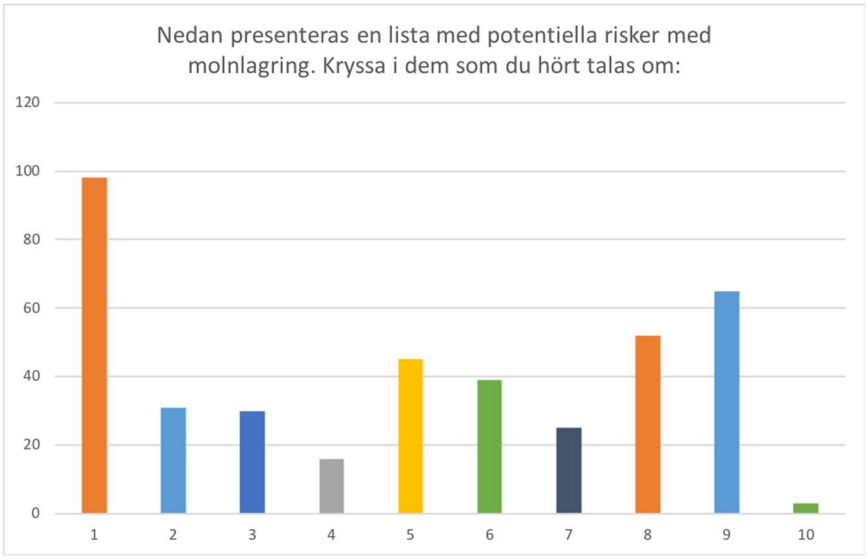
Figur 4.4 Fördelning mellan att inte ladda upp filer och information av säkerhetsskäl

De som svarat ja på att det fanns filer eller information respondenten valde att inte ladda upp av säkerhetsskäl uppmanades ange vilken typ av filer eller information som de valt att inte ladda upp vilket är sammanställt i tabellen nedan.

Tabell 4.3 Frekvens över typ av information eller filer respondenter valt att inte ladda upp

Typ av data	Frekvens
Bankinfo	4
Privata bilder	7
Känsliga dokument	11
Lösenord	3
Personlig information	9
Övrigt	4

De två mest markerade riskerna var dataintrång och phishing som 80 % respektive 53 % valde. De minst valda riskerna var att gränssnittet blir hackat som valdes av 13 % och SQL-injection som valdes av 20 %. 2 % valde alternativet annat och skrev riskerna “att molntjänsten äger datan som ligger där, vilket ej är bra pga plagiat och skolarbete” och “företag som Google utnyttjar info och ger till andra företag”.



Figur 4.5 Sammanställning av valda risker

1. Dataintrång hos leverantören av molntjänsten gör att känslig information läcker eller raderas.
2. Molntjänsten överbelastas på grund av en DoS-attack (Denial of Service – angripare gör extremt många anrop på tjänsten) vilket leder till att tjänsten blir otillgänglig för användare.
3. Ett moln delas av flera organisationer vilket ökar antalet sårbarheter i lagringstjänsten.
4. Gränssnitt som används i molnlagringstjänsten kan utnyttjas av inkräktare.
5. Molnlagringstjänstens kryptering av data är bristfällig.
6. Minskad kontroll över i vilka länder personlig data förvaras. Kan därför vara svårt att kontrollera om data verkligen har raderats eller vilken lagstiftning som gäller.
7. Angripare attackerar tjänsten genom SQL-injection (att skicka in skadlig kod genom formulärfält) för att komma åt exempelvis användares lösenord.
8. Anställda hos leverantören av molntjänsten missbrukar sina behörigheter och orsakar skada på tjänsten eller kommer åt användares uppgifter.
9. Phishing - användaren klickar på en länk i ett mail som ser ut att komma från leverantören av molntjänsten. Länken leder till en falsk hemsida med inloggningsformulär där användaren luras att fylla i sina uppgifter.
10. Annan

Ingen av respondenterna kryssade i mer än 8 risker. Flest respondenter valde två risker (24 %) och minst var de som valde fyra risker eller inte kryssade i någon (6 %).

Tabell 4.4 Antal risker som respondenterna valt

Antal risker	Procent
0	5,7
1	17,9
2	23,6
3	16,3
4	5,7
5	9,8
6	9,8
7	8,9
8	2,4
Totalt	100,0

Eftersom de som använder molnlagringstjänster var en klar majoritet av respondenterna (94 %) är skillnaden i en jämförelse av hur många risker de har valt jämfört med det generella resultatet relativt liten. 47 % har valt noll till två risker, 32 % har valt tre till fem risker och 21 % har valt sex till åtta risker. I tabellen nedan visas andelen som valt respektive antal risker På frågan om respondentens kännedom om risker påverkat valet att använda eller inte använda molnlagringstjänster uppgav 82 % att det inte påverkat deras val medan 18 % uppgav motsatsen.

Tabell 4.5 Antal risker bland de som använder molnlagringstjänster

Antal risker	Procent
0	6,0
1	17,2
2	24,1
3	16,4
4	5,2
5	10,3
6	8,6
7	9,5
8	2,6
Totalt	100,0

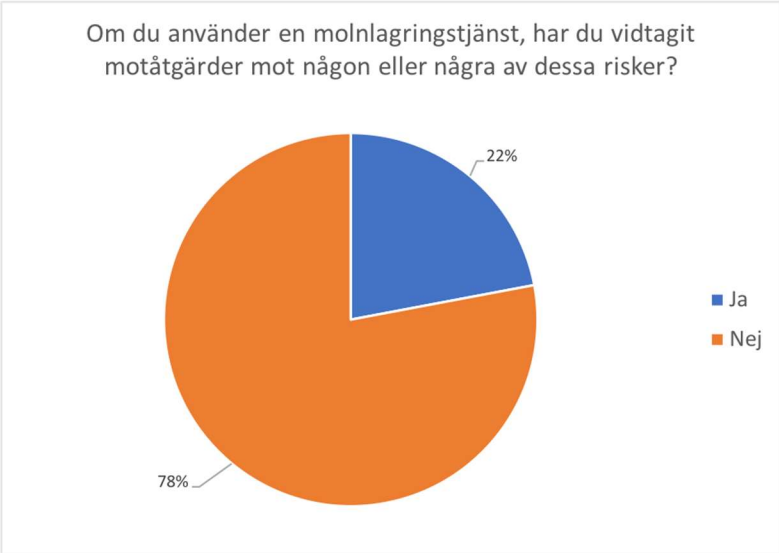
Figur 4.6 Fördelning över hur risker påverkat respondenternas användning

De som svarat ja på föregående fråga uppmanades att skriva numren på de risker som påverkat valet att använda eller inte använda molnlagringtjänster. Det resultatet är sammanställt i följande tabell där vänstra kolumnen visar det procentuella intervall för hur stor andel av riskerna som valts i fråga sex som nämns i fråga sju. Den högra kolumnen visar frekvens i procent för hur stor andel som har svarat för respektive intervall.

Tabell 4.6 Frekvens över hur stor andel risker som påverkat respondenternas användning

Intervall	Frekvens i procent
0-10 %	18
11-20 %	9
21-30 %	9
31-40 %	5
41-50 %	9
51-60 %	0
61-70 %	14
71-80 %	0
81-90 %	0
91-100 %	36

På frågan om respondenterna vidtagit motåtgärder mot någon eller några av riskerna svarade 78 % att de inte hade det medan 28 % hade vidtagit motåtgärder.



Figur 4.7 Fördelning mellan respondenter som vidtagit eller inte vidtagit motåtgärder

Om respondenten svarade ja uppmanades den att uppge på vilket sätt den vidtagit motåtgärder. De motåtgärder som nämndes presenteras i tabellen nedan:

Tabell 4.7 Frekvens över de motåtgärder respondenter uppgett

Motåtgärd	Frekvens
Laddar ej upp personlig/känslig information	13
Läser på/håller sig medveten om risker	4
Byter lösenord ofta	3
Kryptering	2
Back-up	2
Använder extern hårddisk för lagring	2
Extra authentication vid inlogg	1

Sammanlagt sju respondenter uppgav att de inte använder molnlagringstjänster. Deras studieinriktningar var följande:

Tabell 4.8 Studieinriktning för respondenter som valt att inte använda molnlagringstjänster

Studieinriktning	Frekvens
Ekonomi	1
Juridik	2
Mänskliga rättigheter	2
Rättssociologi	1
Service management	1
Totalt	7

Anledningar till varför respondenter valt att inte använda molnlagringstjänster var:

- "Bristande kunskap inom IT"
- "Inte tänkt att det behövs"
- "Ointresse"
- "Använt andra tjänster"
- "Förstår mig inte på det!"
- "Jag är inte i behov av det just nu + att jag inte är fullt påläst om hur det fungerar. "

4.4 Medvetenhet

Det fanns ingen större skillnad (mindre än 10 %) mellan de som valt att inte ladda upp data i molnet på grund av säkerhetsskäl och val av molnlagringstjänst. Det fanns inte heller någon större skillnad mellan de som använder fler än en molnlagringstjänst och de som endast använder en molnlagringstjänst och om de valt att ladda upp eller inte ladda upp filer eller information av säkerhetsskäl.

Av de respondenter som valt att inte ladda upp filer eller information av säkerhetsskäl har 26 % valt att de känner till sju eller åtta risker. Detta kan jämföras mot respondenter som inte valt att inte ladda upp filer eller information där endast 8 % känner till sju eller åtta risker. Däremot var det fler av dem som inte valt att inte ladda upp filer eller information som kände till en eller två risker (52 % jämfört med 26 %).

Av de respondenter som uppgivit att de inte laddar upp viss data av säkerhetsskäl har 94 % markerat att de känner till risken dataintrång. Av de som svarat nej är motsvarande andel 75 %.

I en jämförelse mellan användarfrekvens och antal risker som valts i fråga sex, är det 15 % av de som använder en molnlagringstjänst varje dag eller 2-3 gånger per vecka som valt sju eller åtta risker. Detta kan ställas mot de som använder en molnlagringstjänst en gång per vecka eller mer sällan respektive aldrig där ingen valt sju eller åtta risker. Däremot har ungefär lika många i dessa tre grupper valt att de känner till en eller två risker i fråga sex.

Av respondenter som använder en molnlagringstjänst har 8 % valt ingen eller en risk medan 15% valt sju eller åtta risker i fråga sex. Detta kan jämföras med de som använder mer än en molnlagringstjänst där 26 % valt ingen eller en risk, medan 12 % valt 7 eller 8 risker.

I en jämförelse av resultaten på fråga sju (Påverkade din kännedom om någon/några av riskerna ovan ditt val att använda/inte använda molnlagringstjänster?) och hur många risker respektive respondent valt fann vi att bland de som svarade ja markerade 29 % en eller två risker, bland de som svarade nej markerade 47 % samma mängd risker. Av de som svarade ja markerade 19 % sju eller åtta risker. Andelen bland de som svarade nej var 11 %.

Av respondenter som använder en molnlagringstjänst svarade 15 % att deras kännedom om risker påverkat användningen av molnlagringtjänster, vilket kan jämföras mot respondenter som använder en eller flera molnlagringstjänster där siffran var 18 %. 85% av de som använder endast en molntjänst respektive 82 % av de som använder mer än en molnlagringstjänst svarade att kännedom om risker inte påverkat användningen. Alltså var det ingen större skillnad mellan att använda en eller flera molnlagringstjänster och om kännedom av risker påverkat val att använda eller inte använda molnlagringstjänster.

Av de respondenter som har svarat att de har vidtagit motåtgärder mot säkerhetsrisker markerade 23 % en eller två risker. Av de respondenterna som istället svarade nej på samma fråga var andelen 47 %. Andelen som hade markerat sju eller åtta risker var bland de som hade vidtagit motåtgärder 27 %. Bland de som svarat att de inte vidtagit motåtgärder var andelen 8 %.

Inte heller på frågan om respondenten vidtagit motåtgärder mot någon eller några av riskerna skilde det sig mellan de som endast använder en molnlagringstjänst (23 % som svarade ja, 77 % som svarade nej) och de som använder mer än en molnlagringstjänst (22,5 % som svarade ja, 77,5% som svarade nej.

5 Diskussion

I detta kapitel diskuteras resultatet från den empiriska undersökningen som utvecklats i relation till vårt teoretiska ramverk, som introducerats i figur 2.1.

Som tidigare nämnt, har det teoretiska ramverket influerat vår empiriska undersökning. I korthet utgörs ramverket av huvudområdena cloud computing som i huvudsak handlar om användning, informationssäkerhet som rör grundstenarna samt risker och slutligen de aspekter som definierar medvetenhet. Huvudområdena och deras aspekter har haft inverkan på diskussionens utformning.

Diskussionen inleds med att beskriva den empiriska undersökningens demografi, för att sedan kritiskt granska våra resultat i relation till det teoretiska ramverket och framförallt dess huvudområden och individuella aspekter.

5.1 Demografi

Eftersom alla respondenter var studenter har vi antagit att åldersfördelningen ligger mellan 19 och 29 år. Många yngre personer har växt upp med teknik och internet och ser det som en naturlig del i sin vardag. Därför har troligtvis denna grupp mer kunskap och vana av att använda exempelvis molnlagringstjänster. Men skulle man se till hela befolkningen lär inte användningen vara lika hög, därmed kan vårt empiriska resultat inte appliceras på hela befolkningen. Samtidigt är det fortfarande intressant att studera just yngre personer för att de använder teknik och kommer fortsätta använda det både privat och i arbetslivet i framtiden.

Jämförelsen mellan män och kvinnor och deras riskmedvetenhet visar att det inte fanns någon större skillnad bland de två mest valda riskerna. Däremot skiljer sig det genomsnittliga antalet risker mellan könen då män har valt 4,1 och kvinnor 2,8 risker. Män känner alltså i snitt till 1,3 fler risker än kvinnor enligt vår empiri. Eftersom skillnad mellan könen inte står i fokus i denna studie drar vi inga slutsatser om vad det kan bero på. Dessutom var fördelningen mellan de olika könen ojämn vilket skulle kunna göra en diskussion om skillnader mellan kön missvisande.

Sju respondenter svarade att de inte använder molnlagringstjänster. Skäl som uppgavs var ointresse eller för att de inte förstår hur det fungerar. Det är ingen av respondenterna som har svarat att de inte använder molntjänster av säkerhetsskäl vilket innebär att denna grupp inte har ett större säkerhetsmedvetande än de som använder molntjänster.

Dessa sju respondenter hade ekonomi, juridik, mänskliga rättigheter, rättssociologi eller service management som studieinriktning. Detta kan tyda på att respondenter som studerar en samhällsvetenskaplig inriktning känner sig osäkra på hur de ska hantera teknologin och väljer därför att inte använda tjänsten alls. Däremot behöver detta inte stämma då vi endast baserar det på sju respondenters svar vilket inte räcker för att generalisera eller dra några substantiella slutsatser från.

5.2 Användning

Vi kan se från enkätundersökningen att flest respondenter använder Google Drive för privat bruk samt att den näst mest valda är Google Drive via Lunds universitet. Detta kan vara en slump men det kan också bero på att Google Drive via universitetet erbjuds gratis vilket gjort användare mer vana att använda den tjänsteleverantören och därför valt att använda den även privat.

Som tidigare nämnts i bakgrunden i vår uppsats har de populära molnlagringstjänsterna väldigt många användare globalt. Detta går igen även i vårt resultat då vi funnit att 94 % av respondenterna har uppgett att de använder en molnlagringstjänst. 57 % av de som använder en molnlagringstjänst använder den dessutom varje dag enligt vår enkätundersökning. Av de respondenter som använder molnlagring varje dag eller två till tre gånger per vecka känner 15 % till sju eller åtta risker, jämfört med de som använder mer sällan eller aldrig där motsvarande andel är 0 %. Vi kan därmed se att bland de som använder en molnlagringstjänst frekvent är det cirka en sjättedel som känner till många risker, vilket kan tolkas som att denna grupp har större kunskap om säkerhetsrisker. Det finns alltså en liten grupp respondenter som är mer medvetna om risker medan det generella resultatet visar att de flesta respondenterna har en relativt låg säkerhetskunskapsgrad.

47 % av respondenterna som kryssat för att de använder molnlagringstjänster har endast markerat noll till två risker på fråga sex vilket ytterligare visar på begränsad kunskap om de säkerhetsrisker som finns med molnlagring. Detta kan tyda på att respondenterna därför har svårare för att ta ett genomtänkt beslut i avseende på säkerhetsrisker vilket stöder Coopamootoo och Groß (2014) konstaterande om att användare har svårare att fatta beslut om säkerhet online.

5.3 Informationssäkerhet och risker

Med avseende på vår enkätundersökning konstaterades det att dataintrång är den mest kända risken. Dataintrång kan relateras både till konfidentialitet samt integritet vilket även den näst mest valda risken phishing kan relateras till (Alani, 2016; Galibus et al., 2016; Jathanna & Jagli, 2017; Singh & Chatterjee, 2017). Att dessa två risker är de som valts av flest respondenter kan bero på att många fått kännedom om dem genom medias nyhetsrapportering. Det är positivt att en majoritet av respondenterna hört talas om dessa risker eftersom de har direkt påverkan på respondenternas privata data. Eftersom både konfidentialitet och integritet riskeras vid både intrång och attacker behövs medvetenhet om dessa. Båda dessa risker kan användaren också välja att vidta motåtgärder mot, som att ha en säkerhetskopia av sin data på en annan enhet eller kritiskt granska mail och därmed undvika att klicka på skadliga länkar i dem. Om övriga risker också skulle ges medial uppmärksamhet kan kunskapen om dessa öka.

Det kan diskuteras om några av riskerna som listas i enkätformuläret är metoder som leder till dataintrång. Men då vi i litteraturen funnit riskerna definierade enskilt gjordes valet att ha dem var för sig i enkäten. Resultatet att 80 % markerade dataintrång kan därmed tolkas på två sätt. Antingen tyder resultatet på att det finns en hög riskmedvetenhet då dataintrång täcker in flera av de andra riskerna. Men resultatet kan också tolkas som att många är bekanta med termen dataintrång men inte har samma kunskap om att det finns ett flertal metoder för att orsaka det, därmed kan riskmedvetenheten betraktas som lägre. Att flertalet är bekanta med termen men

inte har tillräcklig kunskap för att förstå det på ett djupare plan stämmer överens med Furnell et al. (2007).

I enkätformuläret presenteras riskerna i nummerordning från ett till nio. Om man ställer det mot resultatet att den första risken var den som blev mest vald kan det ifrågasättas om ordningen bidragit till att flest valt den. Vi är därmed medvetna om att ordningen kan ha påverkat resultatet. Ordningsföljden på riskerna i enkäten baserades på den ordning som riskerna identifierades i litteraturen. Därmed har vi inte gjort ordningen godtyckligt enligt våra egna värderingar utan baserat på teori.

De risker som valts av ett lägre antal respondenter är hackade gränssnitt och APIer samt SQL-injektioner. Dessa två risker är svårare för användare att skydda sig mot då de utförs av en hackare som vill skada tjänsten eller data. Eftersom denna typ av attacker utförs av en människa med uppsåt att orsaka skada är det svårt att skydda sig mot dem. Som motåtgärd kan såklart användare välja att inte använda tjänsten.

I vår enkätundersökning var det få respondenter som var selektiva i vilken data de laddade upp av säkerhetsskäl. En anledning till detta kan vara att användare litar på leverantören av molnlagringstjänsten och att de litar på att data som laddas upp är tryggt lagrad i molnet. Detta kan relateras till Coopamootoo och Groß (2014) som menar att användare törs ladda upp data online om den bibehålls inom samma tjänst. Därmed kan en anledning till att de flesta laddar upp all data bero på att de känner att de kan lita på leverantören och att deras data inte delas till en tredje part.

5.4 Medvetenhet

Ur enkätresultatet har vi kunnat se att fyra av respondenterna på fråga fem har svarat att det inte finns någon data de väljer att inte ladda upp ur ett säkerhetsperspektiv, sedan har de på fråga åtta svarat att de som en motåtgärd mot riskerna har valt att inte ladda upp känslig data. Dessa respondenter har alltså sagt emot sig själva. Även om det endast är fyra respondenter som har svarat detta kan det visa på en tendens att vissa av respondenterna inte har tagit ställning till hur de ska hantera risker de potentiellt kan utsättas för när de använder sig av molnlagring. Tidigare forskning har visat att användare har svårt att fatta genomtänkta beslut online eftersom att det är en väldigt komplex miljö, vilket kan vara en anledning till att vissa respondenter har svarat ambivalent (Coopamootoo & Groß, 2014).

I resultatet framkommer att cirka tre fjärdedelar (78 %) av respondenterna inte har vidtagit en motåtgärd. Detta trots att 94 % av respondenterna fyllde i minst en risk och att genomsnittet för antal risker som respondenterna valt var 3,3 stycken. Enligt James et al. (2013) har man kunnat se att även om användare känner till risker tror de inte att de kommer att drabbas av den personligen och att de därför inte behöver vidta en motåtgärd, vilket är i enlighet med vårt resultat.

Det generella resultatet visar att även om respondenterna i viss mån känner till en eller två risker påverkar det inte användningsgraden. Detta kan relateras till James et al. (2013) som menar att användare resonerar att funktionaliteten och användbarheten hos en tjänst överstiger de potentiella risker som finns med den.

Vid en jämförelse mellan hur många risker de som uppgett att de vidtagit motåtgärder och de som inte har det visar resultatet att de som vidtagit motåtgärder känner till fler risker. Andelen av de respondenter som valt en eller två risker bland de som vidtagit motåtgärder är 23 %, för dem som inte har vidtagit motåtgärder är procentandelen dubbelt så stor, 47 %. Detta visar att bland de som inte vidtagit en motåtgärd är det betydligt fler som har valt ett lågt antal risker jämfört med de som har vidtagit en motåtgärd. Ett liknande mönster finns även om man ser till dem som har valt sju eller åtta risker. Där är resultatet 27 % för de som vidtagit en motåtgärd jämfört med 8 % bland de som inte vidtagit motåtgärder. Detta kan relateras till Hanus och Wu (2016) som konstaterat att användares medvetenhet beror av deras kunskap om säkerhetsrisker i kombination med motåtgärder, vilket vårt empiriska resultat stödjer.

Ett annat resultat som relaterar till att användare inte agerar trots att de har kunskap om en säkerhetsrisk är att 80 % av respondenterna har valt dataintrång som en säkerhetsrisk de känner till, trots det har 73 % svarat att det inte finns någon data som de inte laddar upp av säkerhetsskäl. Detta visar att en stor andel av respondenterna har kunskap om de potentiella konsekvenser som kan inträffa vid molnlagring men att de inte har uteslutit viss typ av data av säkerhetsskäl. En annan anledning till att respondenterna inte vidtar motåtgärder skulle kunna vara att de uppfattar det som tekniskt svårt eller saknar kunskap för hur de skulle göra det. Detta samband har Harbach et al. (2014) konstaterat i sin studie.

Harbach et al. (2014) uppger även att det kan påverka att användare inte förstår säkerhetsriskerna fullt ut och därför inte skyddar sig. Endast 18 % av respondenterna svarade att deras kännedom om säkerhetsrisker påverkade deras val att använda en molnlagringstjänst.

6 Slutsats och förslag på vidare forskning

I detta kapitel presenteras de slutsatser som dras samt förslag på vidare forskning.

6.1 Slutsats

Vi inledde uppsatsen med att studera samspelet mellan cloud computing och informationssäkerhet, vilket formade problemområdet användares medvetenhet gällande molnlagring. Problemområdet mynnade sedan ut i vår forskningsfråga som syftar till att fastställa användares medvetenhet gällande säkerhetsrisker och på så vis påvisa relevansen av det valda ämnet. Därmed avslutas uppsatsen med att presentera forskningsfrågan igen för att sedan besvara den med hjälp av vårt teoretiska ramverk samt vårt empiriska resultat.

I inledningen av uppsatsen presenterades forskningsfrågan, vilken är:

Vilka risker med molnlagringstjänster påverkar säkerhetsmedvetandet hos användare?

Genom enkätundersökningen har vi kunnat konstatera att respondenterna känner till relativt få risker, nästan hälften av de som använder en molnlagringstjänst har valt mellan noll till två risker. Dock har nästan alla respondenter markerat minst en risk. Trots det väljer endast en femtedel att försöka skydda sig genom att vidta motåtgärder. Majoriteten av användare bryr sig alltså inte om att det finns potentiella risker med deras användande, de använder molnlagringstjänster ändå.

Trots att många användare känner till risken dataintrång kan vi konstatera att de flesta inte är selektiva i vilken data de väljer att ladda upp i molnet. Detta kan bero på att de litar på tjänsteleverantören och därmed ser molnet som en trygg miljö. Detta kan även påverkas av att användare inte tror att konsekvensen av en risk kommer att drabba dem personligen. Det finns alltså en kännedom om risker med molnlagring men användarnas medvetenhet är relativt låg då de trots detta inte väljer att agera genom att vidta motåtgärder.

Utifrån vårt resultat konstateras att kunskapen om motåtgärder generellt är väldigt låg. Detta kan mycket väl bero på att användare ser det som för tekniskt svårt. Det finns ett samband mellan att känna till få risker och att inte vidta en motåtgärd samt det motsatta, att känna till många risker och att vidta en motåtgärd, vilket stämmer väl med tidigare forskning. Därmed konstateras att användare som har kännedom om motåtgärder även känner till fler risker och är därmed mer säkerhetsmedvetna än de som endast har kännedom om ett fåtal risker.

Det har även kunnat konstaterats att de respondenter som angett att de inte använder en molnlagringstjänst har valt att göra detta på grund av ointresse eller okunskap. De har alltså inte valt att avstå från att använda en molnlagringstjänst på grund av ett högt säkerhetsmedvetande.

Våra slutsatser i korta drag är följande:

- Användare låter inte kunskap om risker påverka deras användande av molnlagringstjänster.
- Det finns ett samband mellan att vidta motåtgärder och att känna till många säkerhetsrisker. Användare som har kunskap om både potentiella säkerhetsrisker och som dessutom vidtar motåtgärder har ett högt säkerhetsmedvetande.
- De som inte använder en molntjänst gör det inte av ett högt säkerhetsmedvetande utan snarare av ointresse.

De allra flesta användare är medvetna om någon säkerhetsrisk, men inte mer än så. Endast en fjärdedel vidtar någon motåtgärd mot riskerna vilket tyder på ett generellt lågt säkerhetsmedvetande bland användare av molnlagringstjänster.

Slutligen anser vi att vårt teoretiska ramverk kan operationaliseras ytterligare i framtida studier för att kunna dra följande slutsats:

- Informationssäkerhets- och medvetenhetsaspekter borde värderas lika högt när cloud computing som teknologi används för datalagring. Vi anser att detta är ett teoretiskt bidrag eftersom tidigare studier har visat att tekniska aspekter prioriteras framför medvetenhet.

6.2 Förslag på vidare forskning

I vår studie har vi konstaterat att molnlagring är en av de huvudsakliga infrastrukturerna på marknaden som nyttjas av användare eftersom det tillåter för fillagring utan några arkitekturella begränsningar, så länge det finns uppkoppling till internet.

Andra konkurrerande infrastrukturer som IoT erbjuder möjligheter till liknande tjänster, såsom att låta enheter samla in data i realtid utan direkt användarinteraktion, som molnlagring fungerar idag och som vi fokuserat på i vår uppsats.

För att avancera studien som presenterats i denna uppsats skulle det vara intressant att undersöka hur aspekter för automatisk datalagring från en IoT-infrastruktur ses och hanteras av användare. En sådan studie skulle vara aktuell och ha en explorativ natur, med avseende på att detta forskningsområde fortfarande är nytt och tämligen outforskat.

Referenser

Aguiar, E., Zhang, Y., & Blanton, M. (2014). An overview of issues and recent developments in cloud computing and storage security. In *High Performance Cloud Auditing and Applications*. https://doi.org/10.1007/978-1-4614-3296-8_1

Ahmad, N. (2017). Cloud Computing: Technology, Security Issues and Solutions. *2017 2nd International Conference on Anti-Cyber-Crimes (ICACC)*, (:30-35 Mar, 2017).

Ahuja, S. P., & Komathukattil, D. (2012). A Survey of the State of Cloud Security. *Network and Communication Technologies*. https://doi.org/10.5539/nct.v1n2p66

Alani, M. M. (2016). *What is the Cloud?* Springer Science & Business Media. https://doi.org/10.1007/978-3-319-41411-9_1

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, (305), 357–383. https://doi.org/10.1016/j.ins.2015.01.025

AppleInsider. (2016). Apple Music passes 11M subscribers as iCloud hits 782M users. Retrieved April 18, 2018, from http://appleinsider.com/articles/16/02/12/apple-music-passes-11m-subscribers-as-icloud-hits-782m-users

Campanello, S. (2016). Dropbox ber användarna byta lösenord – läcka misstänks - IDG.se. Retrieved April 18, 2018, from https://www.idg.se/2.1085/1.664214/dropbox-losenord-byt

Coopamootoo, K. P. L., & Groß, T. (2014). Mental models for usable privacy: A position paper. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-319-07620-1_36

CSA. (2016). Cloud Security Alliance Releases “The Treacherous Twelve” Cloud Computing Top Threats in 2016 - Cloud Security Alliance : Cloud Security Alliance. Retrieved March 26, 2018, from https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/

D’Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Dropbox. (2016). Number of registered Dropbox users from April 2011 to March 2016 (in millions). *Statista - The Statistics Portal*.

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security*, 113–170. https://doi.org/10.1007/s10207-013-0208-7

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of

personal Internet users. *Computers and Security*, 410–417. https://doi.org/10.1016/j.cose.2007.03.001

Galibus, T., Krasnoproshin, V. V., Oliveira Albuquerque, R. de, & Freitas, E. P. de. (2016). *Elements of Cloud Storage Security Concepts: Designs and Optimized Practices*. https://doi.org/10.1007/978-3-319-44962-3

Gollmann, D. (2011). *Computer Security* (3rd ed.). Chichester: John Wiley and Sons, Ltd.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems, 29(7)*, 1645–1660.

Hanus, B., & Wu, Y. A. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *INFORMATION SYSTEMS MANAGEMENT*, 2–16. https://doi.org/10.1080/10580530.2015.1117842

Harbach, M., Fahl, S., & Smith, M. (2014). Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness. In *2014 IEEE 27th Computer Security Foundations Symposium*. https://doi.org/10.1109/CSF.2014.15

IDC. (2017). Worldwide Cloud IT Infrastructure Revenues Grew 14.9% to $8 Billion in First Quarter of 2017, According to IDC. Retrieved April 18, 2018, from https://www.idc.com/getdoc.jsp?containerId=prUS42831017

Jacobsen, D. I. (2002). *Vad, hur och varför : om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen*. Lund: Studentlitteratur.

James, T., Nottingham, Q., & Kim, B. C. (2013). Determining the antecedents of digital security practices in the general public dimension. *Information Technology and Management*, 69–89. https://doi.org/10.1007/s10799-012-0147-4

Jathanna, R., & Jagli, D. (2017). Cloud Computing and Security Issues. *International Journal of Engineering Research and Applications*, 31–38. https://doi.org/10.9790/9622-0706053138

Johnson, A. (2017). Google Gmail users targeted in massive phishing attack via Google Doc link. Retrieved April 18, 2018, from https://www.cnbc.com/2017/05/04/gmail-google-hack-phishing-attack.html

Johnston, S. (2012). Introducing Google Drive the newest member of Google Apps. Retrieved from https://cloud.googleblog.com/2012/04/introducing-google-drive-newest-member.html

Juniper Research. (2018). Number of consumer cloud-based service users worldwide in 2013 and 2018. *Statista - The Statistics Portal*. Retrieved from https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/.

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. In *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012*.

https://doi.org/10.1109/FIT.2012.53

Kulkarni, G., Waghmare, R., Palwe, R., Waykule, V., Bankar, H., & Koli, K. (2012). Cloud storage architecture. In *2012 7th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2012*. https://doi.org/10.1109/TSSA.2012.6366026

Kumar Sharma, P., Shankar Kaushik, P., Agarwal, P., Jain, P., Agarwal, S., & Dixit, K. (2017). Issues And Challenges of Data Security In A Cloud Computing Environment. In *Electronics and Mobile Communication Conference* (pp. 560–566).

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.

Mohamed, A. (2009). A history of cloud computing. *Computer Weekly*. Retrieved from http://www.computerweekly.com/feature/A-history-of-cloud-computing

Nationalencyklopedin. (n.d.). medvetande - Uppslagsverk - NE.se. Retrieved April 24, 2018, from https://www.ne.se/uppslagsverk/encyklopedi/lång/medvetande

Patil, T. A., Pandey, S., & Bhole, A. T. (2017). A Review on Contemporary Security Issues of Cloud Computing. *Intelligent Systems and Information Management (ICISIM)*, 179–184.

Popper, B. (2017). Google announces over 2 billion monthly active devices on Android - The Verge. Retrieved April 18, 2018, from https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users

Ramel, D. (2017). No Encryption on 82 Percent of Public Cloud Databases. Retrieved April 4, 2018, from https://virtualizationreview.com/articles/2017/05/26/redlock-security-report.aspx

Regalado, A. (2011). Who Coined "Cloud Computing"? *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/425970/who-coined-cloud-computing/

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 88–115. https://doi.org/10.1016/j.jnca.2016.11.027

Sinjilawi, Y. K., Al-Nabhan, M. Q., & Abu-Shanab, E. A. (2014). Addressing Security and Privacy Issues in Cloud Computing. *JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE*, *6*(2), 192–199. https://doi.org/10.4304/jetwi.6.2.192-199

Whittaker, Z. (2017). Apple iCloud hack threat gets worse: Here's what we've learned | ZDNet. Retrieved April 18, 2018, from https://www.zdnet.com/article/icloud-accounts-breach-gets-bigger-here-is-what-we-know/

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey. *2010 Sixth International Conference on Semantics, Knowledge and Grids Security*, 105–112. https://doi.org/10.1109/SKG.2010.19

Bilaga 1 - Enkätformulär

Enkätundersökning

Vi är två studenter som skriver kandidatuppsats inom informatik och undersöker användandet av molnlagringstjänster bland studenter vid Lunds universitet. Enkätundersökningen är frivillig att delta i och är helt anonym. Målet är att öka kunskap om inställningen till att använda molntjänster i kombination med säkerhet.

Kön: ☐ Man ☐ Kvinna ☐ Annat

Vad studerar du för ämne (t ex ekonomi, juridik etc.)? _____

En molnlagringstjänst erbjuder lagring av filer och information online. Exempel på molnlagringstjänster är Google Drive och Dropbox.

1. Använder du en molnlagringstjänst? Om nej, hoppa till fråga 6.

☐ Ja ☐ Nej

2. Om ja, vilken eller vilka?

☐ Google Drive via Lunds universitet
☐ Google Drive för privat bruk
☐ Dropbox
☐ iCloud
☐ OneDrive
☐ Annan:_____

3. Hur ofta använder du en molnlagringstjänst?

☐ Varje dag
☐ 2-3 gånger per vecka
☐ 1 gång per vecka
☐ Mer sällan

4. Vilken eller vilka av följande faktorer påverkade dina val av molnlagringstjänster?

☐ Erbjöds gratis via Lunds universitet
☐ Rekommendation från familj eller vänner
☐ Tillgänglighet
☐ Funktionalitet (t ex stöder rätt filformat)
☐ Säkerhet
☐ Annat:_____
☐ Inget av ovanstående

5. Finns det filer eller information du väljer att inte ladda upp i molnet av säkerhetsskäl?

☐ Ja ☐ Nej
Om ja, vilken typ av filer eller information?

_____

6. Nedan presenteras en lista med potentiella risker med molnlagring. Kryssa i dem som du hört talas om:

1. ☐ Dataintrång hos leverantören av molntjänsten gör att känslig information läcker eller raderas.
2. ☐ Molntjänsten överbelastas på grund av en DoS-attack (Denial of Service – angripare gör extremt många anrop på tjänsten) vilket leder till att tjänsten blir otillgänglig för användare.
3. ☐ Ett moln delas av flera organisationer vilket ökar antalet sårbarheter i lagringstjänsten.
4. ☐ Gränssnitt som används i molnlagringstjänsten kan utnyttjas av inkräktare.
5. ☐ Molnlagringstjänstens kryptering av data är bristfällig.
6. ☐ Minskad kontroll över i vilka länder personlig data förvaras. Kan därför vara svårt att kontrollera om data verkligen har raderats eller vilken lagstiftning som gäller.
7. ☐ Angripare attackerar tjänsten genom SQL-injection (att skicka in skadlig kod genom formulärfält) för att komma åt exempelvis användares lösenord.
8. ☐ Anställda hos leverantören av molntjänsten missbrukar sina behörigheter och orsakar skada på tjänsten eller kommer åt användares uppgifter.
9. ☐ Phishing - användaren klickar på en länk i ett mail som ser ut att komma från leverantören av molntjänsten. Länken leder till en falsk hemsida med inloggningsformulär där användaren luras att fylla i sina uppgifter.
10. Annan:_____

7. Påverkade din kännedom om någon/några av riskerna ovan ditt val att använda/inte använda molnlagringstjänster?

☐ Ja ☐ Nej

Om ja, skriv numren på riskerna från fråga 6 nedan:

_____

8. Om du använder en molnlagringstjänst, har du vidtagit motåtgärder mot någon eller några av dessa risker?

☐ Ja ☐ Nej

Om ja, hur?

_____

9. Om du inte använder en molnlagringstjänst, vad har påverkat detta val?

_____

Tack för ditt deltagande!

Om du är intresserad av att ta del av slutresultatet skicka ett mail till någon av oss:
jup14cni@student.lu.se
sys15ela@student.lu.se