Examensarbete

HÖGSKOLAN
I SKÖVDE

ANALYS AV MOLNTJÄNSTER UTEFTER PRESTANDA, SÄKERHET OCH INTEGRITET

Examensarbete inom huvudområdet Datalogi
Grundnivå 15 högskolepoäng
Vårtermin 2014

Anders Hermansson

Handledare: Helen Pehrsson
Examinator: Jonas Mellin

Sammanfattning

När tekniken ”cloud computing” eller datormoln först upptäcktes var det en teknik som krävde att en användare införskaffade hårdvara och kunskap för att skapa denna miljö. Denna teknik kunde inte uppfylla sin potential pågrund av en otillräcklig internetanslutning. I dagens moderna samhälle är tillgång till fiberanslutning stor och kostnaden låg vilket har lett till att antal hushåll med fiber fortsätter öka. Detta har medfört att datormoln i nutid kan vara av intresse för en hemanvändare, detta i form av molnlagring.

Det här examensarbetet undersöker prestanda, säkerhet, integritet, replikering och skalbarhet hos två olika molntjänster. Dessa molntjänster prestandatestades genom uppladdning och nerladdning av filer av olika storlek. Dessa tester gav sedan en grund för att beräkna hur responstiden förändras av ökad filstorlek, d.v.s. om responstiden dubbleras i takt med att filstorleken dubbleras är skalbarheten linjär. Vidare testades även replikering/synkronisering mellan webbgränssnitt och applikationer mellan två olika klienter. Härnäst utfördes en litteraturanalys på de säkerhet och integritetshot och brister som finns vid uppladdning hos molntjänster och hur dessa appliceras på de bägge molntjänsterna. Studien visar att sambandet mellan högre säkerhet ger en påverkan på hastighet, att skalbarheten i övervägande fall är linjär och att valet mellan molntjänster inte är en självklarhet.

Nyckelord: Cloud, jämförelsestudie, molnlagring, säkerhet

Innehållsförteckning

1 Introduktion ... 3
2 Bakgrund ... 4
2.1 Vad innebär Molnlagring? ... 4
2.1.1 Definition av Molnlagring ... 4
2.1.2 Molnets genomslag ... 5
2.1.3 Molnlagring i dagens samhälle ... 5
2.1.4 Molnanvändning i framtiden ... 5
2.2 Grundläggande frågeställning ... 7
2.2.1 Prestanda ... 7
2.2.2 Säkerhet och Integritet ... 7
2.3 Relaterad Forskning ... 7
2.3.1 Prestandarelaterade studier ... 7
2.3.2 Säkerhet och Integritetsrelaterade studier ... 7
3 Problembeskrivning ... 9
3.1 Syfte ... 9
3.2 Motivering ... 9
3.3 Mål och förväntat resultat ... 10
3.4 Delmål ... 10
3.5 Avgränsningar ... 11
3.6 Underliggande antaganden ... 11
4 Metoder ... 13
4.1 Experiment ... 13
4.1.1 Prestanda ... 13
4.2 Analys baserad på litteraturstudie ... 14
4.2.1 Säkerhet och Integritet ... 14
4.3 Validitetshot ... 15
4.3.1 Hot mot Experiment ... 15
4.3.2 Hot mot Litteraturstudie ... 15
4.3.3 Experimentell design ... 16
5 Genomförande ... 17
5.1 Litteraturstudie ... 17
5.2 Experiment ... 17
5.2.1 Installation av laborationsmiljö ... 17
5.2.2 Konfiguration ... 18
5.2.3 Utförande ... 19
6 Resultat ... 21
6.1 Uppsättning av labbmiljö ... 21
6.2 Uppladdning/Nedladdningstest i lokal miljö ... 22
6.2.1 Uppladdning och Nedladdning ... 22
6.3 Lokal lagring ... 28
6.4 Replikeringstid ... 29
6.5 Skalbarhet ... 35
7 Analys ... 38
7.1 Prestandatest ... 38

7.1.1 Uppladdningsanalys 38
7.1.2 Nedladdningsanalys 38
7.1.3 Lokal lagring analys 38
7.1.4 Replikeringsanalys 39
7.1.5 Skalbarhetsanalys 39
7.2 Litteraturanalys 39
7.2.1 Registrering 40
7.2.2 Transport 41
7.2.3 Kryptering 42
7.2.4 Delning 42
8 Slutsats 44
8.1 Sammanfattning 44
8.2 Diskussion 46
8.3 Framtida arbete 46

1 Introduktion

Molnbaserade fillagringssystem blir alltmer populära att använda både för privat och kommersiellt bruk. Denna studie ämnar att beskriva och testa de två molnbaserade lagringstjänsterna Dropbox och GoogleDrive baserat på deras prestanda, säkerhet och integritet. Är det rimligt för ett företag att lagra sina filer och/eller sina informationstillgångar hos ett externt företag? Hur är lagringshastigheten, det vill säga tiden det tar att skriva/läsa en fil jämfört med traditionella lagringssystem som till exempel HDD eller USB? Hur försvaras integriteten av dessa filer hos molnleverantören? Hur sköts samtidig tillgång till delade filer?

Genom att få svar på dessa frågor och ta reda på de svagheter och styrkor som finns hos dessa tjänster kan det sedan diskuteras om det är rimligt att dessa tjänster inom en snar framtid kan ersätta traditionell lagring eller ifall de endast bör existera som ett komplement till lokal lagring.

Till följd av populariteten och enkelheten i att skapa en molnlagringstjänst finns det väldigt många olika typer (Huth & Cebula, 2011). För att precisera studien kommer två alternativ väljas och tester därefter utföras på dessa. De molntjänster som kommer att analyseras är två av de mer välkända (Lifehacker, 2013) såsom Dropbox och Googledrive.

Dropbox blev utvald eftersom det är en relativt välkänd tjänst som används mest i den privata sektorn (Kholia & Wegrzyn, 2013). Företags specifika alternativ finns att välja men dess popularitet kommer av dess fria val och enkla användning.

GoogleDrive är en av de mest populära molntjänsterna och Google är en av de största aktörerna inom IT-världen (Lifehacker, 2013).

Dessa tjänster kommer via experiment och litteraturstudier jämföras emot varandra samt emot vanlig fillagring.

Prestandatest kommer utföras och testas med mätverktyg för prestanda mot lokal lagring och mot uppladdning och nedladdning till de olika molntjänsterna.

Säkerhet och integritet utvärderas genom litteraturstudier där dessa jämförs och testas gentemot varandra samt gentemot lokal lagring.

Därefter presenteras genomförande av experimentet och de resultat som utfåtts presenteras i form av diagram och grafer.

Slutligen avslutas arbetet med en presentation av resultat, analys och en summerad slutsats.

2 Bakgrund

Detta kapitel är uppbyggt av två delar. Den första delen beskriver kortfattat vad som menas med molntjänster och vilken påverkan det har på dagens och framtidens samhälle. Därefter följer de problem och frågetecken som finns med molnlagring. Kapitlet avslutas med en beskrivning av de tester som kommer att utföras.

2.1 Vad innebär Molnlagring?

Molnet eller molnlagring är två vaga begrepp då molnet och olika molntjänster kan innebära många olika saker. Det finns många olika definitioner, karaktäriseringar och modeller för vad moln och dess tillhörande tjänster kallas.

2.1.1 Definition av Molnlagring

För att ge vägledning och startpunkt så skriver Mell & Grance (2011) i sin artikel deras definition av all sorts molnanvändning:

> ”Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.”

Den definierade molnmodellen är enligt ovan karakteriserad av: fem viktiga egenskaper, tre service-modeller och fyra distributionsmodeller. De tre servicemodellerna som finns heter: IaaS, PaaS och SaaS. IaaS är en förkortning av ”infrastructure as a service” och är samlingsnamnet för molntjänster eller moln där en hel infrastruktur kan virtualiseras åt kunden. Kunden kan till exempel köra valfritt operativsystem med valfria applikationer och kan styra vissa hårdvaruresurser såsom processorkraft eller nätverk. PaaS innebär ”platform as a service” och till skillnad från IaaS så finns här ett operativsystem som leverantören tillhandahåller. Därefter kan användaren köra, installera eller utveckla applikationer på den redan existerande plattformen. I detta arbete ligger fokus på service-modellen SaaS ”software as a service” där fokus ligger på enbart fillagring. IaaS och PaaS är inte viktiga i denna studie då fokus ligger på filer och fillagring och då dessa modeller lämpar sig bättre för utveckling eller virtualisering av applikationer då lagringsplats och hårdvaruresurser är flexibla och kan hyras ”on-demand” (Mell & Grance, 2011).

Service-modellen SaaS innebär att användaren har rättighet att använda leverantörens applikationer och infrastruktur för eget bruk. Denna kan nås via olika verktyg såsom webbläsare, lätt klient eller ett programgränssnitt. Användare hanterar inte underliggande programstruktur såsom applikationer eller operativsystem utan arbetar enbart med hjälp av dessa verktyg. (Mell & Grance, 2011).

Anledningen till varför enbart en av tre modeller utvärderas i denna rapport är att SaaS är den enklaste av de tre olika modellerna eftersom filhantering är i fokus. Därefter har SaaS modellen valts hos de bägge leverantörerna; DropBox och Googledrive. Det är dessutom lättare att mäta prestandan hos leverantörerna då enbart standardkonfiguration används vilket leder till mindre störningar från externa applikationer.

2.1.2 Molnets genomslag

Anledningen till att molntjänster fått så stort genomslag är bland annat för att: det är enkelt att dela filer mellan kollegor, det är billigt att köpa eller hyra lagringsutrymme, gränssnittet är enkelt och filer kan uppdateras av flera parter samtidigt med flera (TrendLabs, 2012). Att analysera molntjänster kan vara till stor nytta för företag och privata användare då dokument enkelt kan finnas till hands vid risk att saker tappas bort. Ett exempel kan vara en anställd som reser i ett företagets ärende. En presentation lagras i molnet och även på ett USB-minne. Dock så tappas USB-minnet bort. Detta innebär, förutom att data försvinner, en säkerhetsrisk då känslig information kan hamna i fel händer och spridas på nätet. Data på USB-minnen kan krypteras men detta är ingen garanti för att informationen är säker då alternativa säkerhetshål kan utnyttjas (Engfors Tommy, 2011).

Eftersom filen i detta exempel är lagrad i molnet kan den anställde komma åt sin fil så fort denne får tillgång till internet. Denna fil kan också uppdateras av en eventuell projektgrupp om information behöver ändras eller läggas till.

2.1.3 Molnlagring i dagens samhälle

Molnlagring existerar och används i nuläget inom företag och privat bruk. Företag nyttjar främst IaaS och PaaS för utveckling och outsourcing på grund av dess låga kostnader medan privatanvändare nyttjar SaaS för lagring och delning av filer (Open Grid, 2009). Det är på senare år som denna utveckling skett till följd av billigare och enklare åtkomst till höghastighetsanslutning (Open Grid, 2009). Molnlagring har under det senaste decenniet slått igenom och kan i den form den existerar idag ses som den teknik som konkurrerar ut USB.

Teknologin och tankesättet med att ta med sig data oavsett vart du är har sitt ursprung i floppy disketten som var ett av de första medierna som möjliggjorde att data kunde tas med mellan datorer utan att påverka innandömet av en dator. Därefter gick utvecklingen vidare och CD-rom skivan utvecklades. Vid mitten av 2000 talet fick USB-minnen sitt stora genomslag. Priserna har minskat i takt med att lagringskapaciteten har ökat (Zetta, 2014).

Gemensamt för dessa tidigare tekniker är att en fysisk enhet behövs. Molnlagring är en teknik som finns virtuellt, som alltid kan tas med oavsett vart man är. Enda kravet är att nätverkstillgång finns och ett verktyg används (Huth & Cebula, 2011). Till följd av populariteten för denna teknik öppnar sig nya hot och säkerhetsrisker som inte finns i traditionell lagring.

I nuläget finns inte så stor kunskap om olika molntjänster och hur säkerheten hanteras (Botero-Perez 2013). Då en användare tidigare fysiskt kunde hantera data har denna kontroll nu lämnats över utanför användarens händer. Hur garanteras säkerheten då all trafik sker över internet? Vad finns det för nya anfallszoner, vad för nya säkerhetshål har upptäcks? Det är viktigt att molnlagring utvärderas, testas och undersöks så dessa frågor besvaras.

2.1.4 Molnanvändning i framtiden

Molnets framtid är god och kommer, ifall samma utvecklingshastighet behålls, säkra sin plats som ledande lagringsservice inom en snar framtid. Med framtidens molnteknik kommer nutidens teknik åldras ut och förkastas förutspår Golden, Bernard (2013). Det förutspås även att applikationsutveckling kommer att rikta in sig mot att vara molnspecifika eller delaktiga i molnet.

Till följd av denna rasande utveckling behöver den publika sektorn undervisas. Florentine & Olavsrud (2013) förutspår att 2014 är året då allmänheten får den utbildning de behöver för att kunna göra taktiska val rörande sin molnhantering och därmed forma och styra behoven för framtida molnutveckling. Det är författarens förhoppning att detta examensarbete kan ge en inblick i vad för säkerhetsaspekter som behöver undersökas samt vilka prestandaskillnader som är av vikt vid val av en molntjänst.

2.2 Grundläggande frågeställning

Denna sektion beskriver den grundläggande frågeställningen runt hur bägge molntjänster kommer att testas.

2.2.1 Prestanda

Prestanda testas genom åtkomsttid, det vill säga hur lång tid tar det att nå en fil i molnet gentemot en lokal fil. Hur många användare kan hantera en fil samtidigt utan problem? Hur lång tid tar det att skriva en fil och vad finns det för gränser inom molnprestanda? Hur ser skalbarheten ut beroende på filstorlek? Mer om detta i sektion 4.1.1.

2.2.2 Säkerhet och Integritet

Hur garanteras säkerhet hos molnleverantörer? Lagras viktiga filer öppet eller krypterat? Finns det några alternativ hos molntjänsterna som påverkar graden av säkerhet? Detta undersöks via litteraturundersökning för att se vad för sorts hot och vilka säkerhetsåtgärder leverantörer har införskaffat för att skydda mot dessa. Argumentation, lösningar eller hantering av dessa brister kommer diskuteras. Mer om detta i sektion 4.2.1.

Integriteten av ett dokument är ett dokuments riktighet. Hur behandlas integriteten av ett dokument när det befinner sig i en delad molnmiljö? Finns det något skydd för att data inte raderas avsiktligt eller oavsiktligt av en medlem i molnet? Detta kommer undersökas i bägge tjänster genom att se i de olika tjänsterna vad det finns för synkroniseringsmöjligheter. Finns det någon möjlighet att återskapa förlorad data som skrivits över i ett delat dokument i molnet eller behövs det kontinuerlig säkerhetskopiering för att undvika att information tappas bort. Finns det någon överföringssäkerhet? Mer om detta i sektion 4.2.1.

2.3 Relaterad Forskning

Denna del diskuterar relaterat arbete till molntjänster och tester på dess prestanda, säkerhet och integritet.

2.3.1 Prestandarelaterade studier

Google (2012) har släppt information om hur deras tjänst Google Drive fungerar. De går dock inte in på eventuella brister (av uppenbara skäl). De benämner de fördelar som finns med Google Drive. (Google, 2012).

Open Grid (2009) förklarar hur ett molnssystem fungerar och informerar om brister och fördelar med molnlagring. Denna är dock likt (Huth & Cebula, 2011) en generell bild av molnlagring. Clouddrive (2013) visar oss fördelar och nackdelar med generell molnlagring.

2.3.2 Säkerhet och Integritetsrelaterade studier

Kholia och Wegrzyn (2013) analyserar säkerheten hos Dropbox genom att hacka Dropbox och komma åt användarens filer. De fokuserar dock inte på prestandan eller integriteten i Dropbox. Mahajan et al. (2012) utvecklar ett eget molnlagringssystem för att lösa problem inom integritet, prestanda och säkerhet. Denna artikel riktar sig mot företag och testar även denna lösning. Dock så testar den inte nuvarande tekniker utan de skapar en egen lösning.

Huth och Cebula (2011) beskriver hur molntjänster fungerar och vilka typer av moln som existerar. De förklarar även bitvis hur säkerhet hanteras i molntjänster. Denna bit ger dock ingen ny insikt utan nämner enbart att man bör undersöka de säkerhetsåtgärder som leverantören av tjänsten erbjuder. (Huth & Cebula, 2011).

Borgmann et al. (2012) ger en bild av säkerhetsproblem inom molnlagring. Denna artikel utvärderar ett flertal tjänster beroende på vissa kriterier. Dessa betygsätts sedan utefter ett poängsystem. Även internationella lagar nämns och förklaras. Detta kommer att komma till nytta då test hos företag eller privat användare sker då internationella lagar och regler behöver följas och även då ett liknande tillvägagångssätt kommer att användas för att utföra analys av litteraturstudier (Borgmann et al, 2012).

3 Problembeskrivning

Detta kapitel beskriver syftet med arbetet och förväntat resultat.

3.1 Syfte

Syftet är att undersöka molnlagringstjänsterna Dropbox och Googledrive utefter systemattributen prestanda, säkerhet och integritet. Av detta kan det jämföras hur molntjänster mäts emot traditionell lagring.

3.2 Motivering

Ett faktum som i nutid existererar i datorvärlden är att data behöver lagras på ett medium. Det finns olika typer av lagring men hur mäter sig molnlagring mot dessa? Liknande undersökningar har gjorts men dessa har testat prestanda eller enbart säkerhet. Det är viktigt för privatpersoner och företag att veta hur data hanteras med tanke på ovan nämda systemattribut då deras data med denna teknik färdas över internet och lagras i ett annat företags hårdvara.

Molnlagring är en lagringsteknik som fått sitt genomslag tack vare dagens IT-infrastruktur. Detta har till stor del påverkat lagringsresonemanget eftersom lagring nu följer en pågående trend som vill undvika att lagra data lokalt, som tidigare ansetts vara säkrast och effektivast, till att vara online och alltid tillgänglig (Huth & Cebula, 2011). Därför är det intressant att undersöka och jämföra populära molntjänster gentemot varandra. Molnlagring är ett alternativ till följd av en allt större allmän tillgång till höghastighetsfiber. Detta gör att tidigare dyr teknik kan spridas till privatpersoner och företag. Privatpersoner kan skapa egna molnlagringstjänster och sprida dessa. Följden av detta blir en kontinuerligt ökad ”soppa” av tjänster där den ena tjänsten inte kan jämföras med den andre.

Få studier har gjorts då molntjänster har utvärderats mellan varandra eller med traditionell lagring (Drago et al, 2012). Möjligtvis då det är svårt att bestämma sig för vilka tjänster eller servicemodeller som ska utvärderas. I denna studie valdes två stycken populära tjänster för både privat och kommersiellt bruk.

Dropbox valdes som privat molnlagringstjänst då det var en av de första som slog igenom som en privat molntjänst (Drago et al, 2012). Därför är det intressant att se hur den presterar när de olika testen genomförs. Finns det någon egentlig skillnad enligt de kriterier detta arbete behandlar emellan en tjänst riktad mot privatpersoner gentemot en riktad mot företag.

Googledrive valdes då den tjänsten enligt flera kända tidskrifter blivit rankad som ledande tjänst riktad mot företag (Bort, 2013 & Butler, 2013).

3.3 Mål och förväntat resultat

Målet med studien är att få svar på hur två olika molntjänster rankas gentemot varandra med avseende på prestanda, säkerhet och integritet. När svaret på detta fås kan det jämföras hur resultat mäts emot traditionell lagring. Har molntekniken avancerat till den grad att traditionell fillagring rankas jämlikt med molnlagring? Finns det någon definitiv vinnare av de olika molnlagringsleverantörerna?

Förväntat resultat är att Googledrive är den som kommer prestera bäst då Google är en av världens största företag med stor hand i utformingen av IT-världen. En hypotes är att dagens molnlagring står sig jämt emot traditionell fillagring såsom HDD eller FLASH. Däremot att SSD-diskar, som blir alltmer populära och vars prissättning minskar bör vara mest effektiv prestandamässigt.

3.4 Delmål

För att prioritera studien delas arbetet upp i olika delmål.

1. Det första delmålet för denna studie är att utföra ett prestandatest genom uppladdning och nedladdningstest mellan de olika molntjänsterna. Denna bör vara så omfattande som möjligt för att erhålla ett tillräckligt tillförlitligt resultat.

2. Det andra delmålet är att utföra en analys av säkerhet och integritet baserat på en litteraturstudie. Detta genom att analysera vetenskapliga och tidsskriftartiklar för att ta reda på allmäna svagheter och säkerhetsbrister som finns inom molnlagring.

3. Det tredje delmålet är ett prestandtest mellan molntjänsterna och traditionell lagring.

4. Det fjärde delmålet är att uföra en skalbarhetsjämförelse mellan bägge molntjänster samt lokal lagring. Detta för att ge svar på hur responstiden förändras till följd av att filstorlek ökar.

5. Det femte delmålet utvärderar replikeringshastigheten mellan molntjänster. När en fil laddas upp på en molntjänst, hur lång tid tar det innan denna replikeras på en annan dator?

6. Det sjätte delmålet är att undersöka vilka specifika säkerhetsrisker/svagheter det finns för varje molntjänst. Detta för att se ifall det finns några specifika svagheter som sevärt kan påverka säkerheten hos molntjänsten.

Delmål 1-3 är ett krav för att uppnå studiens syfte och kommer prioriteras på att utföras först. Delmål 4 är en påbyggnad av prestandatestningen och bör genomföras i mån av tid. Skalbarheten anger hur prestanda förändras vid ökad belastning (i detta fall av ökad filstorlek). Detta delmål utförs genom att samla data från Delmål 1,3 och 5, detta för att mäta tidsintervallet eller den faktoriska ökningen mellan de olika tjänsterna. Exempel är: Om en fil på 50MB tar 10sekunder att ladda upp och nästa fil på 100MB tar 20sekunder så är skalbarheten jämn det vill säga responstiden för uppladdning skalar med filstorleken. Delmål 5 hanterar replikering av filer när de redan finns på en delad molnplattform. Detta mål ses därefter som en bonus att lösa då den kan ge intressant information om prestanda men inte större bidrar till det ursprungliga syftet. Delmål 6 ämnar bygga vidare på litteraturstudien. Denna ses som svår att genomföra då stor kunskap krävs om varje molntjänsts

säkerhetsrutiner, uppbyggnad och struktur. Därför hanteras den enbart då mån av tid finns och i det fall där litteraturstudien i delmål 2 ger ett otillfredställande svar på frågeställningen.

3.5 Avgränsningar

Eftersom området ”cloud computing” är ett brett ämne med många olika modeller och servicetyper har det behövts avgränsningar i arbetet för att kunna prioritera att syftet besvaras i den tid som blivit tilldelat för arbetet.

En av avgränsningarna är att enbart fokusera på servicemodellen SaaS och fillagring. Detta för att då de andra servicemodellerna inte fokuserar på fillagring saknas kunskap och tid för att korrekt utvärdera dessa.

En annan avgränsning är att studien inte behandlar ekonomiska aspekter. Bägge molnleverantörer har olika serviceavtal där lagringskapacitet och resurser kan minskas eller ökas beroende på kapital. För att undvika detta används den gratisversionen som bägge molntjänster använder. Det kan vara intressant att jämföra molnlagringskostnad gentemot vad lokal lagring, exempelvis hårddisk eller USB, hade kostat i jämförelse. Detta ger dock inte svar på studiens syfte.

Nästa avgränsning är test eller experiment av en molntjänsternas säkerhet. De säkerhetshot och svagheter som kommer att beskrivas i litteraturstudien skulle till viss mån kunna replikeras i en laborationsmiljö för att undersöka hur fillagringen påverkas och vilka konsekvenser ett sådant angrepp hade innebärt. Anledningen att detta har avgränsats är pågrund av tidsbegränsning och av lagliga skäl. Tidsbegränsningen berör både studiens omfattning och den tid det skulle ta för skribent att få den kunskap som krävs för att korrekt utvärdera detta. Lagliga skäl att undvika att testa detta är då publika molntjänster används så kommer ett angrepp ske mot ett företag.

Näst sista avgränsningen är valet att utvärdera två stycken molntjänster. Det finns många olika molntjänster och molnleverantörer med många olika serviceavtal och regler. Valet att analysera två molntjänster togs för att prioritera att syftet uppnås inom den tid som blivit tilldelad.

3.6 Underliggande antaganden

Till de olika tjänsterna och generellt över dessa finns det ett antal underliggande antaganden som behöver diskuteras.

Det första är att tjänsterna kräver någon form av betalning för att få en utökad storlek för lagring. Tjänsterna erbjuder en storlek gratis men påverkar en betalningsplan säkerhet eller prestanda? Detta undersöktes och svar erfåddes att prestanda och säkerhetsmässigt är det inga skillnader mellan gratis och betalningsplan för bägge tjänster. Eftersom gratis versionerna av bägge tjänster ska testas utformades filstorlekar av detta då 5GB är maximalt lagringsutrymme för Dropbox (Dropbox, 2014).

Ett annat antagande är att säkerhet lämnas ut till leverantören. Detta medför att ingen kryptering av filer utfördes på klient sidan utan detta ansvar lämnades över till leverantören. Detta medför att leverantörens säkerhet analyseras och inte den som laddar upp en fil.

Ytterligare ett antagande är att tjänsterna kräver att klienter är online, det vill säga har en fungerande nätverksanslutning. Detta då tjänsterna hanteras primärt via internet och därefter kan inte prestandatester utföras om det inte finns någon internetförbindelse. Filer som redan är nerladdade kan nås men uppladdning, nerladdning, replikering och skalbarhet kan inte mätas.

4 Metoder

För att testa de molnbaserade tjänster som bestämts kommer en blandning av kvantitativ och kvalitativ metodik användas. Till en början utvärderas de olika molntjänsterna beroende på de kriterier som nämnts tidigare därefter beskrivs vilka hot som finns mot validiteten.

4.1 Experiment

Experiment kommer att användas för att mäta prestanda mellan de bägge molntjänsterna samt mätning av lokal lagring. Detta då material för detta är relativt lätt att tillgå samt att resultat kan mätas och presenteras via diagram och tabeller.

4.1.1 Prestanda

Utförandet kommer att ske med hjälp av tester av varje molntjänst. För detta ändamål behövs det ett antal virtuella maskiner eller klienter för att testa en tjänsts prestanda. Detta för att kunna få en testmiljö för att kunna uföra tester. Detta för att ge svar på delmål 1 ”Hur lång tid tar det att ladda upp och ned en fil till molntjänst X?

Eftersom molnlagring används så kan den största flaskhalsen uppstå då många försöker skriva eller ändra till en delad nätverksresurs samtidigt. Detta kan påverka delmål 5 där replikering mäts. En ytterligare flaskhals kan vara då en ADSL anslutning används eller när uppladdning och nedladdningshastighet inte är densamma. Detta resultat kan variera beroende på bandbredd, storlek på fil och antal som skriver eller försöker få tillgång till en specifik fil. Därför bör först en vanlig filåtkomst ske till en relativt liten fil till exempel en textfil lokalt lagrad på dator. Detta bör ske på så många olika hårddiskar och hårddisktyper som möjligt såsom SSD, HDD, RAID 0 och så vidare. Därefter testas åtkomst emot samma fil fast lagrad i en molnlagringstjänst. Av resultatet kan det sedan utläsas vad det är för prestandaskillnad på en användare som lagrar en liten fil i bägge lagringsteknikerna. Steget efter är att antalet testklienter ökas och antal filåtkomster/skrivningar till filer ökar och prestandaskillnaden antecknas.

För att få ett så specifikt värde som möjligt och öka tillförlitligheten av experimentet bör 5st tester köras per lagringtyp och därefter ett medelvärde beräknas, detta för att få svar på delfrånga 3 ”Hur förhåller sig lokal lagring gentemot molnlagring?”. För att mäta hastighet mot lokal lagring används ett mätverktyg för prestanda: ”CrystalDiskMark” (CrystalDiskMark, 2013). Detta mätverktyg har valts utefter popularitet och enkelhet (Smith, Matt 2010).

För att mäta hastigheten vid molnlagring utförs två test. Ett uppladdningstest och ett nedladdningstest. Dessa test genomförs först med en liten fil på 50MB. Därefter en större på 100, 250, 500, 1000 och sedan 2000MB. Sedan jämförs uppladdningstiden emellan dessa. Genom att köra, likt ovan, 5 olika test bör detta även lösa problemet med att nätverkshastighet delas av andra deltagare från nätverksleverantören och att hastigheten då kan förändras under testets gång. (Krawczyk, 2013). Att filstorlekar ökar proportionellt emot varandra och att flera tester utförs ger svar på delmål 4 ”Vad har molntjänster för skalbarhet och hur påverkas responstiden av filstorlek?”.

Hypotetiskt bör prestanda minska ju fler som använder tjänsten. Skillnaden mellan olika lösningar och hur stor denna prestandaskillnad blir är av intresse för denna del. Det förväntade resultatet är att prestanda kommer att vara likvärdig både vid molnlagring och

lokal lagring. Detta på grund av tillgång till en snabb internetanslutning via fiber. För att se en negativ påverkan på en molntjänst är det troligt att antalet som skriver en fil samtidigt är väldigt hög och det kan vara svårt att utvärdera var denna gräns går.

Information som samlas in i detta stadie är skrivtid, det vill säga hur lång tid det tar att skriva en fil till hårddisk. Denna tid jämförs sedan med tiden det tar att skriva en fil till en molntjänst. Möjliga alternativa metoder eller tilläggsmetoder kan vara att flytta filer mellan två HDD på en lokal dator gentemot att flytta en fil mellan de olika molntjänsterna eller emellan olika delade mappar på en av tjänsterna.

Vid prestanda test är det även av intresse hur skalbarhet påverkas. Förändras skalbarheten emellen filstorlekar eller paralellitet? Denna fråga tas upp och presenteras närmare i delmål 4 och är av intresse för att kunna bevisa när och om skalbarheten påverkas av filstorlek eller filmängd. Delmålet är inte en del av frågeställningen och kommer därefter att testas inom tiden som utgetts för studien.

4.2 Analys baserad på litteraturstudie

Säkerhet och integritet kommer att utvärderas primärt genom en analys baserad på litteraturstudier. Detta genom att jämföra och sammanfatta och analysera nuvarande utvärderingar och sammanfoga dessa.

4.2.1 Säkerhet och Integritet

Vid test av säkerhet hos en tjänst bör först tidigare studier granskas. Information bör först sökas brett, det vill säga nyckelord såsom ”issues with cloud-computing” eller ”cloud-computing security”. Därefter kan sökning preciseras genom att söka efter rättsliga fall eller tidningsartiklar om det finns incidenter där detta hänt och om detta är fallet vilken leverantör eller tjänst som användes. Slutligen kan nyckelord preciseras beroende på de olika tjänsterna som till exempel ”security issues with Dropbox”. Detta ger information för att få svar på delmål 2 ”vad för säkerhetsproblem/brister finns det i de olika molntjänsterna?”.

Ett exempel på detta är då Kholia och Wegrzyn (2013) skriver i sin artikel hur DropBox-konton kan hackas och information spridas. Har dessa svagheter uppdaterats i DropBox efter artikeln publicerats och är dessa säkerhetshål generella för samtliga molntjänster eller är de specifika för DropBox? För att få svar på detta bör ett flertal artiklar analyseras och sammanfogas för att se vad för svagheter som fanns vid artikelns publisering och vilka svagheter som fortfarande finns kvar. Därefter bör en undersökning ske vad för sorts säkerhetsrisker som finns emot lokal lagring. Kan molnlagring vara ”dyrare” säkerhetsmässigt eller är det lokal lagring som har störst säkerhetsbrister?

Förväntat resultat är att intern säkerhet är mer pålitlig än extern, detta främst inom kommersiellt bruk. Detta då filer kan lagras i en säker zon som t.ex. en DMZ (demilitariserad zon) som är ett isolerat subnät placerad utanför ett internt nät, eller på en server som befinner sig bakom ett företags totala skydd mot angrepp med skydd som brandvägg, IDS (intrusion detection system) som upptäcker potentiella angreppsförsök och så vidare. Detta behöver inte innebära att en molntjänst är osäker eller inte säker nog för att ett företag ska lita på den. För att ta reda på detta bör eventuella säkerhetsbrister och existerande säkerhetsåtgärder dokumenteras. Denna informationshantering bör vara så kvalitativ som möjligt.

Vid privat bruk är säkerhet förmodligen bättre hos molntjänsten, dock så är den mer utsatt för hot än en privat användare. Konsekvensen av förlorad data för en privat användare är svår att sätta ett värde på, det beror på vad för sorts information som lagras. Denna

informationshantering bör vara kvantitativ för att kunna sammanställa information från många olika källor till ett diagram eller graf.

Integriteten analyseras genom att undersöka relaterat arbete. Denna information ska sedan sammanställas och beskrivas. Detta bör ge svar på hur användare hanterar information i filer och ifall dessa kan återställas vid ändringar. Bör även ge insikt i delmål 2: ”hur försvaras integritet i en molntjänst? Vad finns det för lösningar om information skrivs över? Vad händer om ett dokument blir korrupt? Hur hanteras åtkomst av dokument när tillgång till internet är begränsad? Har molntjänster en säkerhetskopiering av ett företags externa filer och om så är fallet, vad innebär detta för eventuell risk mot företagets policy och mål?

Förväntat resultat är att integritet är säkrare vid lokal lagring då eventuella säkerhetskopieringar kan schemaläggas direkt utan inblandning av en tredje part.

Information som behöver samlas in är om leverantörer av molntjänster säkerhetskopierar data eller har något slags integritetsskydd. Detta genom att undersöka existerande dokumentation.

4.3 Validitetshot

Denna sektion listar de eventuella validitetshot som finns emot de tillvägagångssätt som listats för att utvärdera molntjänsterna.

4.3.1 Hot mot Experiment

Möjliga hot mot experiment är då dessa tjänster är publika moln så kan hastigheten fluktuera beroende på antalet som använder tjänsten. Detta validitetshot kan vara svårt att eliminera, dock så kan tester upprepas vid olika dagar och olika tider för att öka validiteten.

Ytterligare hot är då tester utförs på ett nätverk där anslutningen delas emellan användare. Hastigheten som en serviceleverantör leverar kan fluktuera beroende på den last som ligger på nätverk vid någon given punkt. Även detta hot kan åtgärdas likt ovan genom att testa på olika dagar och tider. Samt så kan tester även utföras på en dedikerad nätverksanslutning i labbmiljö ifall tidigare resultat visar sig vara osammanhängande.

Ett annat hot är om de paket som molnleverantörerna marknadsför skiljer sig i basprestanda. Ett exempel är om Dropbox tillåter 10MB/S medan Googledrive tillåter 15MB/S. Detta påverkar då resultatet innan experiment ens utförs. För att åtgärda detta valididetshot bör det undersökas om en likvärdig startposition för bägge tjänster kan anordnas. Om inte så är fallet kan de värden som uträknas beräknas med tanke på de begränsningar som finns.

De enda dokumenterade skillnaderna mellan Googledrive och Dropbox är lagringskapaciteten hos ett nyskapat gratiskonto. Googledrive ger 5GB medan Dropbox ger 2GB. Däremot så kan Dropbox kontot utökas genom sociala medier och spridning till vänner vilket kan ge mer utrymme. Googledrive ger enbart 5GB, vid ett större lagringsbehov behövs en betalningsplan användas.

4.3.2 Hot mot Litteraturstudie

Eventuella hot mot litteraturstudie är ifall ett påstående som beskrivs inte stöds upp av flera källor. Detta kan då bli ett hot mot källvaliditeten. Därefter bör dessa enbart nämnas i korthet med fokus att de inte täcks av flera källor och istället läggs fokus på att beskriva de påståenden där källvaliditet kan bekräftas.

4.3.3 Experimentell design

Experimentet har utförts utefter en slumpmässig design, det vill säga tester har utförs vid olika tidpunker med diverse tester. Detta tillvägagångssätt bör minska yttre påverkan på de resultat som utvunnits och en generell påverkan kan ses (Wohlin, 2012).

I tillägg används även balansprincipen, detta eftersom flera tester utförs för att bekfräfta validiteteten. För detta används flera tester, i detta arbete i form av 5 upprepningar av varje test, där samma faktorer mäts för varje test. Denna princip har valts eftersom att om ett test utförs kan resultatet av detta påverkas internt: om en bakgrundsprocess tar upp bandbredd eller lagringssutrymme, eller externt: om antalet användare som använder tjänster påverkar hastighet. Det kan argumenteras att antalet tester kunde varit fler pågrund av en osäker yttre påverkan då antal användare som använder tjänsten inte kan beräknas vid en viss tidpunkt, men vid utförande av tester visades resultat vara väldigt jämna, i tillägg visas variationerna i resultaten i form av spridningsdiagram i resultatsektionen.

Ovanstående principer hanterar möjligheten till generalisiering, det vill säga den externa validitieten: Gäller resultaten över tid, populationer och olika miljöer? (Wohlin, 2012). Eftersom både balans och slumpmässiga principer har valts bör resultaten (om de är liknande) gälla över tid. Resultat över populationer är svår att validera då inga siffror existerar på hur många användare som använder tjänsterna under en viss tidpunkt på en viss plats. Olika miljöer beror på skillnaden mellan dessa, resultat tros påverkas beroende av nätverkshastighet och nätverksskort. Ifall lagringsmedia eller någon annan intern variabel påverkar resultatet kan validiteten försämras (svar på detta erfås efter tester har utförts).

En annan form av validitet som berör arbetet är konstruktionsvaliditetet, det vill säga: Är slutsatser kring experimentets konstruktion och operationaliseringar korrekta? (Wohlin, 2012). Denna form är svårare att validera då få undersökningar har gjorts emot de två molntjänster som valts. I experimentet används Windows som operativsystem. Datorsystemen som test utförs på är däremot inte i sin standardkonfiguration, det vill säga tjänster oväsentliga för testning är installerade. För att motverka påverkan av dessa tjänster övervakas filöverföringar med hjälp av Windows aktivitetshanterare där hårdvaruanvändning mäts i realtid. Om nätverk och lagringskapaciteten ligger på 0 % resursanvändning kan det ge en bättre konstruktionsvaliditet.

5 Genomförande

Detta kapitel kommer ta upp hur studien har genomförts. Kapitlet är uppdelat i två delar: litteraturanalys och experiment.

5.1 Litteraturstudie

Litteraturanalysen har genomförts genom att studera och granska de litterära verk som avser ämnet. Viss information har tagits från molntjänsternas egen dokumentation angående säkerhet och integritet, dock så har denna information varit sparsam. Som komplement har därefter ett flertal artiklar analyserats både specifikt mot dessa molntjänster men även emot molnteknologin i allmänhet.

Informationen som utvunnits ur litteraturanalysen har sedan lett till det resultat som presenteras i kapitel 7.2.

5.2 Experiment

Denna sektion avser beskriva hur experimentet genomfördes. Sektionen är uppdelad i delsektionerna: installation, konfiguration och utförande.

5.2.1 Installation av laborationsmiljö

Laborationsmiljön består av två klienter som agerar som testmaskiner. En av klienterna är en stationär dator som kommer att ladda upp och ner filer. Klientens resurser innefattar:

CPU	Minne	Nätverkskort	Operativsystem	Lagringsmedia
Intel Core i7 920 @ 2.67GHz	6GB DDR3 1333MHz	Broadcom Netlink Gigabit Ethernet	Windows 8.1 64bit	2x SSD: Corsair Force Series, 555/515MBps, 120GB NTFS (D: och E :)
				2x HDD: Western Digital, 7200RPM, 500GB NTFS (F: och H:)
				USB: Corsair Flash Voyager, USB2.0, 32GB NTFS

Denna klient befinner sig på 100/100Mbit internetuppkoppling mot studentnätet i skövde (SHS) som hanterar anslutningen från internetleverantören SUNET. Vid bandbreddstest, testad: 15/4 2014 13:52, så är: nedladdnings hastighet: 94.61Mbps och uppladdningshastighet 93.96Mbps.

Den anda testmaskinen är en bärbar dator och kommer användas för att mäta replikeringshastighet.

CPU	Minne	Nätverkskort	Operativsystem	Lagringsmedia
Intel(R) Core(TM) i5 CPU @2,40GHz	4GB DDR2 1066MHz	Realtek PCIe FE Family Controller	Windows 8.1 64bit	HDD: Western Digital 5400 RPM, 300GB NTFS

Denna klient befinner sig på samma internetanslutning som klienten.

5.2.2 Konfiguration

Testmaskinerna installeras med ett operativsystem av typen 64bit och installerades på olika hårddiskar, det vill säga ingen virtualisering användes. Detta för att få ett resultat baserat på grundprestanda utan att någon process eller virtualisering påverkar resultatet. För att nå molntjänsternas webbgränssnitt används Google Chrome (v34.0.1847.116 m) då det anses vara den mest använda webbläsaren (W3schools, 2014).

Bägge tjänster har en applikation som kan köras hos en klient. Denna kommer användas primärt för att mäta uppladdning, nedladdning, skalbarhet och replikeringstid. Dessa applikationer installeras på de testmaskiner som används. Dessa applikationer använder sin grundkonfiguration, detta för att få ett så grundläggande svar som möjligt.

Hårddiskmätningen använder mjukvaruprogrammet CrystalDiskMark (Crystal Dew World, 2014). Denna valdes då användargränssnittet var enkelt att använda och man kunde specifiera tester med filer av olika filstorlek vilket gjorde det enklare att få fram medelvärde för läs och skrivhastighet. Detta program installeras även dessa på klienter i sin grundkonfiguration.

Överföring av filer till molntjänsternas applikation sker med hjälp av mjukvaran Robocopy (Microsoft, 2014). Robocopy är en mjukvara som kan automatisera filuppladdning emot en hårddisk. Anledningen till detta är att exakt tidpunkt kan preciseras och alla överföringar som utförs i detta program tidstämplas, det vill säga tiden en överföring tar mäts upp till sekunder. I tillägg så mäts även överföringshastighet i bits/sekund. Dessa funktioner kan även schemaläggas i Windows Task Manager.

För att mäta replikering, nedladdning och uppladdningshastighet för de olika metoderna kommer molnapplikationens webbgränssnitt användas för att läsa av tidsstämplar. Dessa resultat verifieras även med en manuell tidsmätning.

Ifall resultaten påverkas till följd av lagringsmedia används mjukvaran Imdisc (Ltrdata, 2014). Denna mjukvara kan virtualisera en partition av RAM minne och valdes på grund av att det var enkelt att installera och sätta upp en virtuell HDD med denna mjukvara. Resultat kan påverka om det vid t.ex. replikering visar sig att HDD resursanvändande konstant ligger på 100%. Denna metod utförs enbart om hårddiskkapacitet visar sig vara en flaskhals.

De filer som ska användas vid utförande av tester skapas av mjukvaran ”Dummy File Creator” som är en mjukvara som kan skapa särskilda ”dummy” filer, filer som inte har något syfte utan bara är data. Detta program blev valt eftersom den är utvecklad för att skapa filer som är ämnade åt att testa nätverk eller hårddiskkapacitet (Mynikko, 2014).

5.2.3 Utförande

För att utföra experimentet används sex stycken olika filer på 50, 100, 250, 500, 1000 och 2000MB storlek. Detta för att få så många mätvärden som möjligt och för att kunna mäta skalbarhet. Filstorlekarna dubbleras (med undantag för 100-250MB på grund av simplicitet) tills dess att max filstorlek 2000MB har uppnåtts för att få en så bred uppfattning som möjligt vart eventuella skalbarhetssvagheter finns, det vill säga hur stor behöver en fil vara innan skalbarheten påverkas. Varje test utförs fem gånger och därefter väljs ett medelvärde.

Robocopy används genom att specificera två olika mappar. I detta fall blir den lokala mappen den mapp innehållande den fil som ska testas. Destinationsmappen är den delade mapp som skapats i samband med att molntjänstapplikationen installerades. För att köra programmet vid en specifik tidpunkt används som tidigare nämnt Windows Task Manager. Programmet schemaläggs under en bestämd tidpunkt och överföringsstatistik kan sedan avläsas i Windows Task manager och i en dedikerad loggfil.

För att beräkna ett medelvärde utförs tester fem gånger. Därefter räknas medelvärdet ut genom formeln:

$$\frac{Test1+Test2+Test3+Test4+Test5}{5}=Medelvärde$$

Denna metod räknar enbart ut uppladdningshastighet till molnapplikationens mapp. För att mäta replikeringstid och uppladdning direkt till gränssnittet används som tidigare nämnt applikationernas egna loggar samt en manuell metod. För att sedan beräkna hastigheten används formeln:

$$\frac{Filstorlek}{Tid\ I\ sekunder}=xMB/s$$

För att testa lokal lagring används CrystalDiskMark för att mäta lagringsmediumets prestanda. Testen utförs likt ovan 5gånger med 6 olika filstorlekshastigheter och med en typ av ”benchmark” kallad ”sequential”. Detta eftersom det är den vanligaste typen av filläsning och som används vid försäljning av HDDs (Userbenchmark, 2014).

Replikering testas genom formeln: uppladdningstid + replikeringstid. Det vill säga tiden det tar för att ladda upp en fil + tiden det tar för denna fil att replikera sig över molntjänsten. Denna formula har valts eftersom replikering av filer påbörjas så fort en liten del av den totala filen laddas upp. Till följd av detta behöver beräkning börja när uppladdningen startar. Färdig replikering är när filens totala storlek har replikerats till molntjänstens webbinterface samt till andra datorer som kör samma molntjänstsapplikation.

Skalbarhet räknas ut med hjälp av statistik från de första testerna. Eftersom filstorleken ökar proportionellt kan det räknas ut hur skalbarhet påverkas av filstorlek eller andra faktorer.

Samtliga tester utförs då belastning på berörda tjänster är så låga som möjligt. Detta kan ses i ”task manager” i Windows.

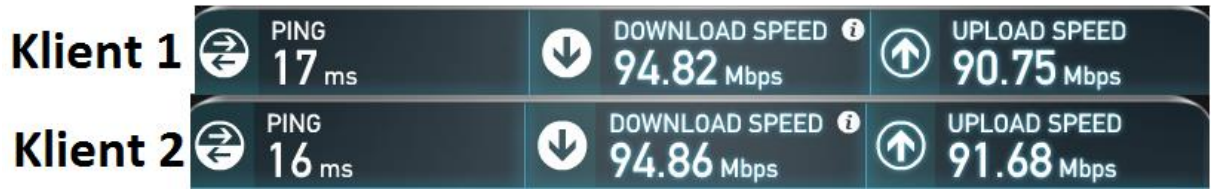
De stapeldiagram som presenterar resultaten är färgkodade och mönsterbaserade. Detta för att göra det lättare vid presentation av data då till exempel färgblinda kan ha svårt att skilja på vissa färger.

6 Resultat

Denna sektion presenterar en sammanställning av resultaten från prestandatester. Den börjar med en introduktion av uppsättning av labbmiljö. Sedan presenteras prestandatester och förklaras samt illustreras i form av grafer eller tabeller.

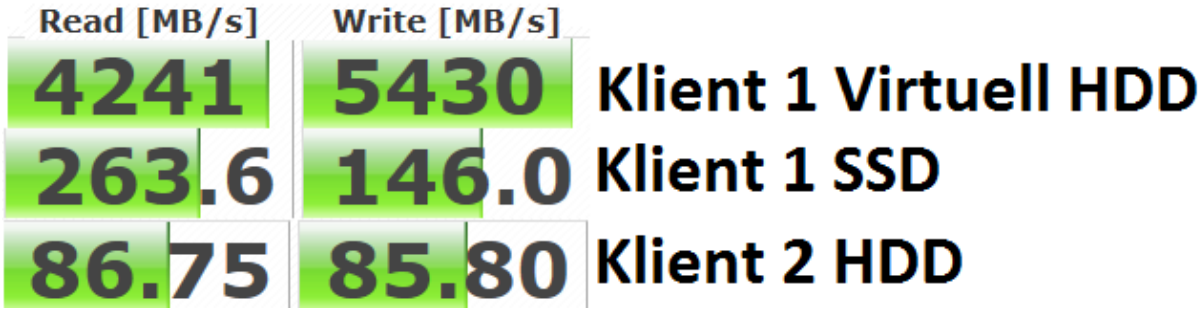
6.1 Uppsättning av labbmiljö

För att säkerhetsställa validiteten och för att redan i början borträkna eller ha i åtanke eventuella skillnader har prestandatest genomförts och jämförts mellan klient 1 och klient 2(se sektion 5.2.2). Det första testet som utfördes var ett bandbreddstest.



Figur 1: Resultat av bandbreddstest.

Resultaten från bredbandstest i Figur 1 visar att klient 1 och klient 2 har samma kapacitet både för uppladdning och nedladdning. Den övre representerar den stationära datorn (klient 1), den undre den bärbara datorn (klient 2). Därefter utfördes ett prestandatest på lagringsutrymmet.



Figur 2: Resultat av test mot lokal lagringmedia.

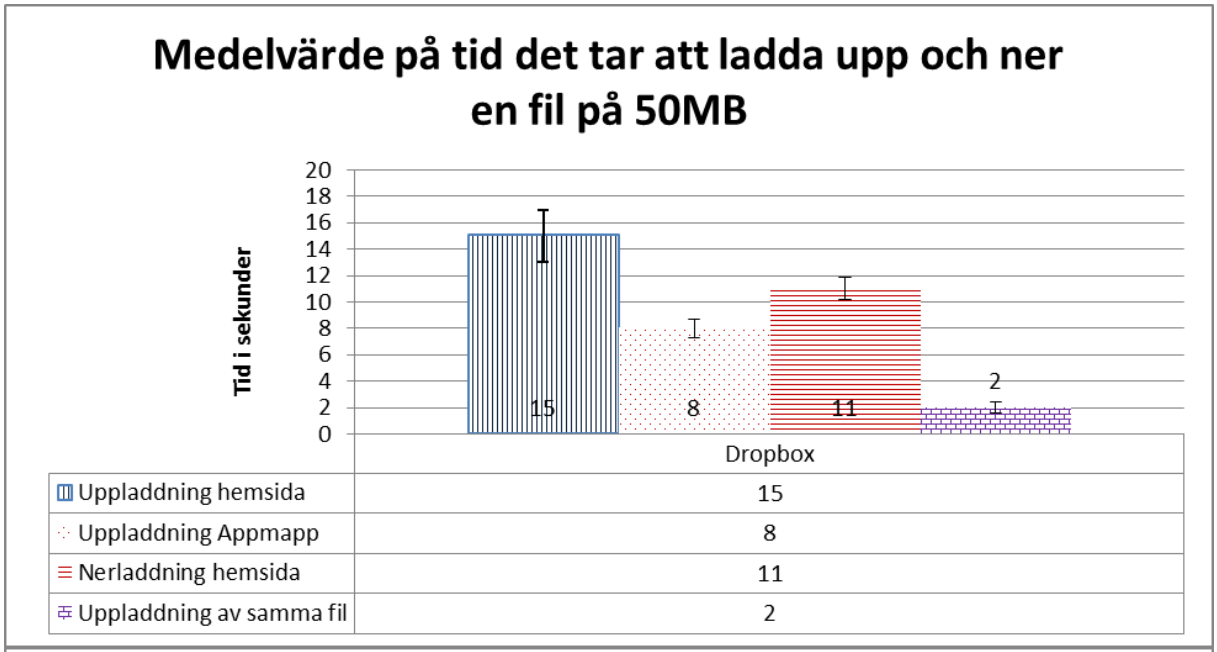
Vid test användes sen sekventiell skanningsmetod 5gånger med en filstorlek på 1000MB. Det övre mätvärdet i Figur 2 representerar hastigheten hos den virtuella disken, den mittersta SSD disken hos klient 1 och den längst ner laptop HDD hos klient 2. Resultaten skiljer sig med marginal, detta då hårddisktyperna skiljer sig i RPM samt uppsättning då laptop HDDs presterar sämre än stationära med samma RPM (eHow, 2014).

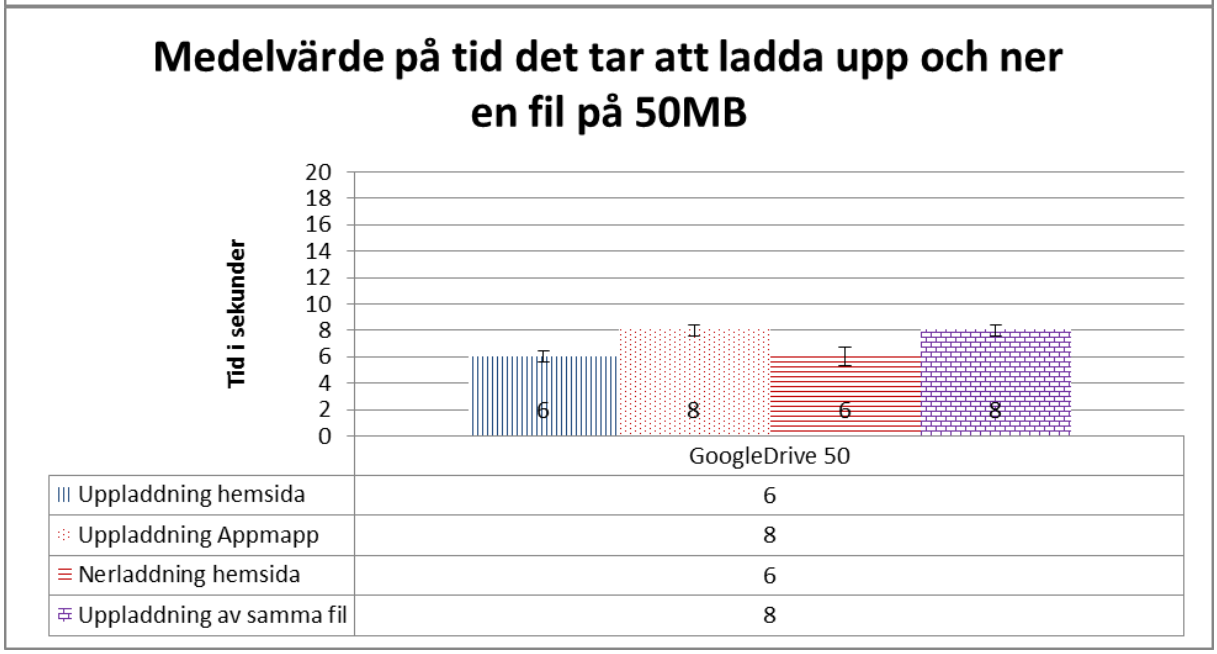
6.2 Uppladdning/Nedladdningstest i lokal miljö

Detta test kommer att besvara delmål 1, vilken molntjänst presterar bäst med tanke på uppladdning eller nedladdning av filer.

6.2.1 Uppladdning och Nedladdning

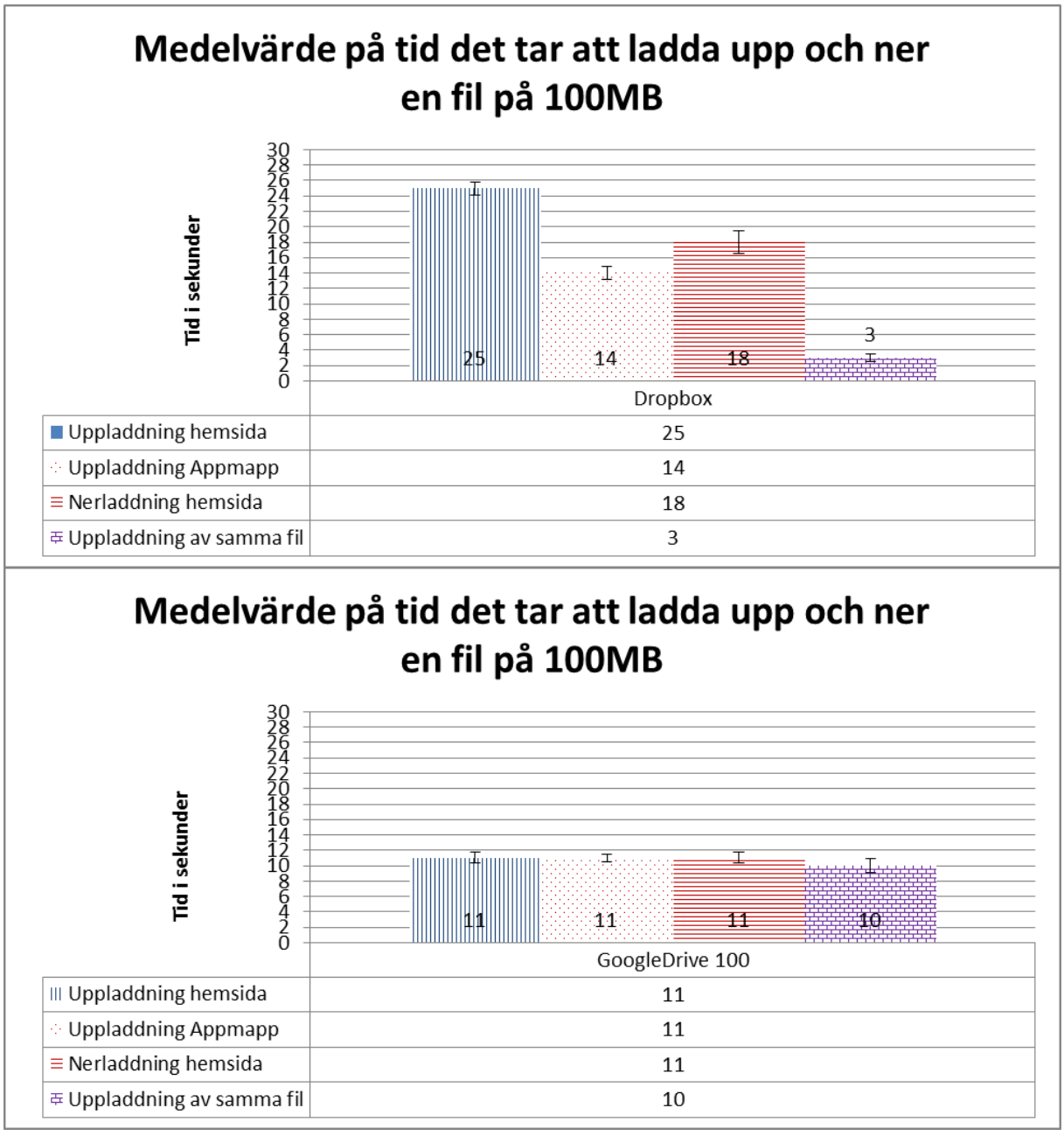
Nedanstående grafer visar prestandaskillnaderna mellan de olika testerna vid uppladdning och nedladdning av filer. Tester har som tidigare nämnts utförts med filstorlekarna: 50, 100, 250, 500, 1000 och 2000MB. Därefter har testerna körts fem gånger för att få fram ett medelvärde. Medelvärdet räknas ut enligt formeln i föregående kapitel. För att få variationen har tester utförts vid olika tider. I tillägg visas även standardavvikelser (spridning) av resultaten i form av en linje i varje stapel. Extern validitet av experimentet beskrivs i sektion 4.3.3.





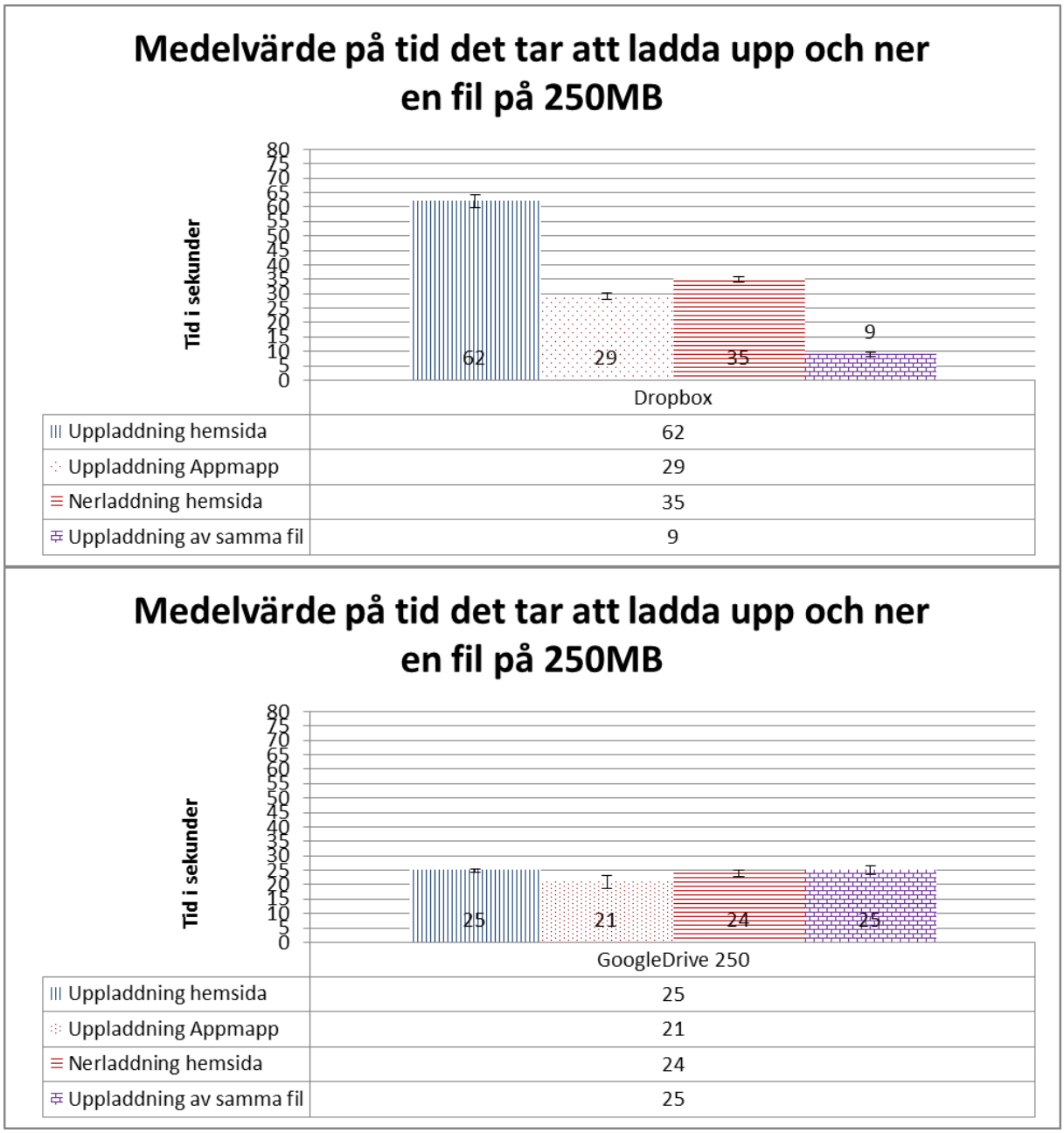
Figur 3: Visar uppladdning och nedladdningstid i sekunder vid en filöverföring på 50MB.

Redan vid en filstorlek på 50MB kan en prestandaskillnad märkas mellan de båda molntjänsterna. Dropbox presterar sämre vid uppladdning direkt till hemsida, däremot håller den en likadan hastighet vid uppladdning till applikationsmapp som GoogleDrive. Vid nedladdning presterar GoogleDrive bättre än Dropbox. Vid uppladdning av samma fil flera gånger är Dropbox märkbart snabbare än GoogleDrive.



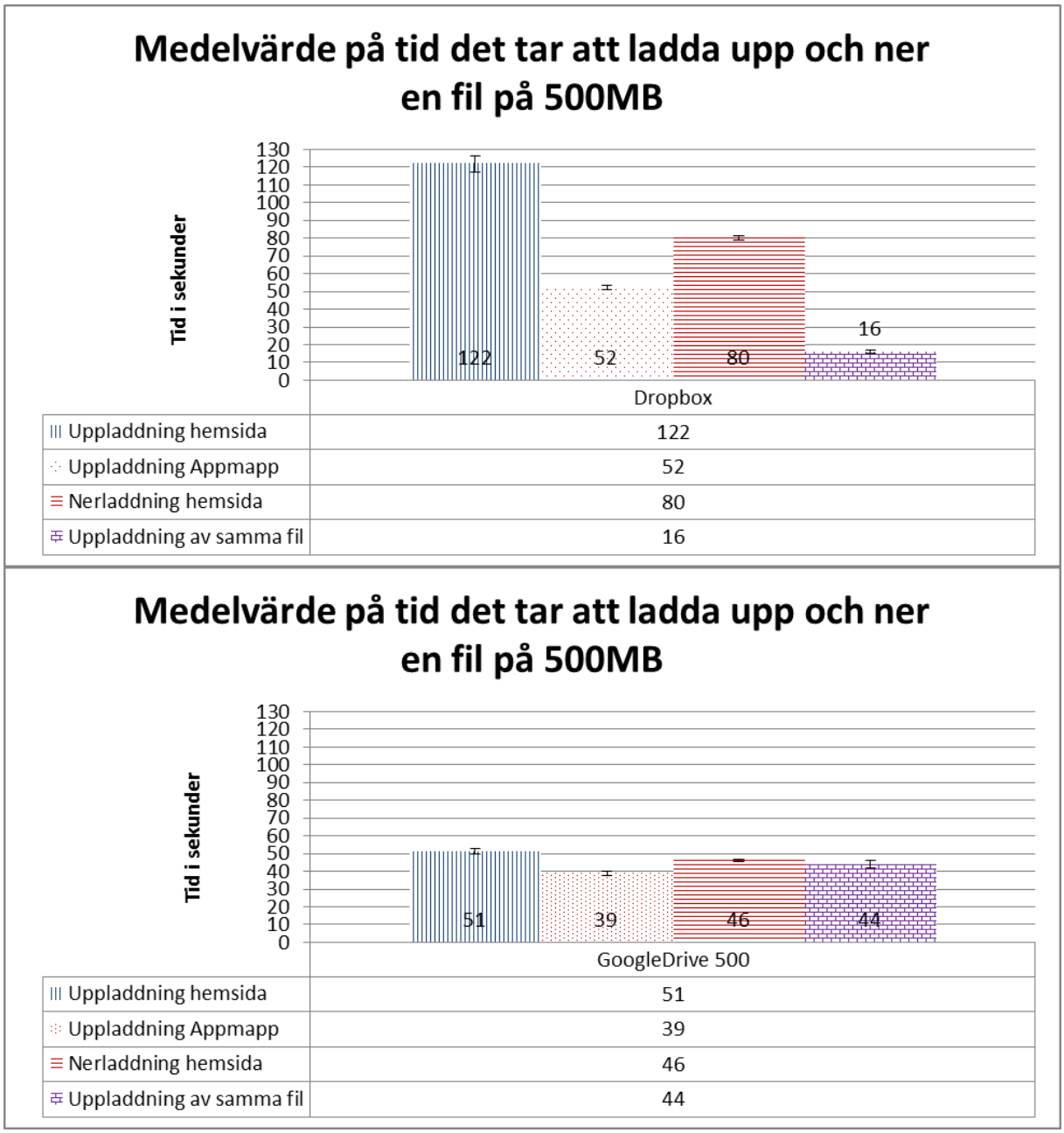
Figur 4: Visar uppladdning och nedladdningstid i sekunder vid en filöverföring 100MB.

Vidare ökning av filstorlek visar en varierande hastighet över samtliga uppladdningsmetoder för Dropbox. GoogleDrive håller en jämn uppladdningshastighet oavsett metod. Nedladdningshastigheten är vid denna filstorlek högre hos GoogleDrive.



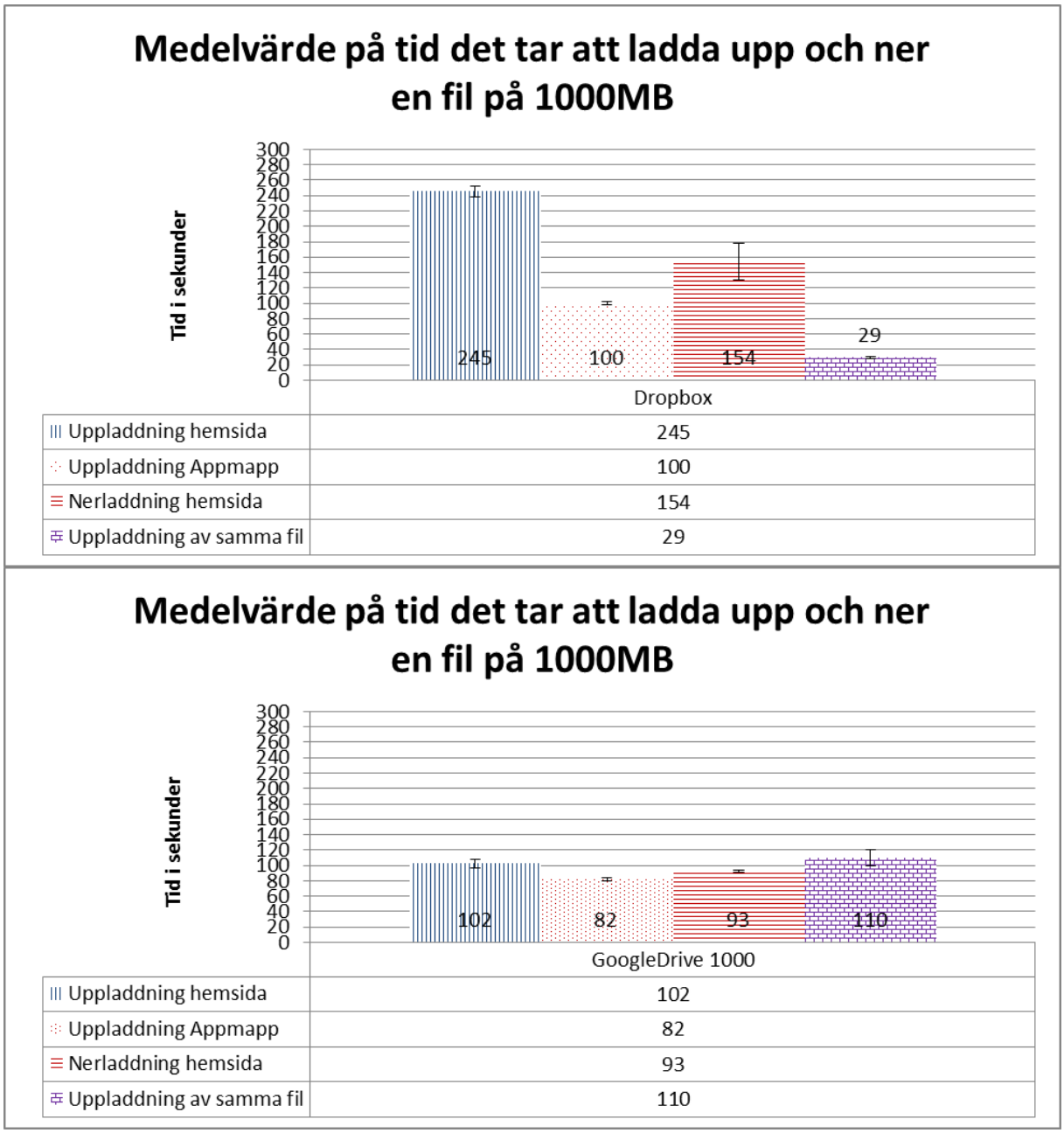
Figur 5: Visar uppladdning och nedladdningstid i sekunder vid en filöverföring på 250MB.

Vid filstorleken 250MB har skillnaderna mellan uppladdning till hemsida ökat ytterligare. Det tar mer än dubbelt så lång tid att ladda upp en fil via webbgränssnittet för Dropbox än för GoogleDrive. GoogleDrive presterar bättre vid uppladdning via appmapp men med låg marginal. Nedladdningshastigheten är fortfarande snabbast hos GoogleDrive.



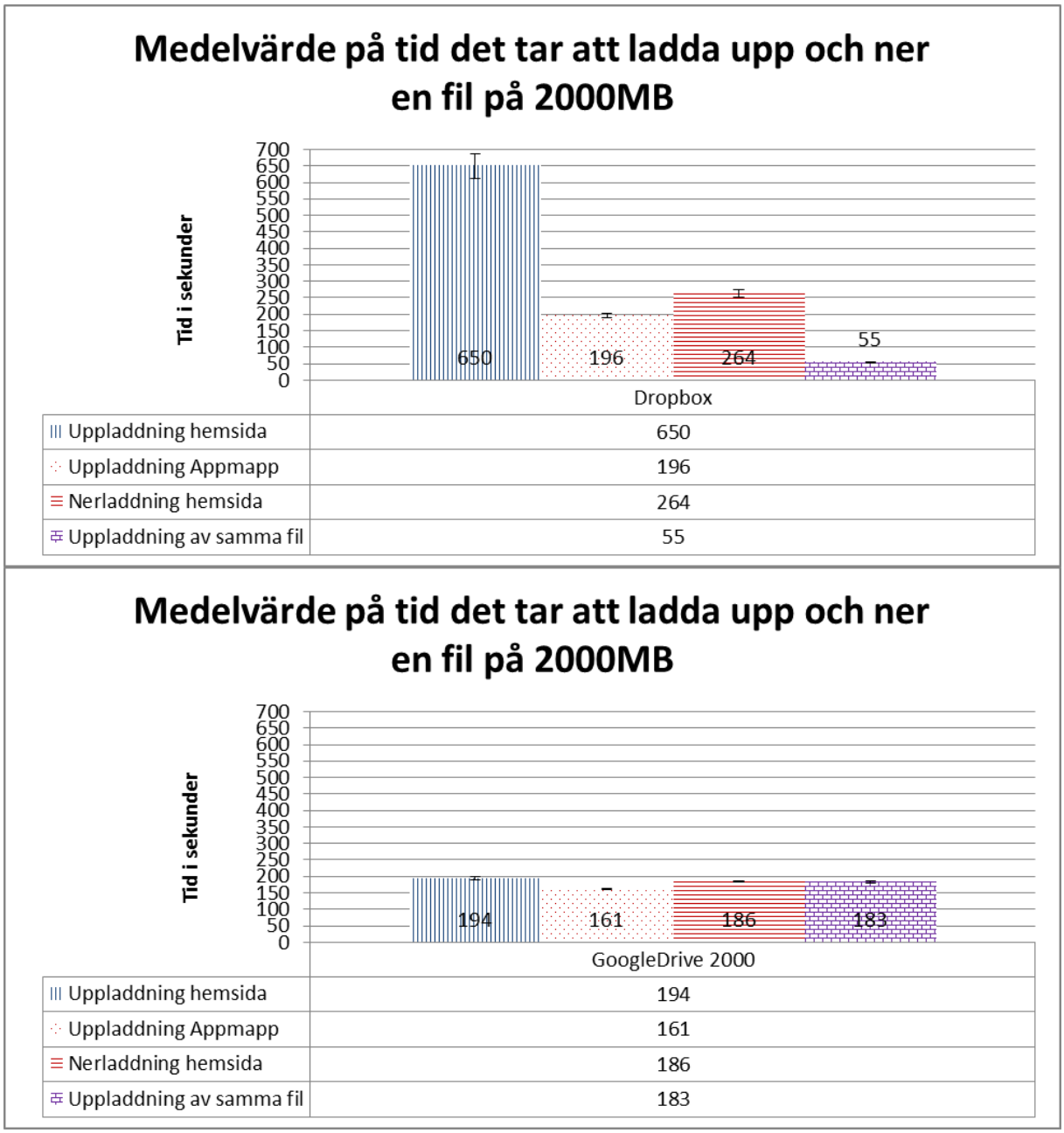
Figur 6: Visar uppladdning och nedladdningstid i sekunder vid en filöverföring på 500MB.

Vid 500MB filstorlek kvarstår föregående påståenden att Dropbox presterar sämre vid första uppladdningen av fil för att vid repeterad uppladdning av samma fil vara bäst. GoogleDrive's resultat håller en jämn nivå där uppladdning till appmapp går lite snabbare än övriga metoder.



Figur 7: Visar uppladdning och nedladdningstid i sekunder vid en filöverföring på 1GB.

Den näst sista filstorleken ger inga nya upptäckter utan är lik föregående bild.

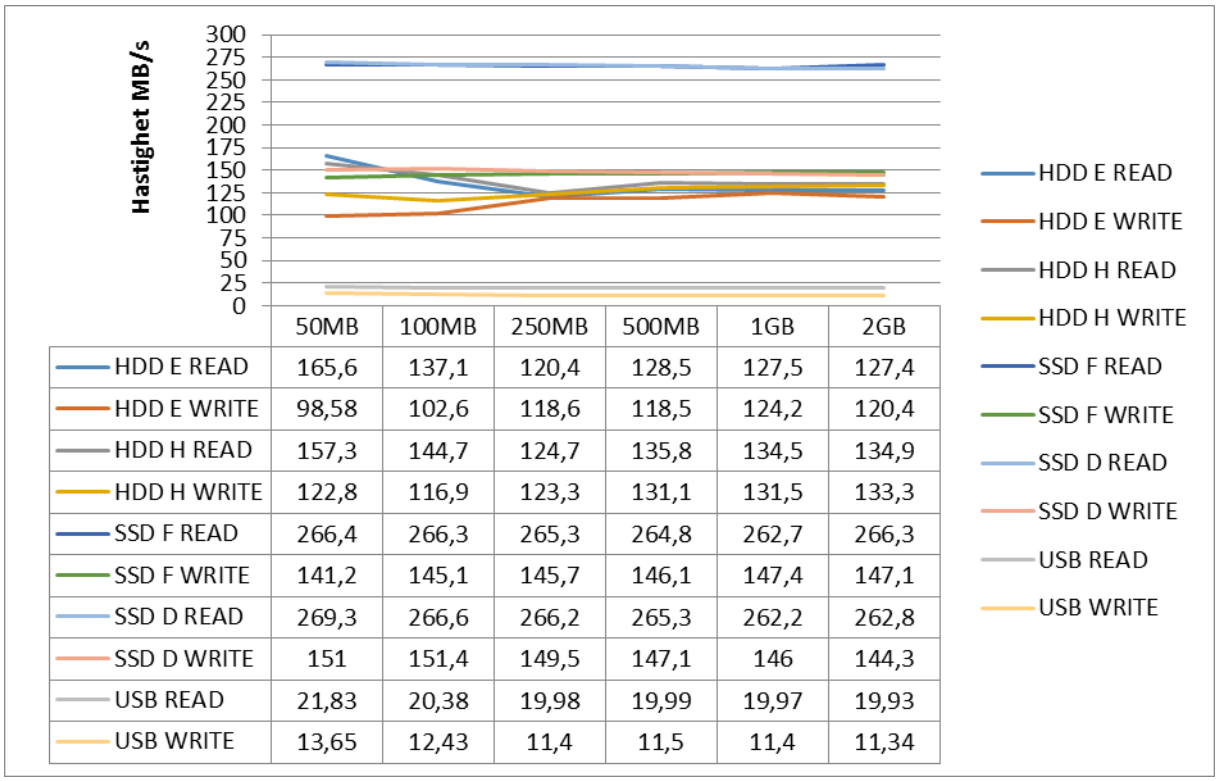


Figur 8: Visar uppladdning och nedladdningstid i sekunder vid en filöverföring på 2GB.

Vid en filstorlek på 2GB kvarstår relationen mellan de olika värdena. Uppladdning till hemsida är den största skillnaden mellan bägge tjänsterna. En uppladdning på 2GB tar 3gånger så lång tid på Dropbox gentemot GoogleDrive.

6.3 Lokal lagring

Denna del visar resultaten av test mot lokal media med verktyget CrystalDiskMark. Resultat som erfås är läs och skrivhastighet. Resultaten av dessa test ger en insikt av prestandaskillnader mellan överföring på lokal lagring gentemot uppladdning/nedladdning mot molntjänst.



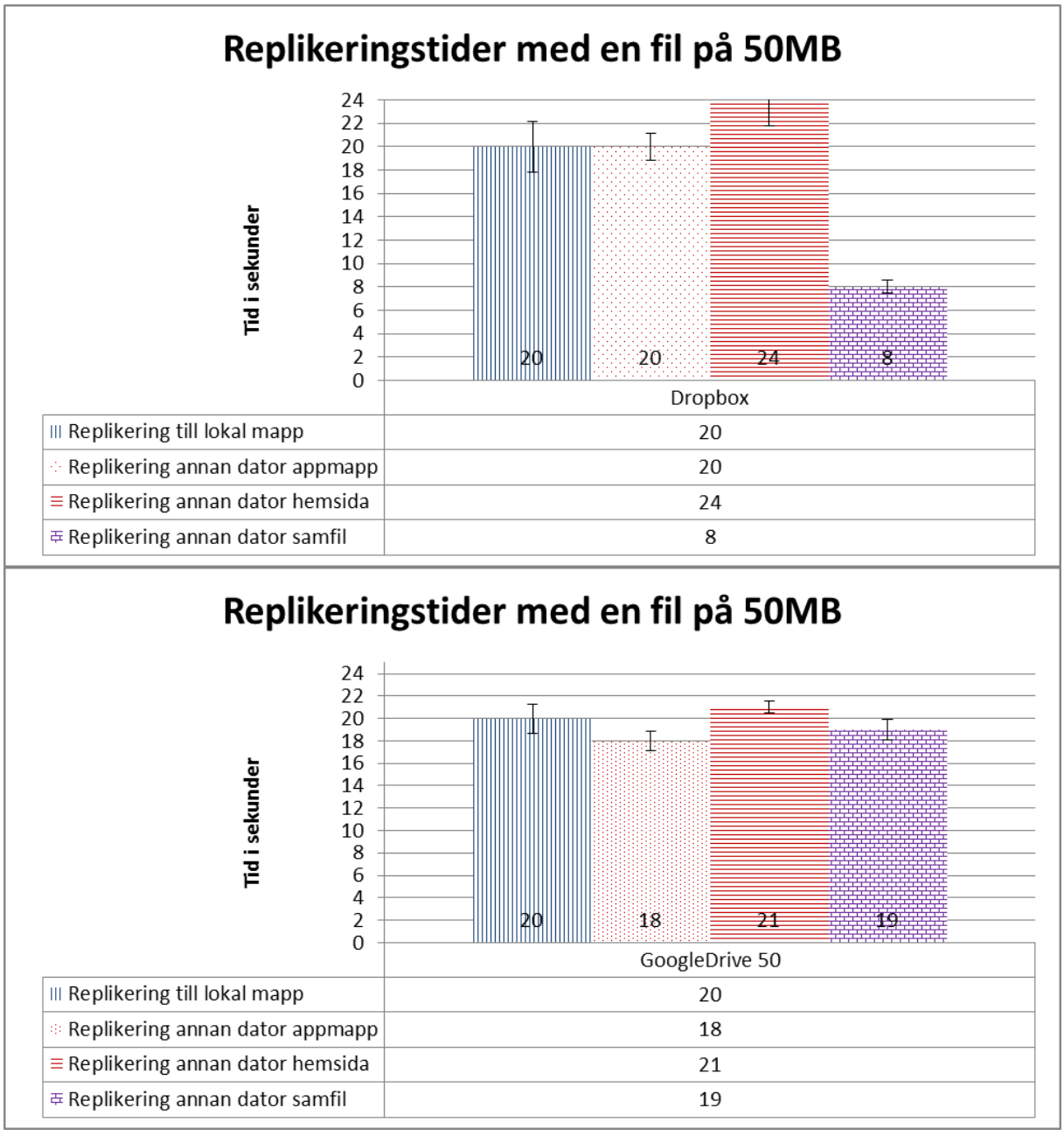
	50MB	100MB	250MB	500MB	1GB	2GB
HDD E READ	165,6	137,1	120,4	128,5	127,5	127,4
HDD E WRITE	98,58	102,6	118,6	118,5	124,2	120,4
HDD H READ	157,3	144,7	124,7	135,8	134,5	134,9
HDD H WRITE	122,8	116,9	123,3	131,1	131,5	133,3
SSD F READ	266,4	266,3	265,3	264,8	262,7	266,3
SSD F WRITE	141,2	145,1	145,7	146,1	147,4	147,1
SSD D READ	269,3	266,6	266,2	265,3	262,2	262,8
SSD D WRITE	151	151,4	149,5	147,1	146	144,3
USB READ	21,83	20,38	19,98	19,99	19,97	19,93
USB WRITE	13,65	12,43	11,4	11,5	11,4	11,34

Figur 9: Visar läs och skrivhastigheter samt skalbarhet för läs och skrivhastigheter på lokal lagringsmedia

Grafen ovan ger en inblick i vad för sorts läs och skrivhastigheter som existerar i olika lagringsmedium. Av grafen kan det utläsas att SSD diskar har en jämn läs och skrivhastighet oavsett de filstorlekar som testades. Läshastigheten för SSD är den högst rankade och ligger på ett medelvärde av 260MB/s medan skrivhastigheten befinner sig på ett medelvärde av 150MB/s. Läs och skrivhastigheterna på en HDD varierar beroende på filstorlek. Vid låg filstorlek är läshastigheten högre än vid större filer, samtidigt som skrivhastigheten är lägre vid låg filstorlek och högre vid större storlekar. Vidare visar grafen även att hastigheten vid USB-lagring är oavsett filstorlek jämn och väldigt låg. Läshastigheten för USB har ett medelvärde av 25, skrivhastigheten har medelvärdet 19.

6.4 Replikeringstid

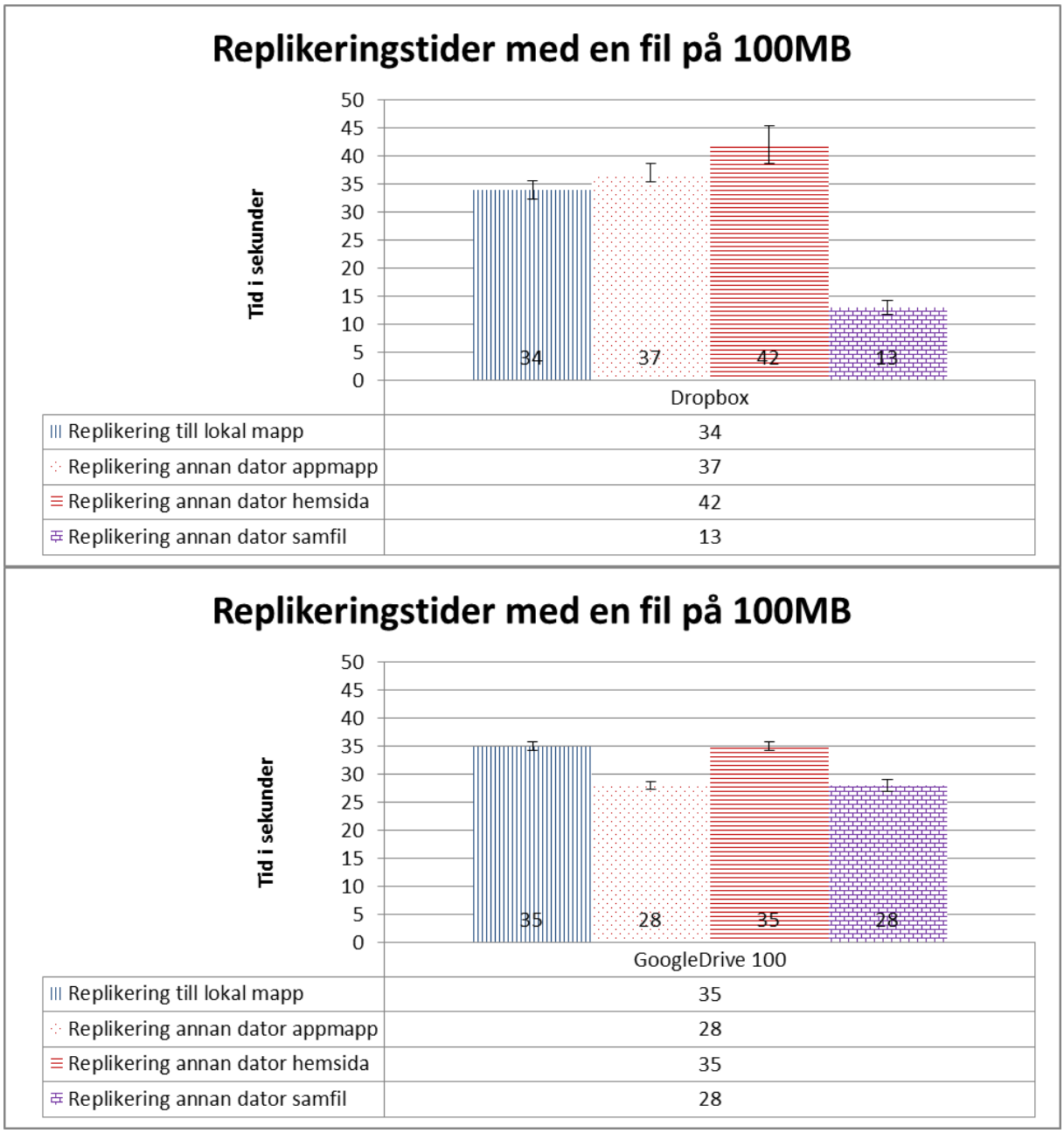
Efter att uppladdning och neladdningstester har körts har även replikationsmätningar utförts mellan båda tjänsterna. Replikation i detta sammanhang menas den tid i sekunder det tar för en fil som laddas upp, till webb eller applikationsgränssnitt, att kopieras eller replikeras till motsvarande gränssnitt och till den andra klientens applikationsgränssnitt.



Figur 10: Replikeringstider vid filstorlek 50MB.

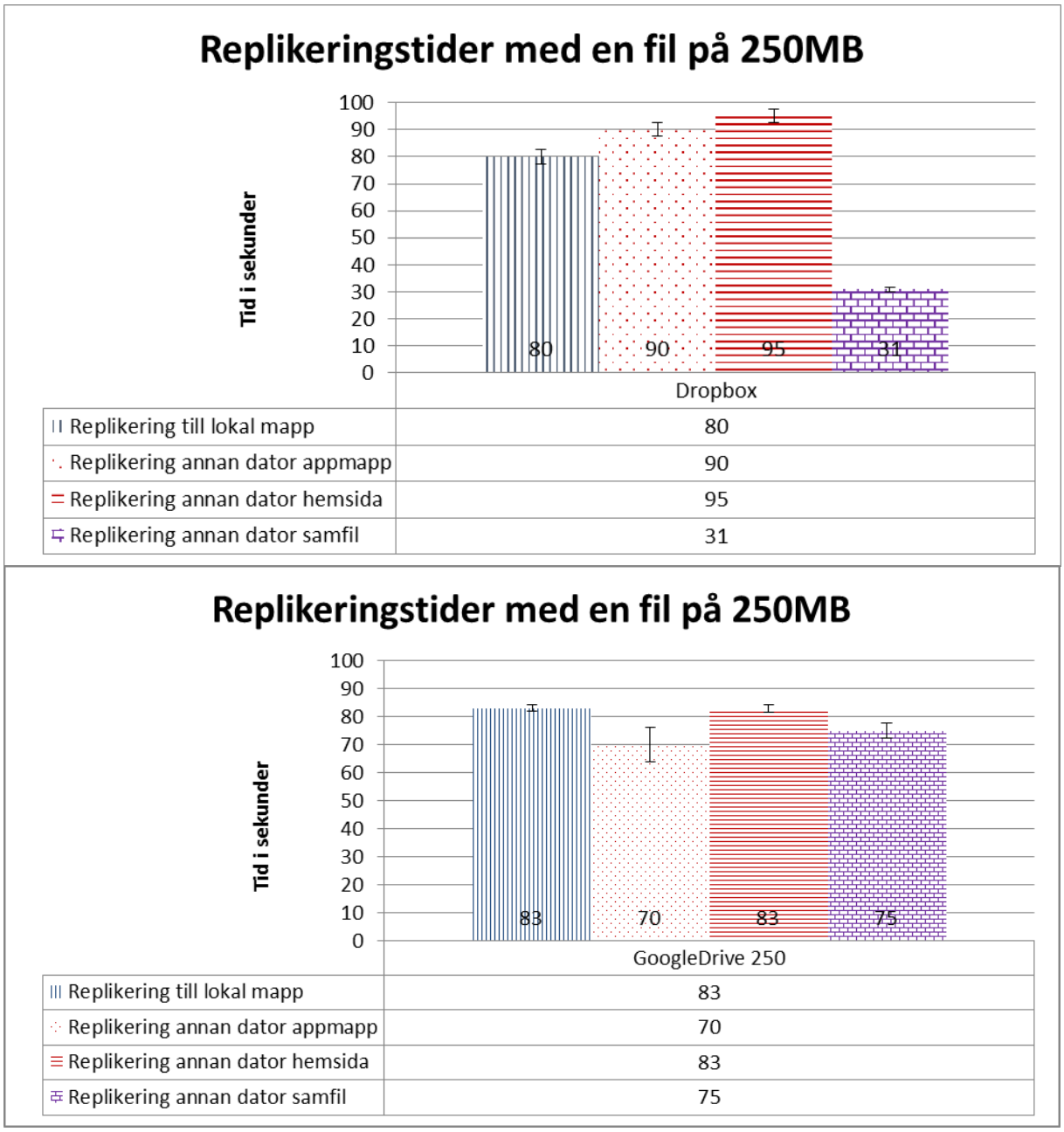
Vid filstorleken 50MB är replikationshastigheten för Dropbox från hemsida till lokal mapp, det vill säga den dator som laddade upp filen till webbgränssnittet, jämlikt med hastigheten för replikering till andra datorer vid lagring direkt i applikationsmappen. Replikering för samma fil som uppladdas flera gånger är låg vilket direkt relaterar till uppladdningsresultatet

i föregående del. Hastigheterna och tiderna för GoogleDrive är jämlika oavsett replikeringsmetod.



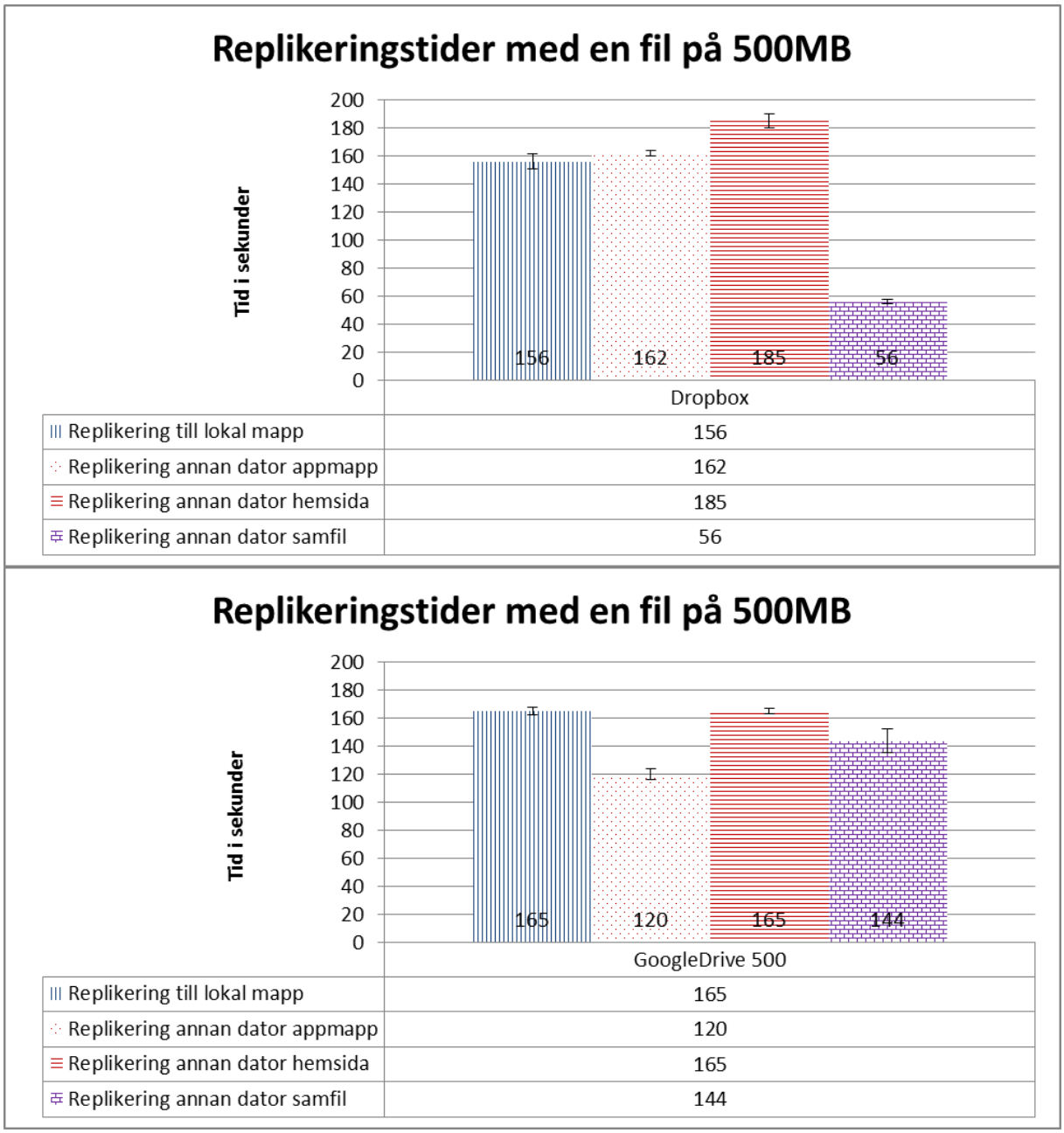
Figur 11: Replikeringstider vid filstorlek 100MB.

Vid filstorleken 100MB har samtliga värden ökats med en faktor av ~1,5x de från föregående test. Förhållanden mellan värdena är likt Figur 10.



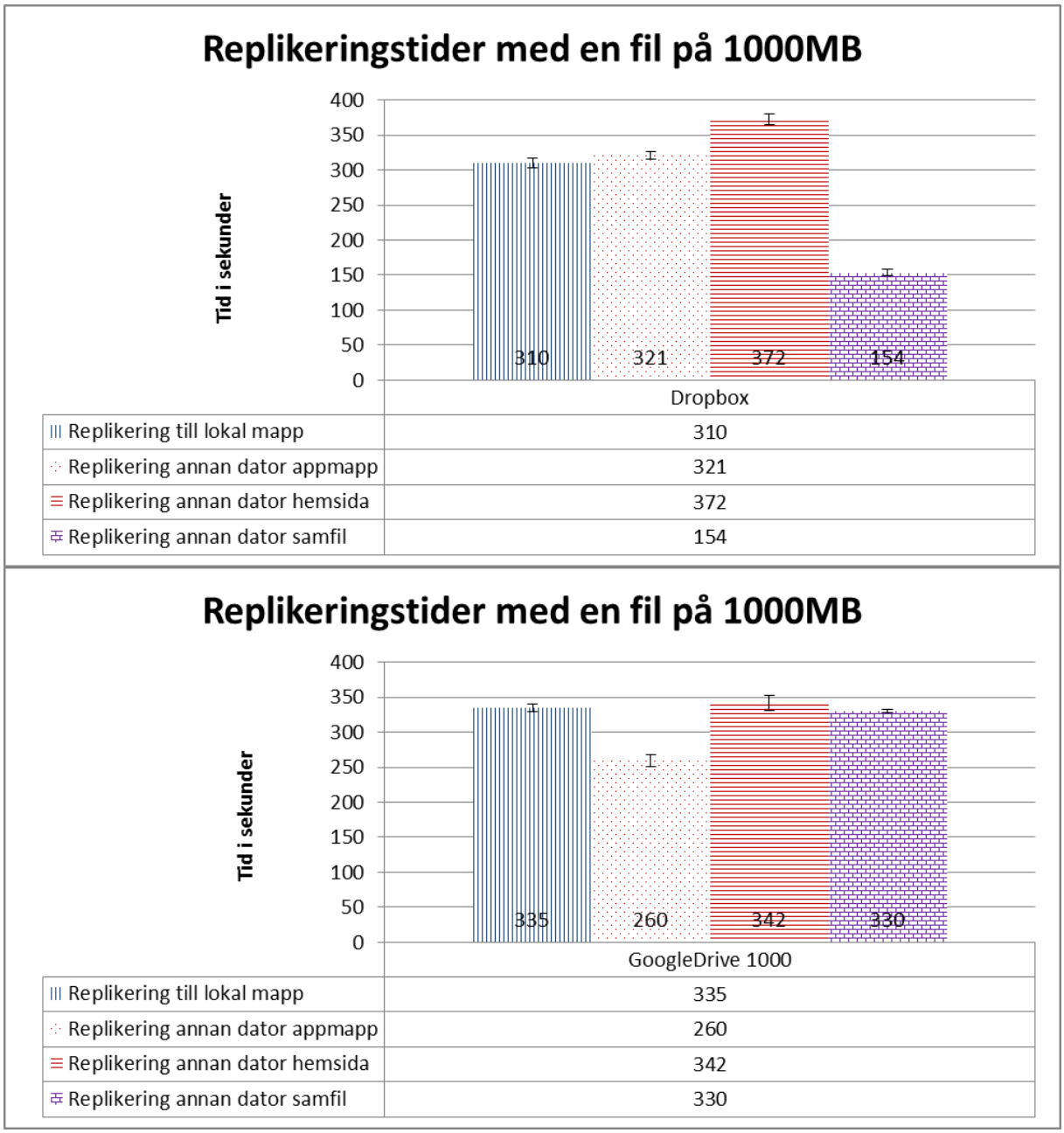
Figur 12: Replikeringstider vid filstorlek 250MB.

Nästa filstorlek visar en ökning på samtliga värden med en faktor av ~2x från resultat i Figur 11. Förhållanden mellan värdena kvarstår.



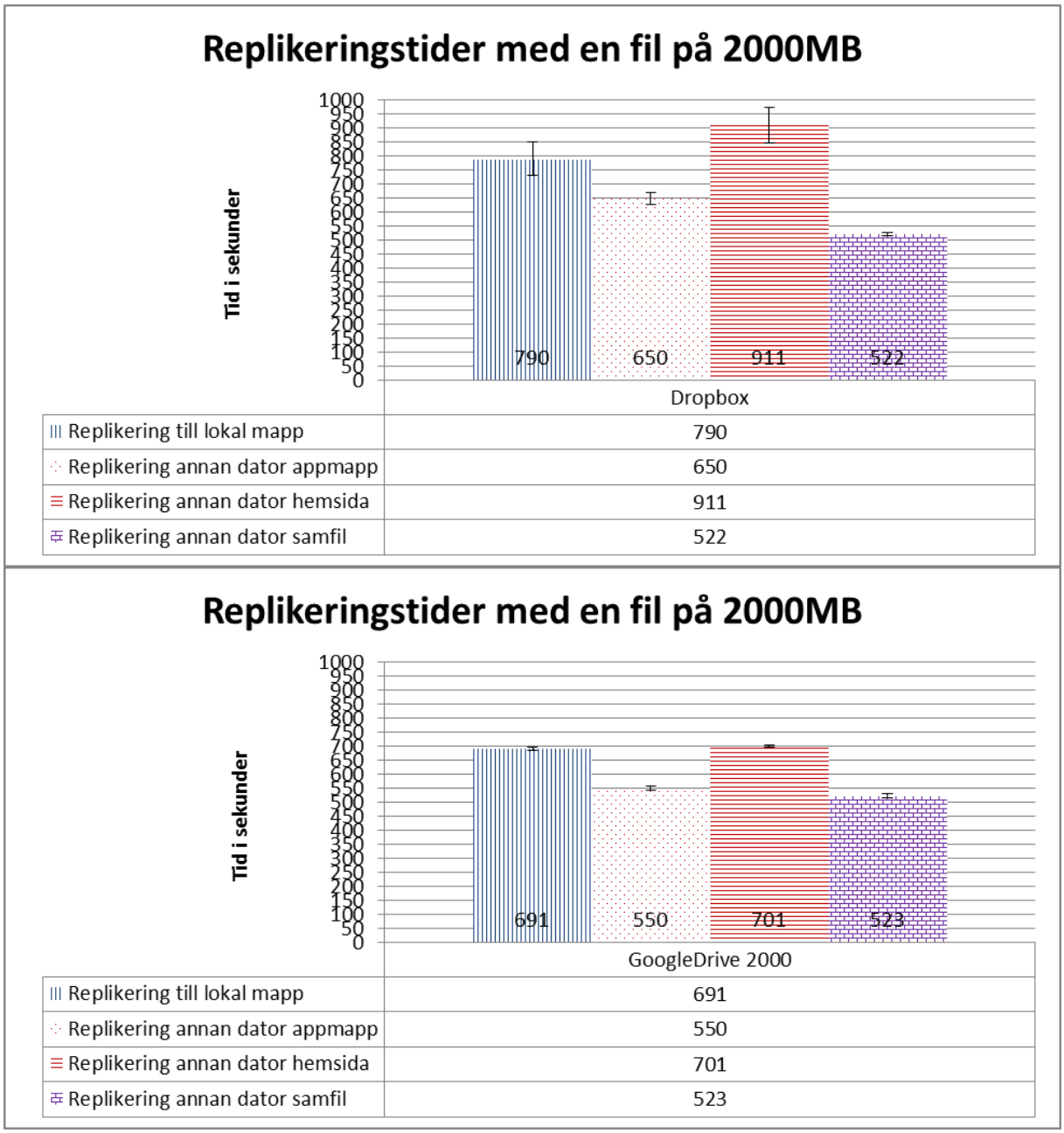
Figur 13: Replikeringstider vid filstorlek 500MB.

Vid filstorleken 500MB har de uppmätta värdena fortsatt öka med faktorn~2x jämfört med resultat från Figur 12. Förhållanden mellan värdena kvarstår.



Figur 14: Replikeringstider vid filstorlek 1000MB.

Likt föregående filstorlek har de uppmätta värdena fortsatt öka med faktorn~2x jämfört med resultat från Figur 13. Förhållanden mellan värdena kvarstår.

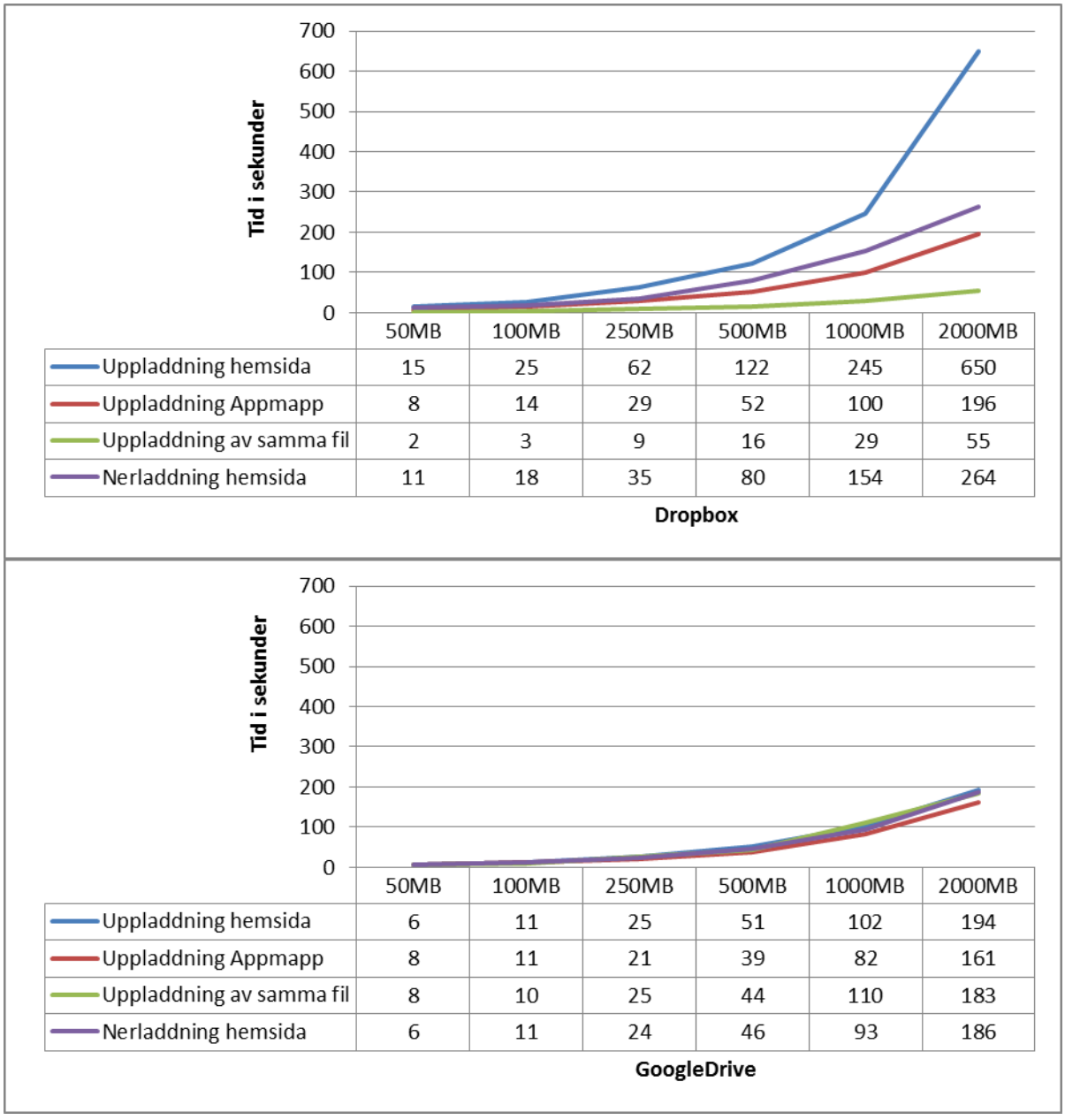


Figur 15: Replikeringstider vid filstorlek 2000MB.

Vid den sista filstorleken på 2000MB har de uppmätta värdena ökat med en faktor av~2x-2,5x jämfört med resultat från Figur 14. Igenom samtliga test har förhållanden mellan de 4olika teknikerna varit densamma.

6.5 Skalbarhet

Efter att ha kört dessa tester med olika tekniker och olika filstorlekar kan vissa mönster märkas. Dessa grafer ämnar beskriva hur responstiden påverkas av filstorlek.



Dropbox	50MB	100MB	250MB	500MB	1000MB	2000MB
Uppladdning hemsida	15	25	62	122	245	650
Uppladdning Appmapp	8	14	29	52	100	196
Uppladdning av samma fil	2	3	9	16	29	55
Nerladdning hemsida	11	18	35	80	154	264

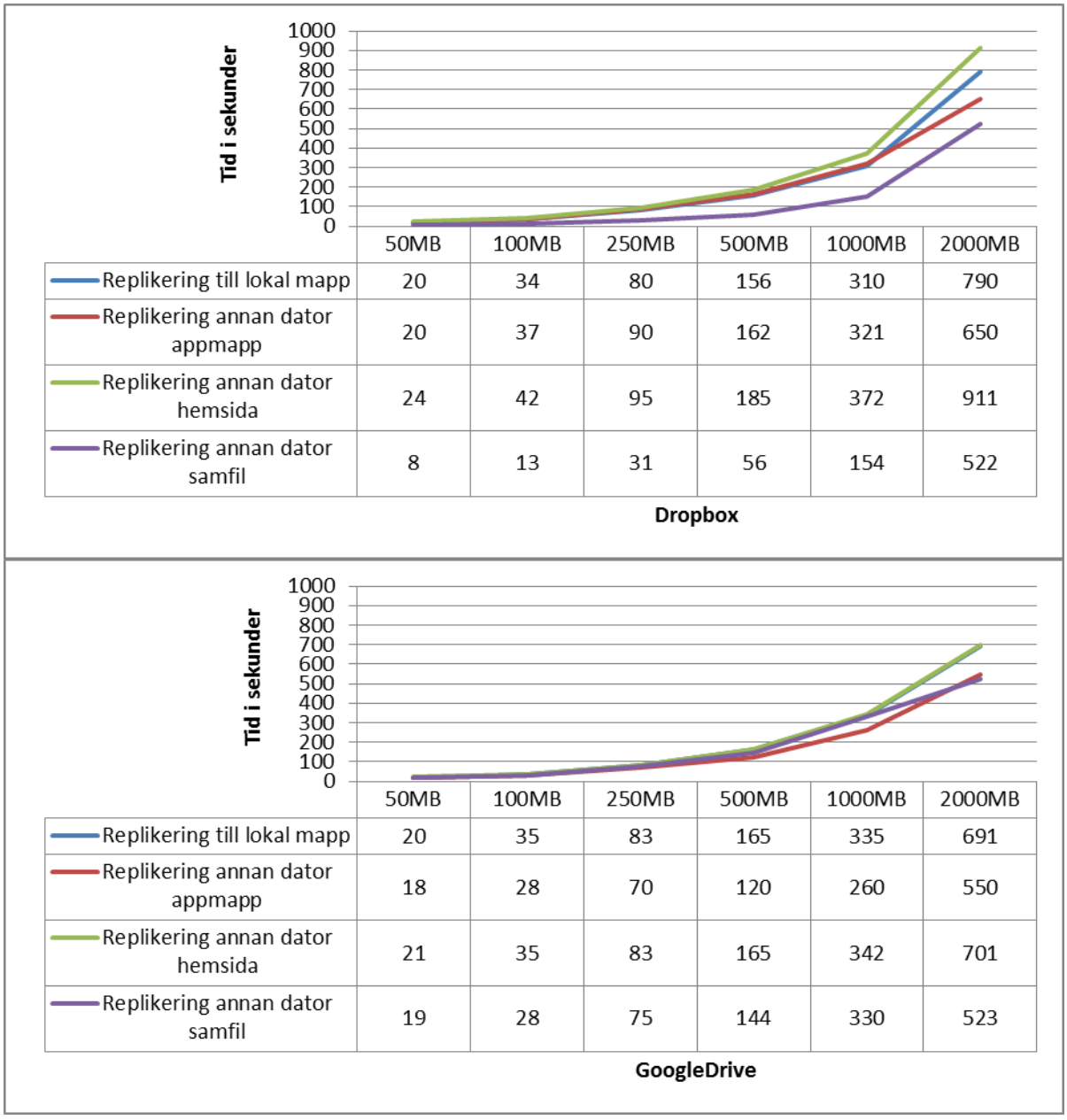
GoogleDrive	50MB	100MB	250MB	500MB	1000MB	2000MB
Uppladdning hemsida	6	11	25	51	102	194
Uppladdning Appmapp	8	11	21	39	82	161
Uppladdning av samma fil	8	10	25	44	110	183
Nerladdning hemsida	6	11	24	46	93	186

Figur 16: Visar förändringen i responstid vid ökad filstorlek för de olika uppladdningarna och nedladdningarna. Dropbox ovan, GoogleDrive under.

Dropbox har en högre responstid vid låga hastigheter i jämförelse med GoogleDrive förutom i metoden ”uppladdning av samma fil. Responstiden förändras med en faktor på ~2 vid hastigheter upp till 1000MB. Vid 1000MB kan en brytpunkt ses i Dropbox grafen på metoden ”uppladdning hemsida” då responstiden ökar med en faktor av ~3. För metoden ”uppladdning appmapp” så ökar responstiden oavsett filstorlek med en faktor av ~2. Responstiden för ”uppladdning av samma fil” är låg vid små filstorlekar (50 och 100MB) och påverkas nästan inte alls av filstorlek. Vid 250MB och uppåt ökar responstiden enligt

föregående metoder med en faktor av ~2. Även responstiden för nerladdning ökar likt föregående med en faktor av ~2 oavsett filstorlek.

GoogleDrive har en lägre responstid än Dropbox för samtliga uppladdningar förutom vid metoden ”uppladdning av samma fil”. Samtliga uppladdningstekniker och filers responstid ökar med en faktor av ~2. Ingen brytpunkt märks vid de filstorlekar som användes i experimentet. Nedladdningshastighetens responstid är lägre för GoogleDrive än för Dropbox. Skillnaden mellan GoogleDrive och Dropbox är nästan 100% det vill säga responstiden är dubbelt så lång för Dropbox oavsett filstorlek. Responstiden över filstorlekar ökas med en faktor av ~2.



	50MB	100MB	250MB	500MB	1000MB	2000MB
Replikering till lokal mapp	20	34	80	156	310	790
Replikering annan dator appmapp	20	37	90	162	321	650
Replikering annan dator hemsida	24	42	95	185	372	911
Replikering annan dator samfil	8	13	31	56	154	522

Dropbox

	50MB	100MB	250MB	500MB	1000MB	2000MB
Replikering till lokal mapp	20	35	83	165	335	691
Replikering annan dator appmapp	18	28	70	120	260	550
Replikering annan dator hemsida	21	35	83	165	342	701
Replikering annan dator samfil	19	28	75	144	330	523

GoogleDrive

Figur 17: Visar förändringen i responstid vid ökad filstorlek för replikering. Dropbox ovan, GoogleDrive under.

Dropbox har en högre responstid vid större filstorlekar än GoogleDrive. Vid låg filstorlek är likheterna mellan de både tjänsterna större då responstiden ökar med en faktor av ~2 oavsett replikeringsmetod. En brytpunk i diagrammet märks vid filstorleken 1000 till 2000MB då responstiden ökar från faktorn ~2 till ~2.5, 3 och 3,5x hastigheten vid tidigare filstorlekar. Metoden ”replikering annan dator appmapp” är den enda som behåller en jämn ökning i responstid. Metoderna ”replikering till lokal mapp” och ”replikering annan dator hemsida” ökar med faktorn ~2.5. Metoden ”replikering annan dator samfil” ökar med en faktor av 3,5 vilket gör den till den replikeringsmetod som har högst responstid och störst prestandaförändring över samtliga metoder och molntjänster.

GoogleDrive har vid låga filstorlekar en replikeringstid som ökar med en faktor av ~1,5 - ~2 över samtliga metoder. Vid större filstorlekar ökar responstidökningen från tidigare faktor till ~2 - ~2.5. Ingen specifik brytpunkt märks då den faktoriska ökningen följer ett jämnt mönster allteftersom filstorleken ökar.

7 Analys

I detta kapitel analyseras resultaten ifrån prestandatest och litteraturanalys.

7.1 Prestandatest

Denna sektion presenterar de analyser som utfåtts ifrån de olika prestandatesterna.

7.1.1 Uppladdningsanalys

Denna del behandlar delmål 1 ”Vilken molntjänst presterar bäst vid uppladdning av filer?”. Vid uppladdning av en enstaka fil till webbgränssnittet syns det i Figur 3-Figur 8 att oavsett filstorlek så presterar GoogleDrive bäst. Förhållandet mellan tidsåtgången mellan Dropbox och GoogleDrive vid denna uppladdningsmetod varierar men är störst vid en filstorlek på 2000MB då skillnaden är ~3 gånger stor. Anledningen till detta antas vara att Dropbox krypterar filer vid uppladdning till skillnad från GoogleDrive som inte gör detta.

Vid uppladdning direkt till molntjänsternas applikation är resultaten mer jämna än mot hemsidan. Vid låg filstorlek som kan ses i Figur 3 är det ingen skillnad i uppladdningstid. Skillnaden mellan dessa ökar däremot kontinuerligt ju större filstorleken är. I Figur 8 är skillnaden som störst med en skillnad på 1.25. Detta resultat är likt det i föregående test. Anledningen till att de skiljer sig kan vara att skrivhastigheten till applikationsmappen innebär mindre uppladdningstid för användaren och mer hos molnleverantören.

Vid uppladdning av samma fil flera gånger märks det en klar skillnad mellan de bägge molntjänsterna. Efter den första uppladdningen av en fil på Dropbox applikationen minskar filöverföringstiden markant gentemot sin motståndare. Figur 8 visar detta tydligast då den första uppladdningen tar 196sekunder medan kommande uppladdning av samma fil enbart tar 55sekunder. Detta beror på att Dropbox använder en ”hash” teknik (Dropbox, 2014b). När en fil laddas upp till Dropbox via applikationsmapp bryts den ner i bitar. Informationen i dessa bitar sparas sedan på Dropbox. När samma fil läggs till igen känner den igen dessa bitar och ”fyller igen” de bitar som redan är indexerade hos Dropbox servrarna.

7.1.2 Nedladdningsanalys

Denna del behandlar delmål 1 ”Vilken molntjänst presterar bäst vid nedladdning av filer?”. Vid nedladdning av filer ifrån molntjänstens webbgränssnitt presterar GoogleDrive bättre än Dropbox över samtliga filstorlekar. Nedladdningshastigheten för filer hämtade från Dropbox håller en jämn hastighet runt 6.5MB/s medan GoogleDrive ligger på en jämn hastighet runt 10MB/s. Detta innebär att responstiden vid nedladdningar är jämn, ökar med en konstant faktor av ~2, i de tester som har körts. GoogleDrive har i sina test maximerad bandbreddskapacitet hos testdatorn. Därefter är det möjligt att hastigheten är högre vid tillgång till Gigabit Ethernet tillgång. Anledningen till att GoogleDrive presterar bättre är för att ingen skanning av filer sker. Vid nedladdning av filer varnar webbgränssnittet att filstorleken är för stor för att kunna verifieras. Detta gäller för samtliga filstorlekar. Detta innebär att det inte finns någon extra overhead utan nedladdningen kan använda full bandbreddskapacitet.

7.1.3 Lokal lagring analys

Denna del behandlar delmål 3 ”Hur förhåller sig prestandan hos lokal lagring mot molntjänster?”.

Figur 9 visar på ett tydligt sätt att traditionella lagringstyper har en högre läs och skrivhastighet än vad Dropbox eller GoogleDrive kan uppnå i den labbmiljö som används. Ifall möjlighet till Gigabit Ethernet fanns tillgänglig hade detta kunnat testas ytterligare och möjligtvis gett ett mer uttömmande svar.

7.1.4 Replikeringsanalys

Denna sektion behandlar delmål 5 ”Vad finns det för skillnader vid replikering av filer mellan Dropbox och GoogleDrive?”. Vid replikering av filer mellan två olika system visar det sig i Figur 3-Figur 8 att GoogleDrive presterar bättre än Dropbox vid samtliga filstorlekar. Denna skillnad är vid låga filstorlekar låg med en skillnad på runt 0.5MB/s medan den i Figur 8 ligger skillnaden som störst på 1MB/s.

7.1.5 Skalbarhetsanalys

När prestandatester har genomförts kan skalbarheten för de olika metoderna analyseras. Vid uppladdning av filer med Dropbox är responstiden jämn vid låg filstorlek och ökar med en faktor av ~2, det vill säga responstiden dubbleras eller följer ökningen av filstorleken. Vid större filer märks det i Figur 16 att uppladdning vid hemsida skalar sämre än de andra uppladdningsmetoderna då responstiden över 1000MB visar att responstiden ökat med en faktor av ~3. En brytpunkt märks här då lutningen av linjen ökar till skillnad från tidigare filstorlekar. Bäst resultat för Dropbox och även över samtliga molntjänster testade är uppladdning av samma fil där responstiden vid små filer knappt påverkades av filstorleken. GoogleDrive har lägst generell responstid, det vill säga responstiden ökar proportionerligt över samtliga metoder och filstorlekar.

Vid nedladdning av filer är GoogleDrive bättre än Dropbox, detta oavsett filstorlek. Vid låg filstorlek är skillnaden 7sekunder och skillnaden ökar när filerna blir större. Vid max filstorlek (2000MB) är skillnaden som störst på 50s. Responstiden för bägge tjänster är jämlik, det vill säga för bägge tjänster relaterar responstiden med filstorleken (den ökar med en faktor av ~2).

Metoden för replikering är som bäst vid replikering av samma fil för Dropbox, detta för anledning tidigare nämnt i uppladdningsanalys. Den metod som har högst responstid är vid metoden ”replikering annan dator hemsida” då Dropbox har ren replikeringstid på 911sekunder. Resterande replikeringsmetoder befinner sig jämlikt sina motståndare oavsett filstorlek och responstiden förändras i samma utsträckning som motsvarande tjänst och filstorlek med en faktor av ~2.

7.2 Litteraturanalys

Denna sektion behandlar delmål två och sex (Utföra en undersökning av säkerhet och integritet baserat på en analys av en litteraturstudie & identifiera specifika säkerhetsrisker/svagheter hos molntjänsterna). Kapitlet är uppdelat i fyra delar. Dessa delar kommer hantera fyra olika steg vid uppladdning av en fil till molnet. Dessa steg är: registrering, transport, kryptering och delning. Dessa steg har valts för att kunna dela upp analysen i nyckelpunkter där säkerhet är viktig. Liknande tillvägagångssätt används även av Borgmann et al. (2012) i artikeln ”On the security of cloud storage services” (Borgmann et al, 2012). Inom varje kapitel listas möjliga svagheter eller attacker, därefter respektive molntjänsts skydd eller brist på skydd mot attack.

7.2.1 Registrering

Delsektionen registrering innefattar de säkerhetsbrister och skydd som berör de bägge molntjänsterna med tanke på inloggning och registrering hos en molnleverantör.

Tvåstegsverifiering

Detta för att skydda mot lösenordsstöld. En tvåstegsverifiering används som ett extra lösenord vid inloggning. Det finns olika varianter av tvåstegsverifiering, den mest vanliga metoden innebär att lösenord först skrivs in. Därefter skickas en kod via sms, telefonsamtal eller mobilapp till en mobiltelefon som är kopplat till kontot (Wikipedia, 2014b).

GoogleDrive = Finns möjligt som tilläggsval.

Dropbox = Finns möjligt som tilläggsval.

Time-based One-Time Password (TOTP)

TOTP är en påbyggnad av tvåstegsverifiering där en algoritm beräknar ett engångslösenord från en delad hemlig nyckel och aktuell tid (Wikipedia, 2014a). Är likt tvåstegsverifiering i den form att efter användaren skrivit in användarnamn och lösenord skickas användaren en TOTP som gäller under en viss tid. Om användaren inte loggar in och lösenordstiden passerar måste användaren logga in igen och få ett nytt TOTP.

GoogleDrive = Kräver installation av tillägsapplikation ”Google Authenticator”.

Dropbox = Finns möjligt som tilläggsval.

Email-registrering

Email-registrering innebär att när en användare skapar ett nytt konto och anger sina uppgifter skickas ett mail till den angivna mailadressen där mottagaren verifierar att registrering är giltig.

Skyddar mot hot: Incrimination attack, det vill säga skyddar att någon skapar ett konto åt en annan för att t.ex. ladda upp olagligt material på detta konto, vilket gör ägaren av mailadressen misstänkt för brott (Borgmann et al, 2012).

Dropbox = Använder INTE email-registreringsskydd, kollar inte om mailadressen finns

GoogleDrive = Använder INTE email-registreringsskydd, använder ”captcha” vid skapande av konto. Kollar inte om backup email-adress finns.

Lösenordspolicy

Med lösenordspolicy menas de krav eller regler för skapande av ett lösenord. Exempel på detta kan vara att ett lösenord måste innehålla speciella karaktärer eller vara ett visst antal tecken långt.

Skyddar mot hot som:
Brute force-attack, dvs. en angripare gissar sig till användarnamn och/eller lösenord genom att testa alla möjliga kombinationer genom massförfrågningar tills login har lyckats.
Dictionary attack, en mer avancerad brute-force attack. Istället för att testa alla möjliga kombinationer testas populära lösenord eller samtliga ord från en ordbok (Borgmann et al, 2012).

Dropbox

Kräver enbart att lösenord är sex tecken långt, inga speciella tecken krävs.
Tvingar ”captcha” login vid upprepade login-försök.

GoogleDrive
Kräver åtta tecken långt lösenord, en blandning av tecken behövs eller ett nio tecken långt lösenord med samma tecken.
Tvingar INTE ”captcha” login vid upprepade login-försök.

Återställningspolicy
En återställningspolicy kan användas av olika anledningar. Ett sätt detta kan ske i registreringsprocessen är om leverantören direkt skickar ut ett lösenord till användaren eller om återställningsfrågor som ”användares första bil” används.

Skyddar mot hot som:
Denial-of-Service = En DoS attack innebär att en användare inte kan använda en tjänst
Social engineering = Om en anfallare har tillgång till en användares privata information kan detta användas för att få åtkomst till kontot (TechNet, 2014).

Dropbox
Resetmail skickas till mailadress associerad med kontot.

GoogleDrive
Reset av lösenord sker antingen via länkad telefon, ett extra mailkonto eller till mobiltelefon.

7.2.2 Transport
Delsektionen transport innefattar säkerheten på kommunikationen mellan klient och mottagare.

SSL/TLS
SSL (Secure Sockets Layer) används för att kryptera anslutningen mellan dator och mottagare. Detta för att undvika avlyssning eller angripande av data som laddas upp eller ner från molntjänsten.

Skyddar mot hot som:
Phishing attack = En anfallare använder en hemsida som är lik måltjänsten i hopp om att få användaren att ange sina login-uppgifter (Computernetworkingnotes, 2014).
Eavesdropping = Om en anfallare avlyssnar kommunikation mellan molnleverantör och användare vid t.ex. login eller skapande av konto kan denne få tillgång till uppladdad information.
Proxy = Anfallare manipulerar meddelanden mellan bägge parter i hopp om att bedra/svindla bägge parter.

Dropbox
SSL/TLS mellan klient-applikation och server.
HTTPS mellan webbläsare och webbgränssnitt.

GoogleDrive
SSL/TLS mellan klient-applikation och server.
HTTPS mellan webbläsare och webbgränssnitt.

7.2.3 Kryptering

Delsektionen kryptering berör skydd ifrån undersökning eller inspektering av data från extern part utanför molnleverantören eller inom företaget som hanterar molntjänsten.

Nyckelhantering

Nyckelhantering kan antingen vara hos leverantören eller lokal hos användaren(client-side). Beroende på vart nyckeln finns kan olika säkerhetsbrister utnyttjas eller förhindras.

Skyddar mot hot som:

Compromised-key attack = En anfallare får tillgång till en nyckel, och kan därefter låsa upp krypterade filer eller begära ytterliggare nycklar som kan påverka andra kanaler (Technet, 2014).

Dropbox
Nyckeln lagras hos Dropbox, detta skyddar mot missbruk av nyckel från parter förutom ifrån Dropbox själv.

GoogleDrive
Inget nyckelubyte.

Kryptering av uppladdade filer

Kryptering av filer kan göras av leverantören eller hos användaren. Valet på vilken kryptering som används och på vilka ställen detta görs kan avgöra vilka säkerhetsrisker som kan avvärjas eller tillåtas.

Dropbox
Data krypteras med AES-256 med hjälp av deras krypteringsnyckel när data laddats upp.
Client-side kryptering stöds inte/måste utföras manuellt av användare.

GoogleDrive
Data krypteras INTE när filer är uppladdade på servern/ytterligare applikationer behöver installeras.
Client-side kryptering stöds inte/måste utföras manuellt av användare.

7.2.4 Delning

Delsektionen delning innebär att skydda dokument internt inom grupp eller övriga aktörer i molnet.

Fildelning

Det finns många olika sätt att dela filer, de som berör säkerhet är delning med subscribers och non-subscribers. Subscribers får tillgång till en fil via en administratör eller skapare av en fil eller mapp. En non-subscriber delas ofta filer via en URL eller webbadress. Viktigt för dessa två fildelningsmetoder är att bara de som har tillgång får tillgång.

Dropbox
Spårbar borttaggning och återskapning av filer
Enbart administratör kan radera filer
Subscribers listas i webbgränssnittet

Non-subscriber URL mappas till en publik mapp. Filnamn i denna mapp visas i URL men förutom detta sprids ingen information.

GoogleDrive
Borttagning och återskapning av filer lagras i en ”Trash” mapp, därefter tas de bort.
Administratör bestämmer på varje fil denna skapar vad som kan göras: edit, comment, view.
Subscribers listas i webbgränssnittet

Non-subscribers måste ha ett google konto.
Non-subscriber URL kan skapas av varje mapp eller fil. Filnamn visas inte i URL.
Enbart subscribers kan öppna URL (måste logga in på google konto)

8 Slutsats

Detta kapitel avrundar arbetet genom en sammanfattning av vad för frågeställning som användes och hur resultat eller vad svaret på denna frågeställning är. Vidare presenteras en diskussion där arbetets tas ur sitt sammanhang och diskuteras mer öppet. Slutligen hypotiseras det hur arbetet skulle kunna fortsättas i framtiden.

8.1 Sammanfattning

Det här arbetet har undersökt och analyserat prestanda, säkerhet och integritet hos molntjänsterna Dropbox och GoogleDrive. De experiment som användes testade tjänsternas: uppladdning, nedladdning och replikering. Vidare utfördes en analys av litteraturstudie med inriktning mot säkerhet och integritet. I tillägg genomfördes ett prestandatest på ett antal olika lagringsmedium.

För att besvara frågan ”Vilken av molntjänsterna Dropbox och GoogleDrive är bäst vid uppladdning och nedladdning av filer” utfördes experiment. Utfallet av experimentet påvisade att vid uppladdning av 1 fil till webbgränssnittet så presterar GoogleDrive bäst med varierande resultat beroende på filstorlek. Vid den största filstorleken 2000MB tog det 194sekunder(10MB/s) att ladda upp en fil i jämförelse med Dropbox 650sekunder(3MB/s). Anledningen till denna stora skillnad nämndes i analysen då Dropbox krypterar filer vid uppladdning till skillnad från GoogleDrive som inte gör detta.

Vid uppladdning till molntjänsternas applikation med 1 fil 1 gång så presterade GoogleDrive bättre än Dropbox. Skillnaden mellan de bägge tjänsterna var låg vid låg filstorlek men ökade i takt med att större filer testades. Vid den största filstorlek 2000MB tog det 161sekunder(12,4MB/s) för GoogleDrive medan för Dropbox tog det 196sekunder(10,2MB/s). Anledningen till detta nämndes i analysen och kan vara att skrivhastigheten till applikationsmappen innebär mindre uppladdningstid för användaren och mer hos molnleverantören.

Vid uppladdning till molntjänsternas applikation med 1 fil upprepade gånger (t.ex. då en fil uppdateras) så presterade Dropbox bäst. Detta resultat stod sig oavsett filstorlek. Vid 2000MB filstorlek tog det Dropbox 55sek att återuppladda en fil medan för GoogleDrive tog det 183sek. Anledningen till detta är att Dropbox använder en ”hash” teknik. När en fil laddas upp till Dropbox via applikationsmapp bryts den ner i bitar. Informationen i dessa bitar sparas sedan på Dropbox. När samma fil läggs till igen känner den igen dessa bitar och ”fyller igen” de bitar som redan är indexerade hos Dropbox servrarna (Dropbox, 2014b).

Vid nedladdning av filer ifrån molntjänsternas gränssnitt presterade GoogleDrive bäst oavsett filstorlek. Skillnaden mellan de båda tjänsterna fortsatte öka ju större filstorlek som testades. Vid filstorleken 2000MB tog det GoogleDrive 186sek(10,5MB/s) att ladda ner en fil medan för Dropbox tog det 264sek(7,5MB/s). Detta resultat berodde på att GoogleDrive inte utför skanning av filer. Vid nedladdning av filer varnar webbgränssnittet att filstorleken är för stor för att kunna verifieras. Detta innebär att det inte finns någon extra overhead utan nedladdningen kan använda full bandbreddskapacitet.

För att besvara frågan ”Vilken av molntjänsterna Dropbox och GoogleDrive har bäst prestanda vid replikering av filer” utfördes tidsberäkning på ovanstående experiment. Replikering testades genom att beräkna den tid det tog för en fil att skapas eller synkas till en

annan dator som är aktör i samma molngrupp eller mapp. Detta mättes både när filer laddades upp direkt till webbgränssnittet eller till applikationen. Då replikering startas så fort en filuppladdning startar beräknas den totala tiden som replikeringstid, det vill säga uppladdning+replikering=total replikeringstid.

Vid replikering av låg filstorlek presterade de bägge molntjänsterna likvärdigt, gemensamt för bägge var att replikering var snabbare när filer laddades upp till applikationen istället för till webbgränssnittet. Vid större filstorlekar presterade GoogleDrive bättre än Dropbox med en hastighet med medelvärdet 600sekunder emot 800sekunder.

För att besvara frågan ”Hur mäter sig molntjänsterna Dropbox och GoogleDrive sig emot lokala lagringsmedium med tanke på prestanda” användes mätningar på prestanda av lokal lagringsmedia.

Resultatet visade tidigt att SSD presterar långt över de hastigheter som kunde uppmättas i uppladdning och nedladdningstesterna med en läshastighet på medelvärde 260 och skrivhastighet med medelvärde 150MB/s.

Testerna mot HDD visar att hastighet kan skilja sig vid små filstorlekar från 100-150MB/s för att vid större filstorlekar prestera jämt med en läshastighet på medelvärdet 140MB/s och en skrivhastighet på medelvärde 130MB/s.

Resultat vid test av USB visar en låg men jämn skriv och läshastighet oberoende av filstorlek. Med en läshastighet på ett medelvärde av 25MB/s och en skrivhastighet med ett medelvärde på 19MB/s tas slutsatsen att prestandatesterna som utfördes mot molntjänsterna i detta arbete inte kan prestera bättre än ett USB-minne, detta då gränsen för uppladdning och nedladdning på en 100/100 fiberanslutning är 12MB/s.

För att besvara frågan ”Vad finns det för säkerhet och integritetsbrister i molnlagring, hur påverkar detta Dropbox och GoogleDrive och hur hanterar de sin säkerhet” har en analys av litteraturstudier utförts. Denna visar att Dropbox har en större säkerhet, främst pågrund av dess nyckelhantering och kryptering av filer. Denna ökade säkerhet medför att prestanda sänks.

Utefter sammanfattade resultat kan en slutsats dras att vid krav av säkerhet och arbete emot samma fil så är Dropbox att rekommendera. Möjliga intressenter för denna lösning kan vara till exempel småföretag som vill hantera sina filer på internet istället för att använda ”BYOB” (bring-your-own-device). Ifall prestanda är viktig och säkerhetskraven är låg lämpar sig GoogleDrive bättre då den i tester presterade bättre på nästan samtliga prestandatester.

8.2 Diskussion

För att testa prestanda för de olika molntjänsterna genomfördes ett flertal experiment. I arbetets begynnelse planerades filerna vara 10,50,100,500,1000,2000MB stora. Detta ändrades då det fanns ett stort tomrum mellan 100 och 500MB filerna, ett mellanrum där det visade sig att resultaten ändrade sig stort. Ändringen till nuvarande filstorlekar baserades även på storleksökningen mellan de olika filerna. Optimalt utgångsläge är att filer relaterar till varandra med en faktor av 2, det vill säga storleken på filerna ökar med 100 %. Detta visade sig vara svårt då som innan nämnt, ett stort mellanrum fanns. Att sätta en filstorlek på 250MB medbar att nästa filstorlek ökas med 100 %. Detta fick bli en kompromisslösning.

För att testa säkerhet var det planerat att testa de uppdagade säkerhetsbristerna ifrån litteraturanalysen. Detta visade sig vara ett för ambitöst mål då flera av dessa krävde utrustning som inte gick att tillgå samt att lagbrott förmodligen hade ägt rum. Vissa av testerna kunde testas manuellt som t.ex. de i kap 7.2.1.

De validitetshot som identifierades i sektionen 4.3.3 har till viss del besvarats av resultaten. Problemet med spridning och balansering åtgärdades genom att utföra tester på olika tidpunkter. Resultatet av detta var att marginalen på resultaten mellan de olika testerna var accepterbar för att minska den yttre validiteten. Vid körning av fler tester hade denna kunnat förstärkas ytterligare med ett tydligare spridningschema. Den externa validiteten med tanke på generalisering över en population kunde inte stärkas efter tester. Detta pågrund av sparsam information om användarantal och den egentliga påverkan på användning. En generell slutsats som kan dras är att inom samma land med samma hårdvara och nätverkshastighet bör resultaten vara generaliserbara.

Konstruktionsvaliditeten, det vill säga slutsatserna kring konstruktion och operationaliseringar kunde till viss del stärkas. Labbuppsättningen med Windows 8.1 och förinstallerade program och tjänster störde inte uppladdning eller skrivprestanda då tester utfördes när aktivitetshanteraren visade 0 % utnyttjande.

8.3 Framtida arbete

De prestandatester som utförts har gett en grundläggande insikt i hastigheter och tidsåtgång vid uppladdning, nerladdning och replikering av filer. Vidare studier hade kunnat ge mer intressanta värden.

Vid prestandatester användes skapades ”dummy” filer innehållande ingen direkt data, ingen mappstruktur. Mer resultat hade kunnat presenteras om prestanda påverkas av typen av fil. Test av filtyper som: mp3, komprimerade filer, text dokument eller mappstrukturer hade kunnat ge ett större djup till arbetet.

De tester som presenterades utfördes i en begränsad labbmiljö. Experimentet hade ytterligare kunnat valideras ifall de repeterats i en annan labbmiljö med liknande resurser och/eller oliknande resurser för att mäta exakt vart prestandagränsen går. Att utföra experimentet i en utökad miljö hade ochså kunnat ge svar på hur prestanda påverkas vid samtidig uppladdning eller nerladdning av en fil.

Referenser

Amazon. (2013). *Amazon Clouddrive*. Tillgänglig på Internet: http://aws.amazon.com/ Hämtad [09.03.14].

Borgmann, M., Hahn, T., Herfert, M., Kunz, T., Richter, M., Viebeg, U. & Vowé, S. (2012). *On the security of Cloud Storage Services.* Fraunhofer Institute for Secure Information Technology.

Bort, Julie. (2013). *The 10 Most Important Companies In Cloud Computing*. Tillgänglig på Internet: http://www.businessinsider.com/10-most-important-in-cloud-computing-2013-4?op=1 Hämtad [09.03.14].

Botero-Perez, D., Szefer, J. & Lee, R. B. (2013) *Characterizing hypervisor vulnerabilities in cloud computing servers*. Cloud Computing'13 Princeton University, Princeton, NJ, USA.

Butler, Brandon. (2013). Gartner: Top 10 cloud storage providers. Tillgänglig på Internet: http://www.networkworld.com/news/2013/010313-gartner-cloud-storage-265459.html Hämtad [13.04.14].

Clouddrive. (2013). *Cloud drive*. Tillgänglig på Internet: http://www.clouddrive.com.au/download/www.clouddrive.com.au-WhitePaper.pdf Hämtad [05.11.13].

Computernetworkingnotes. (2014). *Network Security Types of attacks*. Tillgänglig på Internet: http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html. Hämtad [07-06-14].

Crystal Dew World. (2014). CrystalDiskMark. Tillgänglig på Internet: http://crystalmark.info/software/CrystalDiskMark/index-e.html. Hämtad [06-06-14].

Drago, I., Sperotto, A., Mellia, M., Sadre, R., Munafó M, M. & Pras, A. (2012). *Inside Dropbox: Understanding Personal Cloud Storage Services*. University of Twente

Dropbox. (2014a). *Your stuff, anywhere*. Tillgänglig på Internet: https://www.dropbox.com/. Hämtad [09.03.14].

Dropbox. (2014b). *Does dropbox always upload/download the entire fil any time a change is made?* Tillgänglig på Internet:https://www.dropbox.com/help/8/en. Hämtad [07-06-14].

eHow. (2014). Laptop Vs. Desktop Hard Drives. Tillgänglig på Internet: http://www.ehow.com/way_5459146_laptop-vs-desktop-hard-drives.html. [Hämtad 25.05.14].

Engfors, Tommy. (2011). *Kryptering ingen garanti för säkerhet i usb-minnen*. Tillgänglig på Internet: http://techworld.idg.se/2.2524/1.364196/kryptering-ingen-garanti-for-sakerhet-i-usb-minnen. Hämtad [09.03.14].

Florentine, Sharon & Olavsrud, Thor. (2013). *2014 Forecast for Cloud Computing*. Tillgänglig på Internet: http://www.cio.com/article/745155/2014_Forecast_for_Cloud_Computing?page=1&taxonomyId=3024. Hämtad [09.03.14].

Garcia, L. J., Langenberg, R. & Suri, N. (2012) *Benchmarking cloud security level agreements using quantitative policy trees*. CCSW'12 Dept. Of CS, TU Darmstadt, Germany.

Golden, Bernard. (2013). *10 Cloud Computing Predictions for 2014*. Tillgänglig på Internet: http://www.cio.com/article/745155/2014_Forecast_for_Cloud_Computing?page=1&taxonomyId=3024. Hämtad [09.03.14].

Google. (2012). *Google Cloud Storage – a simple way to store, protect, and share data*. Tillgänglig på Internet: https://cloud.google.com/files/CloudStorage.pdf Hämtad [05.11.13].

Gusev, M., Ristov, S. & Donevski, A. (2013) *Security vulnerabilities from inside and outside the eucalyptus cloud*. BCI'13 Princeton University, Princeton, NJ, USA.

Huth, A. & Cebula, J. (2011). *The Basics of Cloud Computing*. Carnegie Mellon University.

Ltrdata. (2014). *Tools and utilities for Windows*. Tillgänglig på Internet: http://www.ltr-data.se/opencode.html/. Hämtad [06-06-14].

Krawczyk, Konrad. (2013). *What's the Fastest Cloud Storage Service?*. Tillgänglig på Internet: http://blog.laptopmag.com/whats-the-fastest-cloud-storage-service. Hämtad [10.03.14].

Kholia, D. & Wegrzyn, P. (2013). *Looking inside the (Drop) box*. Openwall/University of British Columbia, CodePainters.

Lifehacker. (2013). *Five Best Cloud Storage Providers*. Tillgänglig på Internet: http://lifehacker.com/five-best-cloud-storage-providers-614393607. Hämtad [25.05.14].

Mahajan, P., Setty, S., Lee, S., Clement, A., Alvisi, L., Dahlin, M. & Walfish, M. (2012). *Depot: Cloud Storage with Minimal Trust*. The University of Texas at Austin.

Mell, Peter & Grance, Timothy. (2011). *The NIST Definition of Cloud Computing*. U.S. Department of Commerce. National Institute of Standards and Technology.

Microsoft. (2014). *SyncToy 2.1*. Tillgänglig på Internet: http://www.microsoft.com/en-us/download/details.aspx?id=15155. Hämtad [15.04.14].

Mynikko. (2014). *Dummy File Creator*. Tillgänglig på Internet: http://www.mynikko.com/dummy/. Hämtad [06.06-14].

Open Grid. (2009). *Cloud Storage for Cloud Computing*. Tillgänglig på Internet: http://ogf.org/Resources/documents/CloudStorageForCloudComputing.pdf Hämtad [05.11.13].

Ristenpart, T. & Tromer, E. & Shacham, H. and Savage S. (2009) *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds*. CCS'09 Dept. Of Computer Science and Engineering University of California, San Diego, USA.

SiSoftware. (2014). *SiSoftware*. Tillgänglig på Internet: http://www.sisoftware.net/. Hämtad [10.03.14].

Smith, Matt. (2010). *The 5 Best Free Benchmark Programs for Windows*. Tillgänglig på Internet: http://www.makeuseof.com/tag/5-free-benchmark-programs/. Hämtad [10.03.14].

TechNet. (2014). *Common Types of Network Attacks*. Tillgänglig på Internet: http://technet.microsoft.com/en-us/library/cc959354.aspx. Hämtad [07-06-14].

TrendLabs. (2012). *What You Need to Know About Cloud Storage*. Tillgänglig på Internet: http://about-threats.trendmicro.com/ebooks/files-in-flight/files/assets/downloads/files-in-flight.pdf. Hämtad [05.11.13].

Userbenchmark. (2014). *What is sequential read speed?* Tillgänglig på Internet: http://www.userbenchmark.com/Faq/What-is-sequential-read-speed/44. Hämtad [21.05.14].

W3schools. (2014). *Browser Statistics*. Tillgänglig på Internet: http://www.w3schools.com/browsers/browsers_stats.asp. Hämtad [15.04.14]

Wikipedia. (2014a). *Time-based One-time Password Algorithm*. Tillgänglig på Internet: http://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm. Hämtad [25.05.14].

Wikipedia. (2014b). *Two-step verification*. Tillgänglig på Internet: http://en.wikipedia.org/wiki/Two-step_verification. Hämtad [07-06-14].

Zetta. (2014). *The History of Computer Storage*. Tillgänglig på Internet: http://www.zetta.net/history-of-computer-storage/. Hämtad [10.03.14].