CHALMERS

Konfidentialitets- och integritetsbevarande datautbyten

Kandidatrapport VT2020 – TEKX04-24

Alfred Arvidsson
David Bejmer
Mattias Gemborg
Jakob Hendén
Johan Ljusegren
Theodor Stenhammar

INSTITUTIONEN FÖR TEKNIKENS EKONOMI OCH ORGANISATION

CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige 2020
www.chalmers.se

Kandidatarbete TEKX04-20-24

Kandidatarbete TEKX04-20-24

Konfidentialitets- och integritetsbevarande datautbyten

Confidentiality preserving data exchanges

ALFRED ARVIDSSON
DAVID BEJMER
MATTIAS GEMBORG
JAKOB HENDÉN
JOHAN LJUSEGREN
THEODOR STENHAMMAR

TEKNIKENS EKONOMI OCH ORGANISATION

CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige 2020

Konfidentialitets- och integritetsbevarade datautbyten

ALFRED ARVIDSSON DAVID BEJMER
MATTIAS GEMBORG JAKOB HENDÉN
JOHAN LJUSEGREN THEODOR STENHAMMAR

Kandidatarbete TEKX04-20-24
Teknikens ekonomi och organisation
Chalmers tekniska högskola
412 96 Göteborg
Sverige
Telefon + 46 (0)31-772 1000

Omslag: Ett hänglås inneslutet av kretskort. Bilden symboliserar datasäkerhet.

Göteborg, Sverige 2020
Gothenburg, Sweden 2020

Confidentiality preserving data exchanges
A study of computer security and security in data transmissions

ALFRED ARVIDSSON DAVID BEJMER
MATTIAS GEMBORG JAKOB HENDÉN
JOHAN LJUSEGREN THEODOR STENHAMMAR

Department of Technology Management and Economics
Chalmers University of Technology

SUMMARY

In an increasingly digitalized world, more data is shared between various actors in society. This opens up for data leaks and attacks that can compromise the security of sensitive data and people's privacy. Today there are several technologies that potentially can aid different parts of this problem but few are implemented.

In this study we analyse various security shortcomings in a given number of next generation digital services and which confidentiality and privacy preserving technologies has the potential to address these. The analysis provides discussions about the different technologies' strengths and weaknesses in terms of a number of criteria and how these can be applied to improve the security of the studied scenarios.

The study concludes that there are several flaws that can be managed by the implementation of existing technologies. However, there is no silver bullet and often a combination of different technologies are required. This makes security and functionality trade-offs necessary to consider today, which makes it valuable to further research and develop technologies like these.

The report is written in Swedish.

Keywords: Data security, Data transmissions, Confidentiality, Privacy, E-voting, E-health, Telehealth, Digital benchmarking, Encryption, Edge computing, Distributed Ledgers, DAO

SAMMANFATTNING

I en allt mer digitaliserad värld delas allt mer data mellan olika aktörer i samhället. Detta öppnar upp för dataläckor och attacker som kan äventyra säkerheten för känslig data och människors integritet. Idag finns flera tekniker som potentiellt kan lösa delar av problemet men få är implementerade.

I denna studie analyseras olika säkerhetsbrister i ett visst antal nästa generations digitala tjänster och vilka tekniker för skydd av konfidentialitet och integritet som har potential att hantera dessa brister. I analysen diskuteras olika teknikers styrkor och svagheter i termer av ett antal kriterier och hur dessa kan tillämpas för att förbättra säkerheten i de studerade scenarierna.

Studien drar slutsatsen att det finns flera brister som kan hanteras genom implementering av befintlig teknik. Det finns dock ingen universiallösning och ofta krävs en kombination av olika tekniker. Detta gör avvägningar av säkerhet och funktionalitet nödvändiga att ta hänsyn till idag, vilket gör det värdefullt att vidareutveckla och utveckla tekniker som dessa.

Ordlista

Här följer ett antal definitioner med syfte att klara upp tvetydiga begrepp och koncept, samt för att underlätta förståelsen av vissa tekniska termer.

Konfidentiella data
Känsliga data som inte får spridas fritt, till exempel brottsregister eller information som skyddas av avtal med en arbetsgivare.

Säker datahantering
En teknisk lösning som garanterar att information som lagras och byts ut inte kan användas i syften som ägaren av datan var omedveten om.

Open respektive Closed source-mjukvara
Mjukvara vars källkod endast är synlig för ägaren eller en stängd grupp ursprungliga utvecklare kallas Closed source. Open source-mjukvara är mjukvara där utvecklingen sker öppet och vem som helst kan bidra till projektet.

Integritet
Med integritet menas rätten till en dold identitet vid exempelvis datatransaktioner. Detta kan innebära skydd av personuppgifter eller en persons beteende och utseende.

Konfidentialitet
Begreppet konfidentialitet används i detta sammanhang som skyddandet av data från icke-auktoriserade utomstående parter. I de bredare och mer generella diskussionerna låter vi begreppet konfidentialitet även innefatta integritet, såvida inte annat anges.

Internet of Things (IoT)
Det nätverk som uppstår med alla enheter, så som övervakningskameror, sensorer och hushållselektronik, som är anslutna till internet.

Innehållsförteckning

1 Inledning

En följd av digitaliseringen i samhället är att allt fler privatpersoner och andra aktörer delar data med varandra. Datadelning lägger grunden för både digitala tjänster och nöjesplattformar, vilka båda är snabbt växande områden.

Europeiska unionen har nyligen implementerat åtgärder (GDPR) för att tvinga företag att lagra data mer transparent och därmed öka privatpersoners medvetenhet om vilka personliga data som lagras av företag samt försöka hindra att individers data missbrukas (Datainspektionen, u.d.). Denna lagstiftning förhindrar dock inte trenden att mer data delas mellan fler parter.

Ett flertal initiativ har som mål att förbättra integriteten för världens befolkning genom digitala tekniker på internet och i andra sammanhang. MyData (2020) är ett projekt som strävar efter att privatpersoner ska få bättre kontroll över data som samlats in från dem. ESSIF (2020) är ett EU-finansierat projekt för att ge alla en digital identitet som kontrolleras av en själv, för att underlätta till exempel digitala och fysiska transaktioner. Dessa initiativ är bara några tecken på att integritet blir en allt viktigare fråga.

Trots en tilltagande diskussion om integritet lyfter Internetstiftelsen (2019) fram att de allra flesta internetanvändarna accepterar användarvillkor för tjänster utan att läsa dess villkor. Detta antyder dessutom att många internetanvändare saknar insikt om hur deras data delas och används.

1.1 Bakgrund

Ökad datadelning leder till ökad risk för intrång och missbruk av data. I en undersökning av Greenwich associates (2016) uppger över hälften av de tillfrågade att konfidentialitet i digitala transaktioner är ett stort säkerhetsbekymmer. I en undersökning av McAfee uppger dessutom 43% att de känner en avsaknad av kontroll över deras personliga data (Davis, 2018). Utifrån dessa undersökningsresultat kan det konstateras att säkerhet i transaktioner med data är ett viktigt område att utveckla, och att hitta metoder för att bättre bevara konfidentialiteten vid delning av data är högaktuellt idag.

Det har under senare tid uppstått skandaler och dataläckor på grund av bristande säkerhet i datahantering. Exempelvis i fallen med Ring Security Systems där privata videoströmmar från övervakningskameror exponerades till icke-behöriga (Cox, 2020) och TastSev Borger där 1.2 miljoner personers privata personnummer läcktes (Cimpanu, 2020). Eftersom det finns starka ekonomiska incitament att genomföra cyberattacker behöver dataskyddsåtgärder utvecklas löpande för att kunna hålla jämna steg med hackare (Kesan, Majuca, & Yurcik, 2004).

En risk som uppstår i samband med storskalig delning av data är att till synes orelaterade data tillsammans kan göra det möjligt för ytterligare slutsatser att dras. Detta medför att en aktör indirekt kan dela med sig av information utan att själv inse det, då informationen endast existerar implicit.

1.2 Syfte

Studien syftar till att utreda vilka konfidentialitets- och integritetsbevarande tekniker som finns idag och hur de kan kombineras för att göra dataöverföringar mer konfidentialitets- och integritetsbevarande.

1.3 Avgränsningar

På de tekniskt avancerade områden rapporten behandlar begränsas detaljgraden till den nivå som är nödvändig för att förstå områdets syfte. Det betyder att många koncept inte beskrivs ingående, utan att de snarare beskrivs utifrån dess relevans för studien och vilken in- och utdata som behandlas.

1.4 Frågeställning

- Vilka säkerhetsbrister förekommer i digitala tjänster idag?
- Vilka konfidentialitets- och integritetsbevarande tekniker finns idag?
- Hur står sig de befintliga teknikerna jämfört med varandra och hur väl bevarar de konfidentialitet och integritet?

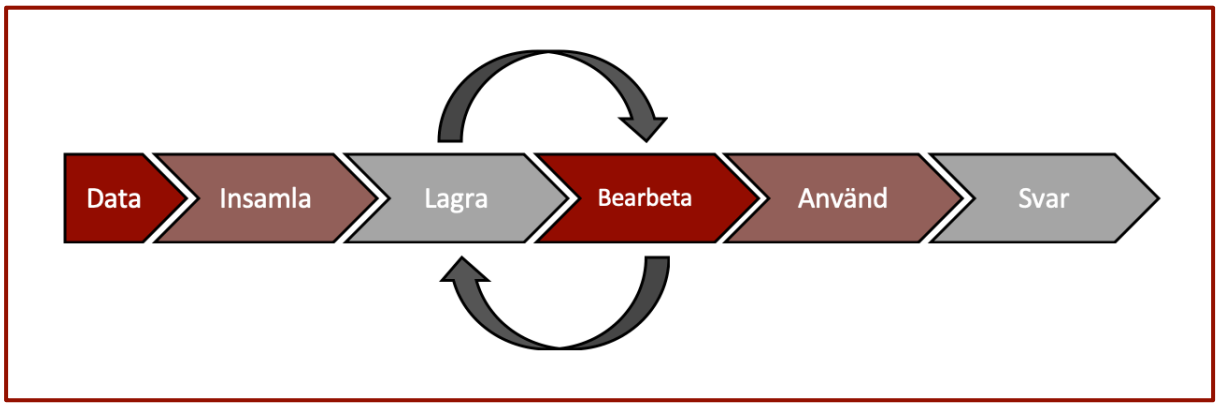
2 Litteraturgenomgång

För att öka konfidentialitets- och integritetsbevarandet i digitala tjänster finns ett antal olika tekniker som är applicerbara i olika situationer och sammanhang. Nedan presenteras de tekniker som är relevanta för rapportens fortsatta innehåll. Avsnittet kan med fördel användas som ett uppslagsverk under läsning av rapporten.

2.1 Data och datautbyten

Data kan komma i många olika former och strukturer men vad de alla har gemensamt är att information sammanställts på ett sätt som ska lämpa sig för kommunikation, beräkningar eller avläsning (University of Minnesota, u.d.). I tekniska termer är data information som kan lagras i till exempel strängar och tabeller.

Data som samlats in kan behöva olika grader av bearbetning innan den kan leverera relevanta svar till konsumenten. Till exempel kan data innehålla information om lufttryck och vind, men behöva bearbetas för att säga något om vädret. Bearbetningen och lagringen av data behöver inte ske på samma plats, eller av samma aktör, som datan samlades in. Processen från att data samlas in till att insikter genereras kan se ut som iillustreras enligt figur 1.



Figur 1 – Tidslinje för bearbetande av data

2.2 Kryptering

Kryptering är en metod som kan användas för att hålla meddelanden eller annan data hemlig, och fungerar genom att på ett systematiskt sätt chiffrera eller omvandla datans innehåll till en annan form som inte enskilt kan avslöja den ursprungliga

informationen (Buschmann, 2004). Att omvandla chiffrerad information tillbaka till sin ursprungliga form kallas dekryptering eller dechiffrering. En säker kommunikation utnyttjar en kombination av krypterings- och dekrypteringsalgoritmer och följer ett tillvägagångssätt som vanligtvis kallas ett schema (Goldreich, 2004).

Det är en så kallad krypteringsnyckel som bestämmer enligt vilka regler som meddelandet har chiffrerats (Delfs & Knebl, 2007). Olika krypteringstekniker utnyttjar krypteringsnycklar på olika sätt, och är olika flexibla när det gäller vad den krypterade data hindrar eller möjliggör. Nedan presenteras metodiken och egenskaperna för de mest kända krypteringsmetoderna.

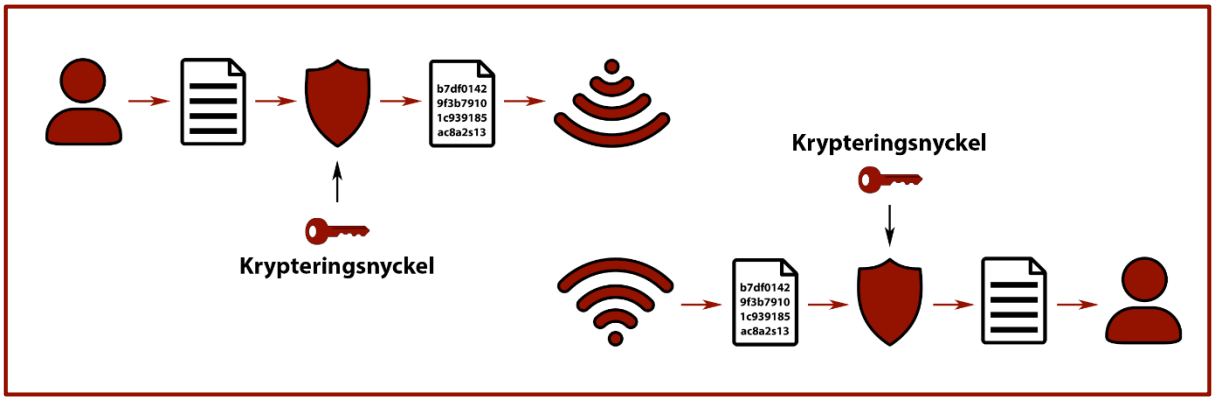
2.2.1 Symmetrisk kryptering

Symmetrisk kryptering tillåter sekretess i kommunikation mellan två parter. En tredje part som avläser informationen däremellan kan inte få ut någon signifikant information om dess innehåll. Symmetrisk kryptering har den snabbaste implementeringen i både mjukvara och hårdvara, och är därmed väl passande för kryptering av stora datamängder (Delfs & Knebl, 2007).

För att detta ska vara möjligt måste båda parter i transaktionen komma överens om en gemensam krypteringsnyckel k och vara överens om att hålla den hemlig från tredje parter. Innan sändaren skickar meddelandet m krypterar den meddelandet med en krypteringsalgoritm E, och resultatet är en oförståelig röra av bokstäver (chiffertext) $c = E(k, m)$. Denna chiffertext skickas till mottagaren. Eftersom c är den enda information som lämnar sändaren, hindras eventuella tredje parter från att avläsa informationen. Mottagaren dekrypterar chiffertexten med algoritmen $D(k, c)$ och får därmed ut det ursprungliga meddelandet $m = D(k, c)$ med vetskapen att ingen kunnat avläsa det sedan det lämnat avsändaren (Delfs & Knebl, 2007) (Buschmann, 2004).

Symmetrisk kryptering är i teorin en säker krypteringsmetod, men inte lika mycket så i praktiken. Anledningen till detta är att den baserar sig på antagandet att de ingående parterna enas om en krypteringsnyckel k som de håller hemlig från utomstående parter (Goldreich, 2004). Detta är problematiskt, eftersom parterna behöver utbyta k

genom en annan säker kommunikationskanal för att försäkra att de är ensamma om att inneha den. En säker kommunikationskanal kan exempelvis uppnås genom användning av asymmetrisk krypering som behandlas i avsnitt 2.2.2. I figur 2 presenteras ett översiktligt schema över hur symmetrisk kryptering används.



Figur 2 - Symmetrisk kryptering (Goldreich, 2004)

2.2.2 Asymmetrisk kryptering

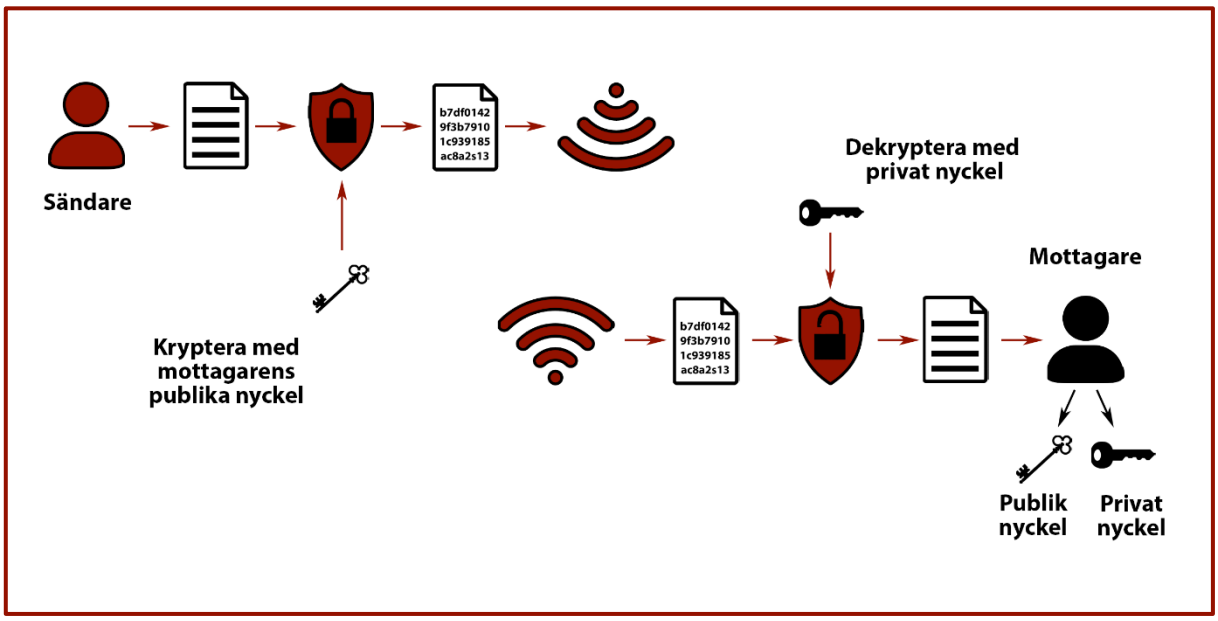
Asymmetrisk kryptering (AK), mer känt som public key cryptography garanterar sekretess i kommunikation mellan två parter utan behovet av en gemensam krypteringsnyckel k. AK kan utöver detta användas till autentisering av avsändare eller mottagare (Delfs & Knebl, 2007).

Ingen gemensam krypteringsnyckel krävs. Istället har varje aktör två nycklar som har ett matematiskt samband, sådant att vardera nyckeln fungerar asymmetriskt och endast kan chiffrera (K_p) eller dechiffrera datan (K_s). Chiffreringsnyckeln kallas publik nyckel (public key) och dechiffreringsnyckeln kallas privat nyckel (private key) (Delfs & Knebl, 2007).

En säker transaktion med AK fungerar genom att sändaren använder sig av mottagarens publikt tillgängliga chiffreringsnyckel K_{pm} för att chiffrera meddelandet m med en krypteringsalgoritm E. Alltså kan inte sändaren själv upphäva krypteringen efter att meddelandet skickats.

Resultatet av denna är chiffertexten $c = E(K_{pm}, m)$. Denna chiffertext skickas till mottagaren. Chiffertexten c är oläslig och intetsägande för en eventuell tredje part som

skulle avläsa meddelandet innan det nått mottagaren. Mottagaren dechiffrerar meddelandet med dekrypteringsalgoritmen D, och meddeladet $m = D(K_{sm}, c)$ erhålls genom utnyttjande av mottagarens privata nyckel (Delfs & Knebl, 2007). I figur 3 presenteras ett översiktligt schema över hur multinyckel-kryptering används.



Figur 3 – Asymmetrisk kryptering (Goldreich, 2004)

2.2.3 Homomorfisk kryptering

Homomorfisk kryptering tillåter utförande av modifierande matematiska operationer på den krypterade datan (Fan & Vercauteren, 2012). Det finns inte någon standard eller heltäckande homomorfisk krypteringsmetod som används och som i praktiken tillåter alla slags matematiska modifieringar, men Gentry (2009) har bevisat att det är teoretiskt möjligt.

Alla existerande homomorfiska metoder har gemensamt att ”brus” genereras som en konsekvens av de matematiska operationerna. Utförande av operationer på datan amplifierar brusets storlek, och när bruset växt tillräckligt stort så börjar datan förloras. Framför allt homomorfisk multiplikation är ett stort hinder för skapandet av homomorfiska metoder, då det genererar mycket brus (Fan & Vercauteren, 2012).

2.3 Multifaktorautentisering

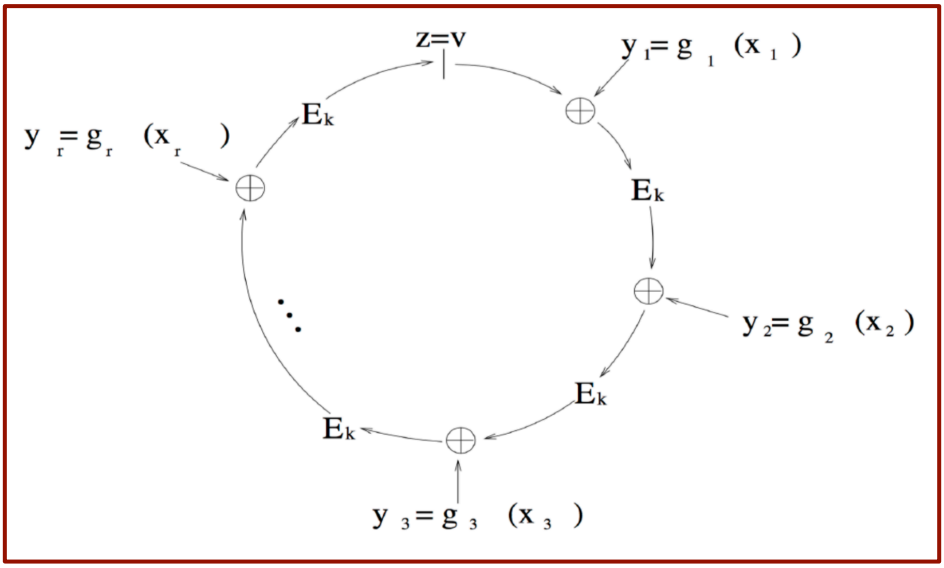
Multifaktorautentisering (MFA) är en slags identitetsautentisering som kräver fler än en slags information om användaren. Det krävs alltså två eller flera autentiseringsfaktorer för att säkerställa att det verkligen är rätt person som ligger bakom autentiseringen. De vanligaste autentiseringsfaktorerna är; någonting användaren vet, någonting användaren har, någonting användaren är och användarens plats (Dasgupta, Roy, & Nag, 2017). Praktiska exempel kan vara lösenord som användaren vet, en mobil som användaren har och ett fingeravtryck eller röst som användaren ”är”.

Anledningen till att multifaktorautentisering är säkrare är att informationen från en dataläcka inte är tillräckligt för att en person ska kunna autentisera sin identitet som någon annan (Dasgupta, Roy, & Nag, 2017).

2.4 Ringsignaturer

Ringsignaturer är ett sätt att skapa en digital signatur som inte avslöjar vem som ursprungligen signerat informationen, genom att låta flera bulvaner delta i signeringen. Det går att verifiera att signaturen är gjord av gruppen, men inte vilken enskild individ som ligger bakom indatan. Detta faktum innebär att så länge alla ringmedlemmar enskilt uppfyller kraven för signering, så kan en ringsignatur substituera vilken digital signatur som helst, men samtidigt säkerställa integritet för indatans ägare.

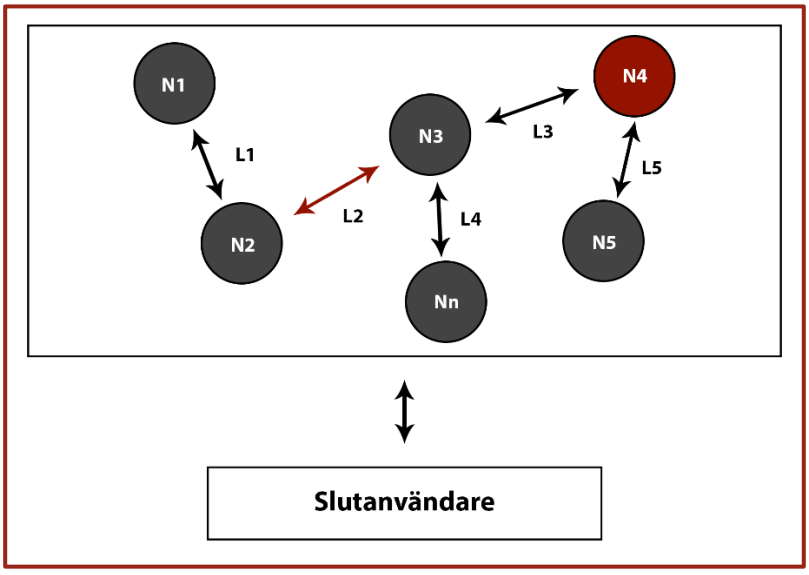
Genom att konstruera en ringformation av medlemmarnas publika nycklar, och låta utdatan från en kryptering vara indatan i nästa, kan man genom att endast ha kännedom om en private key verifiera att slutliga utvärdet z är lika med det ursprungliga indatan v. Ursprungliga schemat för en ringsignatur av Rivest, Shamir & Tauman (2001) illustreras i figur 4.



Figur 4 - Schemat för en ringsignatur (Rivest, Shamir, & Tauman, 2001)

2.5 Distribuerade system

Distribuerade system är ett paradigm inom datahantering och innebär att två eller fler noder arbetar tillsammans och koordinerat för att uppnå ett gemensamt mål (Bashir, 2018). För användaren kan det dock vara svårt att skilja på vad som är ett distribuerat system och vad som är en enda plattform, då de oftast inte skiljer sig på ytan. Noderna som bygger upp ett distribuerat system består av ett minne och en processor och brukar sägas kunna vara ärliga, oärliga eller felaktiga. Ett exempel på ett distribuerat system visas i figur 5.



Figur 5 - Exempel på ett distribuerat system (Bashir, 2018).

Bashir (2018) menar att den största utmaningen med distribuerade system är samspelet mellan noderna samt toleransen för fel. Fel kan leta sig in i form av felaktiga eller oärliga noder (N4 ovan), eller genom dåliga kopplingar (L2 ovan) som därmed skapar partitioner i nätverket. En stor del av utvecklingen kring distribuerade system handlar därför om att skapa system som klarar av att fungera i ej felfria miljöer.

Utifrån dessa inneboende svårigheter med distribuerade system har det så kallade *CAP-teoremet* bevisats. CAP-teoremet menar att distribuerade system inte kan ha samstämmighet (consistency), tillgänglighet (availability) och partitionstolerans (partition tolerance) samtidigt (Gilbert & Lynch, 2002). Samstämmighet betyder här att systemet returnerar rätt svar till en given begäran, tillgänglighet att en begäran ens returnerar ett svar, oavsett svarstid, och partitionstålighet hur bra systemet klarar av situationer där delar av nätverket tappar kontakt med varandra.

Då ett distribuerat system per definition är benäget till partitionering betyder det i praktiken att man antingen får offra tillgänglighet eller samstämmighet. Det sker dock mycket utveckling inom området och det finns modeller som till hög grad kan garantera båda dessa (Gilbert & Lynch, 2012).

2.6 Blockkedjor

Blockkedjor är en teknik som baseras på distibuerade system. Ett generellt problem att beakta vid transaktioner av information mellan två parter är hur registerföringen ska ske. Såvida inte de två parterna förlitar sig på att en extern central auktoritet håller register eller tillsammans godkänner att en av de två ingående parterna gör detta så är enligt Witte (2016) den enda lösningen två noggrant koordinerade och matchade självständiga register som samtidigt hålls av de ingående parterna.

År 2009 introducerades Bitcoin vilket var den första framgångsrika implementationen av en blockkedja (Bashir, 2018). Blockkedjeteknologin utgörs av en distribuerad databas som består av en kedja av block, registret, som ej kan manipuleras eller revideras i efterhand, vilket möjliggör transaktioner mellan olika parter som inte litar på varandra utan inblandning av en tredje part (Bashir, 2018). Detta garanterar också att inga nya pengar olagligt kan skapas i fallet med exempelvis Bitcoin (Witte, 2016).

Yli-Huumo, Ko, Choi, & Sooyong Park (2016) förklarar att majoriteten av forskningen på blockkedjor fokuserar på att förbättra deras användningsområde, och att kringgå dess brister, men att många av de föreslagna lösningarna saknar konkret utvärdering av deras effektivitet. Dessutom fokuserar fyra femtedelar av forskningen på kryptovalutor, och en mycket mindre andel avser forskning på blockkedjebaserade program och applikationer.

2.7 Lokal beräkning

Cao, Zing och Shi (2018) definierar edge computing, vilket i rapporten benämns som lokal beräkning, som de teknologier som möjliggör bearbetande av data vid ett nätverks gräns. Principen bygger på att behandlingen av data kan ske i närheten av insamlingspunkten och alltså inte behöver skickas iväg till en molnbaserad tjänst för att processas. Genom att flytta processandet av data närmre källan kan bland annat latensen minskas (Hamilton, 2018). Vid en prototyp av en platform för ansiktsigenkänning gick exempelvis responstiden ner från 900 millisekunder till 169 millisekunder (Cao, Zhang, & Shi, 2018).

Tidigare har processkraften hos en molntjänst ofta varit bättre än den vid en lokal enhet. Detta är dock något som ändrats under senare år då processorkraften haft en hög utvecklingstakt i jämförelse med utvecklingen av bandbredd i nätverk (Cao, Zhang, & Shi, 2018). Bandbredden blir alltså en flaskhals för bearbetande av data, vilket innebär att lokal beräkning är fördelaktigt då data inte behöver skickas iväg för att bearbetas.

Detta blir relevant i exempelvis bilbranschen då Toyota (2017) uppskattar att datautbytet mellan bilar och molntjänster kommer uppgå till tio exabytes (10 000 000 terabytes) år 2025. Enligt Toyota kommer bilarna då kräva mer än bara molnbaserade tjänster. Fortsatt ökar antalet enheter som ingår i internet of things vilket i sin tur innebär att antalet enheter vid gränsen av ett nätverk också ökar. Detta kan leda till en drastisk ökning av rådata vilket skulle kunna göra typiska molntjänster otillräckliga för att hantera all data (Cao, Zhang, & Shi, 2018).

Kapacitetsbegränsande faktorer som responstid och bandbredd hos molnbaserade tjänster har drivit utvecklingen av lokal beräkning men det finns ytterligare en fördel; säkerhet. Risken att data hamnar i orätta händer minskar om den inte behöver skickas och lagras på fler enheter. Om data inte är lagrad på en molntjänst minskar risken för att stora datamängder ska utsättas för ett dataintrång eller en eventuell läcka. Det blir istället viktigt att den lokala enheten är tillräckligt pålitlig och inte känslig för dataintrång (Hamilton, 2018).

Chapple (2019) föreslår dock att lokal beräkning inte kommer att fullständigt ersätta centraliserad analys och lagring i fallet av hälsodata, utan att lokal beräkning kan komma att utvecklas som ett komplement till centraliserad dataanalys.

3 Metod

I detta kapitel presenteras vilka metoder som används under studiens genomförande. Ställningstaganden som görs är vilken forskningsdesign och forskningsmetod som ska väljas. I forskningsdesign beskrivs de metoder som används i studien med stöd från relevant metodlitteratur. Avsnittet forskningsmetod redogör mer specifikt för arbetsgången. Därefter följer en diskussion om dessa val och hur de påverkar den övergripande forskningskvaliteten.

3.1 Forskningsdesign

Med kvalitativ forskning menas olika tolkande tekniker och metoder som syftar till att beskriva, översätta och förstå meningen av skilda fenomen (Frostling-Henningsson, 2017). Området som rapporten behandlar är väldigt brett och innefattar många tekniskt och konceptuellt svårförståeliga delar. Med detta som utgångspunkt har studien genomförts utifrån ett kvalitativt angreppssätt.

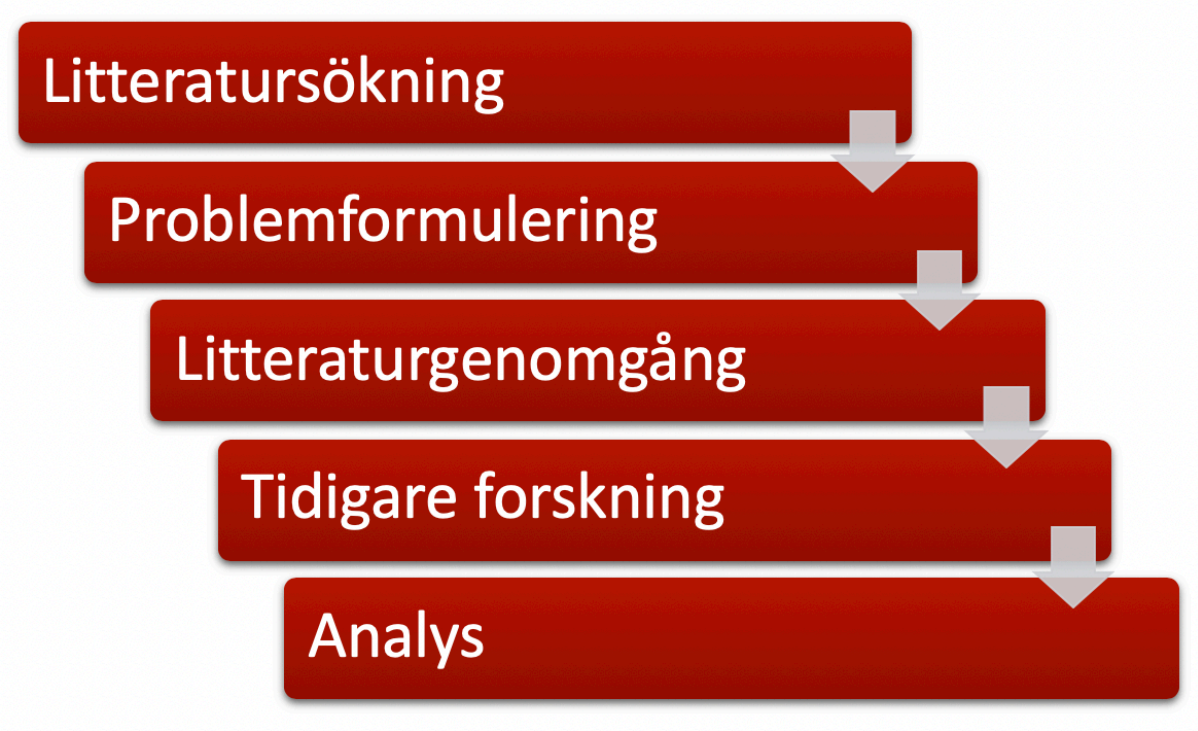
För att ytterligare konkretisera rapportens innehåll byggs den upp kring tre skilda fall, då det enligt National research council (1994) kan det lämpa sig att beskriva koncept inom området experimentell datavetenskap med hjälp av praktiska exempel istället för enbart med text.

Arbetssättet kan liknas till vad William M.K. Trochim (2020) kallar för induktiv metodansats. Trochim (2020) förklarar att den induktiva metodansatsen kännetecknas av ett pragmatiskt och utforskande första angreppssätt. Detta för att sedan notera mönster och kopplingar i litteraturen och utifrån dessa utforma teorier eller slutsatser, något som passar studiens arbetsgång.

Vid litteratursökning används kedjesökning vilket är ett sätt att hitta ytterligare relevanta källor och tillföra ett djup i det teoretiska ramverket (Ejvegård, 2003). De olika källorna kan dessutom med denna metod jämföras och ställas emot varandra. Denna triangulering av litteratur är en metod för att undvika felkällor i kvalitativa studier och kan bekräfta eller stärka resonemang och teorier (Hedin, 2011).

3.2 Forskningsmetod

I detta avsnitt presenteras studiens tillvägagångssätt. Genomförandet är uppdelat i den initiala litteratursökningen, problemformulering, litteraturgenomgång, studier av tidigare forskning och till sist analys. Tillvägagångssättet illustreras i Figur 6.



Figur 6 - Tillvägagångssättet i en 5-stegsmodell

3.2.1 Litteratursökning

Den initiala inläsningen ligger till grund för studiens problemanalys och utgår framförallt från litteraturrekommendationer av handledare Peter Altmann. Utöver dessa används också kedjesökning och triangulering av relevant information.

3.2.2 Problemformulering

Studiens initialt breda problemområde fokuseras mot en mer precis formulering av frågeställning och syfte genom diskussioner i samråd med handledare.

3.2.3 Litteraturgenomgång

Relevant litteratur sållas ut med utgångspunkt i rekommendationerna som anges i metodikkällorna som anges i avsnittet forskningsdesign och utifrån studiens frågeställning och syfte.

3.2.4 Tidigare forskning

En litteratursökning görs med de specifika fallen som utgångspunkt, där resultat från tidigare forskning samlas in. Dessa ligger sedan till grund för analysen som utförs enligt avsnitt 3.2.5.

3.2.5 Val av fall

Valen av fall är gjorda utifrån att de tillsammans fångar upp olika viktiga och relevanta aspekter för bevarande av konfidentialitet och integritet. Dessa är att de utgör kommunikation mellan olika aktörer i samhället där de tre fallen fokuserar på personliga-, samhälleliga- och företagsrelaterade tjänster. De illustrerar också olika slags datautbyten på grund av deras varierade utformning. Därtill ligger de också i framkant vad gäller digitala tjänster som utvecklas för att skapa ytterligare värde för samhällets aktörer. Med dessa kriterier hade ett mycket stort antal fall kunnat vara aktuella och det slutgiltiga valet gjordes utifrån intresse och preferenser. I den bedömningen ligger även relevansen av att skydda de olika aspekterna av konfidentialitet och integritet.

3.2.5.1 Fall 1 – Nyckeltaljämförelse

Nyckeltalsjämförelse är ett användbart medel för företag för att kunna jämföra sin position på en marknad mot andra aktörers. Det kan handla om att jämföra vinstmarginaler, personalkostnader, kvalitetsaspekter eller andra viktiga nyckeltal för att skapa insikt om sin prestation på marknaden.

En kritisk aspekt av nyckeltalsjämförelse är att den egna informationen eller nyckeltalet inte får läcka ut till övriga parter om informationen är av kompromettерande art, till exempel om det förekommer konkurrens dem emellan.

I dagsläget är det vanligt att det involveras en tredje betrodd part så som en managementkonsult som förädlar data och sedan distribuerar resultatet till parterna. Detta kan utgöra ett problem då det är svårt att avgöra huruvida en betrodd part verkligen är opartisk och inte går att påverka till någons fördel och dessutom kostar mycket pengar.

Då denna tredje part får full tillgång till de olika parternas data garanteras inte heller att deras integritet skyddas, vilket för med sig att den tredje partens ansvar ökar, och samtycke med gällande lagar och regler för säker datahantering kompliceras (The GWG task team on privacy preservation techniques, 2019).

I detta sammanhang kan nyckeltalsjämförelse anses utgöra ett viktigt och representativt exempel på när en grupp vill kunna dela data med varandra utan att blotta sin egen. Studien kommer därför titta på ett specifikt exempel på nyckeltalsjämförelse och utreda hur det med befintliga metoder går att göra nyckeltalsjämförelse mer konfidentialitets- och integritetsbevarande. Fokus kommer att ligga på hur beräkningen sker samt hur integriteten hos medlemmarna i nätverket kan bevaras utifrån resultatet.

3.2.5.2 Fall 2 – Hemtjänst

Datautbyten mellan två parter, en sändare och mottagare, sker överallt. Beroende på datautbytets natur kan det vara relevant att dölja en eller flera av data, avsändare och mottagare. Det kan även vara viktigt att kunna säkerställa trovärdighet av information och att kunna kontrollera att de delaktiga parterna är vilka de utger sig för att vara. Dessa problemområden är högst relevanta för studien och ett exempel där en part behöver dela med sig av känslig information till en andra part studeras i mer detalj.

Där teknologisk utveckling kan rädda liv och med en uppsjö av känsliga data är hälso- och sjukvården ett väldigt relevant område. Vidare väntas antalet IoT-enheter passera 500 miljarder dollar i värde inom sjukvården år 2025 (Tynan, 2019). Samtidigt har antalet dataintrång också ökat i detta område det senaste decenniet (Dwivedi, Srivastava, Dhar, & Singh, 2019). Med dessa uppenbara förväntningar och problem lämpar sig hälso- och sjukvården väl som ett fall i studien.

Exempelvis; En äldre person som bor hemma och använder sig av hemtjänst vill att hemtjänsten ska kunna bevaka dennes aktivitet, för att kunna hitta avvikelser och i så fall åka dit. Den äldre vill dock inte att hemtjänsten ska ha direkt tillgång till exempelvis kamera-feeds från hemmet eller realtidsdata från andra sensorer, eftersom det ses som integritetskränkande. Samtidigt är det lika viktigt att ingen kan ändra på den data som skickas från den äldre, då detta skulle kunna vara livsavgörande. Det blir i detta exempel även viktigt att kunna säkerställa att både den äldre och hemtjänsten kan bevisa äktheten av sin identitet.

3.2.5.3 Fall 3 – Digital röstning

När en population ska delta i ett offentligt val finns uppenbara krav på integritetsbevarande och säkerhet. Inte endast ska varje deltagande kunna veta att deras röst blivit inskickad korrekt, rösten ska dessutom vara anonym för alla övriga. För att detta ska säkerställas används i Sverige idag är ett system som till hög grad fungerar på grund av att många olika parter kontrollerar varje delsystem i den stora röstprocessen. Fallet syftar till att exemplifiera hur digitala tillvägagångssätt kan användas för att ersätta de kontrollmekanismer som används i Sverige idag, för att kunna möjliggöra tillgänglig, säker, transparent och integritetsbevarande röstning för en population.

Ett optimalt digitalt röstningssystem ska med matematiskt motiverade grunder säkerställa totalt integritetsbevarande för varje röstande person. Systemet blir tekniskt komplicerat och intuitivt abstrakt för den genomsnittliga röstaren. Därför är det viktigt att möjliggöra verifiering av att ens röst faktiskt räknades för varje enskild röstare. Annars riskerar ett system som detta att tappa tillit från allmänheten.

En viktig aspekt som måste beaktas är hur identiteten på den som lägger rösten ska säkerställas. I dagsläget kontrolleras denna av en fysisk person, via legitimation och röstkort (Valmyndigheten, 2020). En digital lösning skulle inte kunna ersätta den kontrollen, utan endast säkerställa att den röstandes digitala legitimation använts, till exempel med Bank-ID. Det är möjligt att någon har tillgång till flera Bank-ID samt tillhörande telefoner, alternativt tvingar andra att lägga sin röst på ett specifikt parti, antingen genom hot eller mutor. Detta är ett problem som fallet bortser ifrån,

antagandet är att den ökade tillgängligheten som digital röstning skulle medföra är en fördel som överväger nackdelarna.

3.3 Metoddiskussion

Risken med kedjesökning är att många liknande källor hittas då risken finns att många källor vidare till liknande källor. Detta kan leda till att utomstående perspektiv förloras och att läsaren kan fastna i en ”bubbla” av vilken information som tas in.

Källorna har valts utifrån dess användbarhet för studien. I syftet för att säkerställa källornas pålitlighet har flera källor använts, och deras innehåll har jämförts. Vid litteraturgenomgång har även informationens ursprung granskats, för att försöka säkerställa informationens legitimitet. Detta tillvägagångssätt minskar också risken för feltolkningar.

I en teoretisk litteraturstudie finns risken för att författarna bidrar med egen konfirmationsbias eftersom författarnas intresse kan styra vilken information används. Information som författarna anser ointressanta riskerar att bortses från i inläsningsprocessen, och därmed kan analysens bredd drabbas. I en så pass diversifierad författargrupp som denna anses inte risken vara överhängande.

4 Tidigare forskning på fallen

Det finns tidigare förslag på lösningar till exempelfallen och andra liknande scenarion. Analysen tar avstamp i ett urval av dessa, som presenteras nedan indelade efter fall.

4.1 Fall 1 – Nyckeltaljämförelse

Det har gjorts en del forskning på området kring konfidentiell nyckeltalsberäkning eller nyckeltalsjämförelse, och ett antal förslag till lösningar finns att tillgå i rapporter och projekt. Gemensamt för de lösningsförslag som finns tillgängliga är att de baseras på tekniken homomorfisk kryptering. En del skillnader mellan olika lösningar finns dock, vilket redovisas med sammanfattningar av tre olika studier och projekt här under.

4.1.1 Practical privacy-preserving benchmarking

Florian Kerschbaum (2008) gjorde ett, enligt honom själv, första försök i världen att ta fram ett konfidentiellt nyckeltalsjämförelsesystem. Detta protokoll tillåter bland annat jämförelse av medelvärden, varians och maximum och kan enligt Kerschbaum användas för att skapa en integritetsbevarande plattform för nyckeltalsjämförelse som beräknar statistik utifrån nyckeltal för medlemmarna.

Protokollet bygger på säker distribuerad beräkning (SDB), secure multi-party computation, vilket är en kryptografisk teknik som behandlar problemet att i grupp utföra beräkningar på uppdelad krypterad data. Varje part i gruppen har bara tillgång till en, för den enskilde parten, okänd del av den hela datan och utför beräkningar homomorfiskt på denna, för att senare tillsammans med hela gruppen ta del av resultatet.

Dessa distribuerade beräkningsprotokoll garanterar ett korrekt resultat och tillåter beräkningar av känslig data bland parter som ej litar på varandra (The GWG task team on privacy preservation techniques, 2019). Systemet kräver dock en betrodd tredje part (BTP), trusted third party, vid registrering som bland annat upprättar säkra kommunikationskanaler. All kommunikation sker via en central plattform där full anonymitet råder medlemmarna emellan. Något som medlemmarna dock kan se i denna lösning är hur många medlemmar som är med i gruppen. För att få bli medlem

i en grupp föreslås också att en ”myndighet för nyckeltalsjämförelse” ska utfärda en slags certifikat till dem som berättigas att vara med.

4.1.2 Compare confidential information while keeping it secret

I projektet COBE (confidential benchmarking) som är finansierat av danska institutet för vetenskap, teknik och innovation pågår forskning på hur konfidentiell nyckeltalsjämförelse kan genomföras med hjälp av SDB. Projektets mål är att leverera ett konfidentiellt verktyg för nyckeltalsjämförelse som ska kunna användas av industrier som vill jämföra sin energikonsumtion i syfte att effektivisera verksamheterna (The Alexandra Institute, 2020).

Prototyplösningar har redan testats inom olika scenarier såsom utvärdering av miljöpåverkan vid sjöfart och anges ha varit framgångsrika. Lösningen sägs vara av sådan karaktär att den klarar av mer avancerade och tyngre beräkningar än tidigare, men inga närmare förklaringar på hur protokollet är uppbyggt anges annat än att säker distribuerad beräkning och homomorphic encryption används.

4.1.3 Private collaborative business benchmarking in the cloud

Sobati-Moghadam & Fayoumi (2019) presenterar en integritetsbevarande prototyp av molnbaserad kollaborativ nyckeltalsjämförelse. I denna prototyp ingår gruppen av parter som vill jämföra sina nyckeltal med varandra, en molntjänsteleverantör (SP) där beräkningen utförs samt en betrodd server som spelar en roll i dekrypteringen av resultatet. Antaganden som är gjorda är att den betrodda servern ej uppsåtligt samarbetar med SP, och att alla inblandade parter är intresserade av att få ett korrekt resultat och därmed ger ifrån sig rätt data.

Prototypen erbjuder både anonymitet kring vilka de inblandade parterna är samt hur många de är till antalet och består av tre faser. Fas A där publika och privata nycklar genereras och distribueras till parterna, fas B där kryptering och sedan lagring hos SP sker och slutligen fas C där beräkning och dekryptering av datan sker. Beräkningen görs med hjälp av ett partial homomorphic encryption-schema och dekrypteringen görs utefter ett threshold group decryption-schema, vilket innebär att flera av deltagarna (åtminstone ett visst antal krävs) tillsammans dekrypterar datan.

Enligt författarna är deras prototyp säker mot passiva inkräktare (”tjuvlyssnare”), medan säkerheten behöver förbättras med autentiseringsmekanismer såsom meddelandeautentiseringskoder (MAK), message authentification codes, eller digitala signaturer för att även hindra aktiva inkräktare. MAK och digitala signaturer används för att autentisera att ett visst meddelande kommer från en viss person.

4.2 Fall 2 – Hemtjänst

Det finns ett antal olika tidigare konceptuella lösningar. Bland dessa använder ett flertal lokal beräkning, men andra lösningar i form av blockkedjor förekommer också.

4.2.1 A decentralized privacy-preserving healthcare blockchain for IoT sensors

Dwivedi et al. (2019) föreslår en blockkedje-lösning för leverans av hemvård. Deras koncept bygger på att kombinera decentraliseringen som blockkedjor möjliggör tillsammans med ringsignaturer för att försäkra sig om att patientens identitet förblir anonym och att data inte kan komprometteras. De menar vidare att oförmågan att kunna radera information i ett block ur en blockkedja förhindrar möjliga förändringar av data.

Tekniken bygger på att använda sig av smart contracts, en form av digitalt kontrakt som automatiserar kontraktets avtalade funktioner (Savelyev, 2017), för att skapa avtal mellan IoT-enheter. Dessa avtal kan exempelvis ha ett högsta och lägsta värde av blodtryck. Om dessa värden över- eller underskrids skickas en varning till vården och data sparas på blockkedjan (Dwivedi, Srivastava, Dhar, & Singh, 2019).

En av utmaningarna vid denna typ av lösning är att informationen som samlas in någon gång måste skickas till blockkedje-nätverket och under denna transmission riskeras data att komprometteras (Dwivedi, Srivastava, Dhar, & Singh, 2019).

4.2.2 An edge-based architecture to support efficient applications for healthcare industry

En lösning baserad på lokal beräkning föreslås av Pace et al. (2018) kallad Bodyedge. Deras idé bygger på en egenframtagen mjukvara till IoT-enheter och en egen lokal enhet. Tanken är att data samlas in från en sensor i en IoT-enhet för att sedan skickas till den lokala enheten. Alternativt samlas data in på samma sätt fast skickas sedan till

den lokala enheten via en reläpunkt (exempelvis en smartphone). Detta innebär att systemet har reducerade förseningar vid kommunikation. Vidare talar det också för en minskad bundenhet till bandbredd då enbart statistik behöver skickas från den lokala enheten. Bodyedge medför även ökade säkerhetsaspekter då enheten kan ses som ett privat moln (Pace, o.a., 2018).

I artikeln testas även lösningen utifrån flera olika parametrar. Bland annat presenterar de olika systemkrav på att läsa av fabriksarbetares puls jämfört med idrottares puls. Detta då de resulterar i olika belastningar på deras system. En Raspberry Pi3 kan exempelvis vara tillräckligt för att stöda avläsningen av 100 arbetare eller idrottare, fast med olika responstid (Pace, o.a., 2018).

Några av svårigheterna Pace et al. (2018) presenterar är kompabiliteten bland alla olika IoT enheter, då det finns en extrem variation av dessa och nya ständigt produceras. Fortsatt ser de även prioriteringen av olika hälsofall som ett problematiskt område.

4.2.3 Smart Homecare System for Health Tele-montoring

Leijdekkers, Gay & Lawrence (2007) presenterar i ett konferenspapper år 2007 en prototyp för hur patienters hälsa kan övervakas i deras hem och hur deras läkare kan ta del av informationen på avstånd. Prototypen involverar användandet av sensorer som samlar in information om patientens tillstånd, vilket sedan skickas till en smartphone i patientens ägo för att sedan synkas till vårdtjänstens server.

Lösningen inkluderar användandet av flera olika sorters sensorer för att möjliggöra identifiering av felaktiga varningssignaler, och tilldelar även patientens smartphone uppgiften att utföra enklare analyser av hälsodata, till exempel jämförande av blodtryck med ett förbestämt intervall. Prototyplösningen inkluderar även användandet av kameror i patientens hem för att verifiera nödsignaler från övervakningsutrustningen, samt för att möjliggöra direktkontakt med vårdtagaren genom ljud- och bildlänk.

Detta konferenspapper ger en inblick i en tidig prototyp på en helhetslösning för användning av digitala verktyg för vårdgivande i hemmet. Tekniken har utvecklats

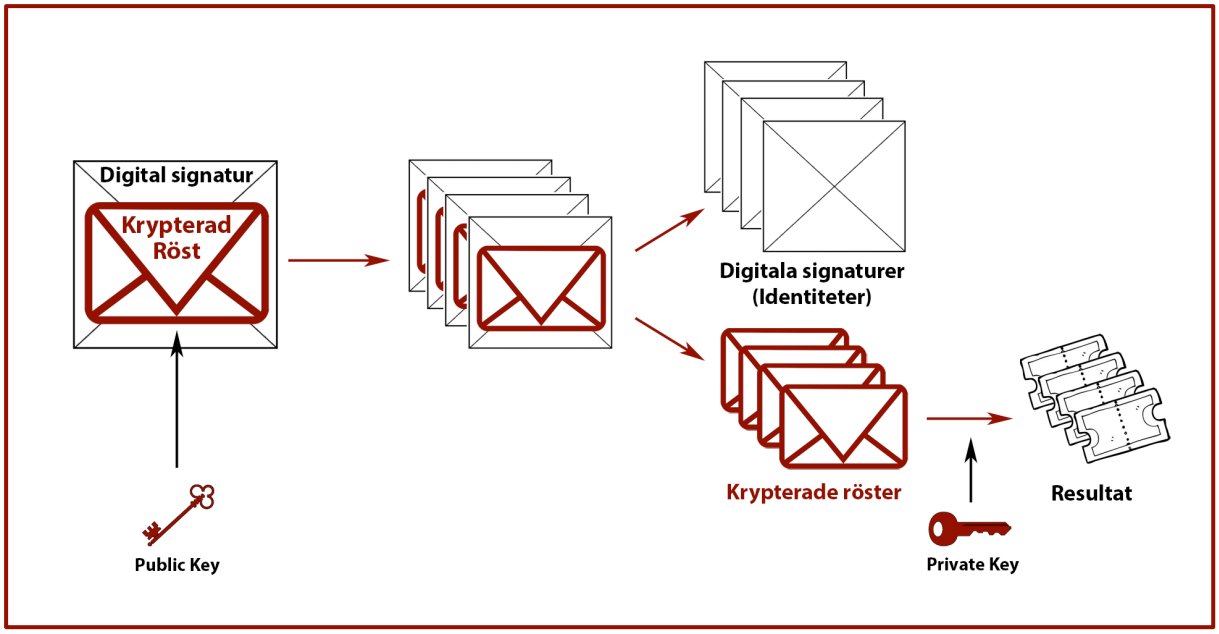
mycket sedan konferenspappret presenterades och möjligheten för att utföra ytterligare analyser i hemmet har ökat både vad gäller hårdvara och mjukvara. Konferenspappret lyfter inte säkerhetsaspekter mer än att videokameror inte ämnas användas mer än i nödfall eller vid på förhand avtalad tid. Lösningen bygger med andra ord på principen att all data delas mellan patient och vårdgivare, vilket öppnar upp för risker i form av dataläckor och missbruk.

4.3 Fall 3 – Digital röstning

Två tidigare projekt inom elektronisk röstning tas upp, Estlands redan implementerade system, samt en rapport med föreslagna metoder baserade på korta länkade ringsignaturer.

4.3.1 I-voting: Lessons from Estonia

Sedan 2005 har det varit möjligt att som estnisk medborgare rösta i nationella val digitalt. Systemet uppmuntras av E-Estonia med motiveringen att lösningen är en *”unik lösning som enkelt och bekvämt hjälper folket att engagera sig i den statliga styrningsprocessen”* (E-Estonia, u.d.). Medborgarna legitimerar sig med flerfaktorsautentisering och väljer en av möjliga kandidater att rösta på. Rösten krypteras och bifogas tillsammans med personens identitet, en digital signatur. Likt hur personen kopplas från röstkortets nummer i en verklig röstlokal separeras den digitala signaturen från den krypterade rösten, och endast den krypterade rösten skickas vidare till slutdestinationen. Valmyndigheten använder sin privata nyckel för att dekryptera rösten, och inkluderar den i rösträkningen (Tsahkna, 2013). Proceduren illustreras i figur 6.



Figur 7 - Estlands digitala röstningssystem (E-Estonia, u.d.)

4.3.2 Short Linkable Ring Signatures For E-Voting, E-cash and Attestation

Till skillnad från tidigare forskning på gruppsignaturer presenteras i denna rapport det första korta länkade ringsignaturschemat. Länkade ringsignaturer möjliggör verifiering av att två från ringen utfärdade signaturer inte har samma ursprung (Wei, Tsang, & Victor, 2004).

Simpla ringsignaturers nackdel är att de, eftersom de gömmer ursprungliga avsändaren i en grupp av möjliga avsändare, inte kan begränsa avsändare från att göra någonting upprepat. Det betyder att simpla ringsignaturer möjliggör för en medborgare att rösta helt anonymt, men det möjliggör även för medborgare att skicka in flera röster, och därmed beröva de andra ringmedlemmarna på sina röstmöjligheter.

5 Analys och diskussion av fallen

Analysen av fallen utförs genom en poängbedömning utifrån de fem faktorer som presenteras i tabell 1 nedan. De betygssätts på en skala från ett till fyra, där ett är svagt och fyra är starkt. Innebörden för betyg ett och fyra framgår i tabellen. Betyg två och tre utgör gradskillnader däremellan. Samma gradering används för att betygsätta den föreslagna lösningen, för att belysa de förbättringsområden och eventuella uppoffringar som förslaget innebär. Vid betygsättning utgås ifrån att lösningen är en fyra varpå poängavdrag görs vid identifierade svagheter under varje kriterie.

Kriterier	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Betyg 1	Lösningens implementerbarhet är ej bevisad	Tekniker och metoder saknar dokumentation	Det finns flera tydliga säkerhetsbrister	Det finns flera tydliga säkerhetsbrister	Lösningen saknar funktioner från specifikationen
Betyg 4	Lösningen kan implementeras i dagsläget	Alla tekniker och metoder är noggrant dokumenterade	Inga uppenbara säkerhetsbrister finns	Inga uppenbara säkerhetsbrister finns	Lösningen uppfyller fallbeskrivningens krav

Tabell 1 - Kriterier för jämförelse

Mognadsgrad är taget från det redan vedertagna begreppet *technology readiness level* vilket bedömer olika teknikers mognadsgrad. Dock har den niogradiga skalan komprimerats till en fyragradig. Transparens syftar till teknikens grad av dokumentation och hur tydlig den underliggande metoden klargörs. Konfidentialitet bedömer hur väl attackvektorerna mot systemet är hanterade. Hur väl de inblandade aktörernas integritet är skyddade i lösningen bedöms med kriteriet integritet. Funktion avser i vilken grad lösningen funktionsmässigt uppfyller de krav som skulle göra att den omnämnda lösningen skulle kunna klassas som säker.

5.1 Fall 1 – Nyckeltalsjämförelse

Utifrån presenterad forskning finns ett antal olika lösningar för att bibehålla konfidentialitet vid nyckeltalsjämförelse. Ingen av de enskilda lösningarna adresserar dock alla möjliga svagheter samtidigt utan fokuserar på olika aspekter. De teknikerna som föreslås blottlägger också olika delar av databehandlingen och dataöverföringen.

5.1.1 Practical privacy-preserving benchmarking

Lösningen finns endast på teoretisk nivå och förutsätter bland annat att någon form av myndighet för nyckeltalsjämförelse existerar. Den har heller aldrig testats praktiskt med deltagare även om protokollet presenteras i sin helhet.

Inblandning av en BTP försvagar alltid skyddet av både konfidentialitet och integitet för deltagarna. Dessutom har den i detta fallet tillgång till all data. I denna lösning är dessutom antalet gruppmedlemmar känt. Detta försämrar skyddet av integriteten ytterligare då förändringar i antalet medlemmar riskerar att avslöja enskildas data. I tabell 2 syns hur denna lösning på grund av dessa faktorer inte får ett högt betyg på varken konfidentialitet eller integritet.

Lösningens funktion är bra men jämförelserna är begränsade till ett antal matematiska beräkningar vilket innebär att den inte lämpar sig för alla områden.

Kriterier	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Poäng	2	4	2	2	3

Tabell 2 - Bedömning practical privacy-preserving benchmarking

5.1.2 Compare confidential information while keeping it secret

En prototyp med denna lösning har tagits fram och testats med framgång på ett enskilt fall. Protokollet är dock ej publikt vilket försvårar analys av de tekniska lösningarna och kan försämra förtroendet för produkten.

Utifrån den information som finns att tillgå om systemet så finns tekniska lösningar på plats för att hantera bevarande av konfidentialitet och integritet. En BTP är dock inblandad vilket återigen försämrar skyddet. Det framgår inte huruvida gruppstorleken är känd för övriga medlemmar men då det är det vanligaste utgår vi från att så är fallet även här.

Funktionaliteten sägs vara mycket bra och till skillnad från andra lösningar kan den hantera avancerade och prestandakrävande matematiska beräkningar. Dock är det utvecklat för en specifik bransch vilket gör att det är svårt att bedöma hur applicerbar

den är för mer generell nyckeltalsjämförelse. I tabell 3 syns en sammanställning av betygen lösningen får utifrån kriterierna.

Kriterier	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Poäng	3	1	3	2	3

Tabell 3 - Bedömning COBE-projektet

5.1.3 Private collaborative business benchmarking in the cloud

Lösningen presenteras som en teoretisk prototyp som ännu inte har testats med deltagare. Transparensen får anses mycket hög då protokollet presenteras i sin helhet och är publikt, dock utan detaljerad beskrivning.

I denna lösning finns det två BTPs men då informationen är uppdelad mellan de två så utgör de bara en mindre risk för konfidentialiteten detta fallet.

Funktionaliteten är mycket hög i denna lösning och har potential att tillämpas generellt för nyckeltalsjämförelse i olika brancher och för olika syften. I tabell 4 framgår hur lösningen betygssätts utifrån kriterierna.

Kriterier	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Poäng	1	3	3	4	4

Tabell 4 - Bedömning molnbaserad nyckeltalsjämförelse

5.1.4 Diskussion

De vanligaste lösningarna, som fortfarande dock bara är prototyper i försöksstadiet, bygger på säker distribuerad beräkning. Dessa lösningar erbjuder anonymitet åt parterna, men storleken på gruppen är för de inblandade känd. Ett problem med dessa prototyper är att det finns en risk att konfidentialiteten röjs utifrån analyser av resultaten. Med kännedom om antalet inblandade parter tillsammans med resultatet skulle det exempelvis över tid finnas möjlighet att ta reda på indatan för enskilda parter som tillkommer eller lämnar nyckeltalsjämförelsegruppen.

Ytterligare ett problem med denna lösning är att det blandas in en betrodd tredje part som sköter registrering av gruppmedlemmar samt upprättar och möjliggör anonym och säker kommunikation dem emellan. Detta leder alltså till ytterligare en attackvektor i systemet som något försämrar konfidentialiteten.

Ett annat alternativ som presenteras bygger istället på en molnbaserad plattform där homomorfisk kryptering utnyttjas. Vid denna lösning hålls antalet ingående parter hemligt vilket betyder att analyser på resultatet inte alls riskerar att röja konfidentialiteten för enskilda parter i samma utsträckning som om gruppantalet vore känt. Där föreslås också användning av en extern proxy-server för dekryptering av datan. Beräkningar skulle ske homomorfiskt på en extern server och därefter skickas resultaten krypterat till proxy-servern.

Innebörden av detta skulle vara att en enhet känner till antalet i gruppen, och en annan enhet resultatet från beräkningen. Detta är två delar information som tillsammans skulle ge samma möjlighet att röja konfidentialitet som i prototypen med SDB, något som de inte kan göra var och en för sig. Litteraturen gör antagandet att dessa enheter inte samarbetar, men det är dock en svaghet för konfidentialitetsbevarandet.

Denna beskrivna svaghet som i viss mån förekommer i samtliga av nämnda lösningar, där analyser på resultatet kan röja konfidentialiteten för deltagare, kan adresseras genom att det läggs på så kallat noise på indatan. Det leder till att vetskapen om hur många som är delaktiga i gruppen förlorar sitt värde, eftersom det beroende på hur mycket noise som läggs på blir svårare att räkna ut mätvärdet hos en part som lämnat eller tillkommit till gruppen mellan två beräkningar.

I förlängningen innebär det att den part som utför beräkningarna inte behöver betros med kompromettерande information, förutsatt att homomorfisk kryptering används. Detta ger en fördel eftersom systemet blir mindre sårbart. Det är dock viktigt att påpeka att ju mer noise som läggs på, desto mindre blir precisionen i resultatet. Kopplat till kriterierna leder alltså en ökning av noise till en lägre funktion men en högre konfidentialitet och vice versa.

Endast ett av de fallen som presenteras tar upp frågan kring hur det ska bevisas att en medlem är legitim och uppfyller kravspecifikationen på att få ingå i gruppen. I det fallet hanteras det genom att involvera en BTP vilket exponerar gruppen för större risker.

Ett alternativ till denna lösning är att hitta en teknik som inte kräver en tredje part. En kandidat till en sådan teknik skulle kunna vara nollkunkapsprotokoll, Zero Knowledge Proofs, där medlemmarna bevisar att de uppfyller kriterier för att få ingå i gruppen utan att avslöja vem man är.

Detta skulle alltså kriteriemässigt leda till betydligt bättre konfidentialitet och integritet. De praktiskt implementerbara användningsområdena för dessa protokoll har dock en otydlig teoretisk grund, framför allt när det gäller vilken typ av påståenden som kan bevisas.

Viss litteratur utgår från antagandet att dessa skulle kunna bevisa godtyckligt valda påståenden. En problematisk aspekt i detta antagande är dock att de fungerande bevis som finns på nollkunskapsprotokoll behandlar mycket specifika numeriska påståenden (exempelvis “Jag är 21 år gammal eller äldre.”), som konceptuellt är väldigt långt ifrån de omdiskuterade användningsområden som finns i litteraturen.

Mot bakgrund av detta bedöms forskningen på området inte är tillräckligt utvecklad för att möjliggöra till exempel nollkunskapsprotokoll för att bevisa tillhörighet till en fysisk grupp, och att tekniken för detta ändamål därför inte är särskilt mogen. Användandet av en BTP skulle alltså vara ett mer rimligt tillvägagångssätt. Likt hur Kerschbaum (2008) låter en betrodd part avgöra om aktörer är värdiga och ge ut certifikat behöver en BTP avgöra om aktören är välkommen att delta i nyckeltalsjämförelsen.

De ingående teknikerna homomorfisk kryptering och SDB är beräkningsmässigt kostsamma, vilket tills nyligen gjort de mindre praktiskt användbara. I COBE-projektet har man dock lyckats ta fram prototyplösningar där de visat att nyckeltalsjämförelseberäkningar kan användas och appliceras på praktiska fall, vilket ger den specifika lösningen en högre mognadsgrad.

5.2 Fall 2 - Hemtjänst

Det finns flera aspekter och möjliga attackvektorer som de presenterade tidigare lösningarna inte adresserar. Vissa av de tekniker som används är inte redo att användas i dagsläget och vissa leder eventuellt till en ökad osäkerhet. Problematiken kring validering av data som samlas in tas heller inte upp.

5.2.1 A decentralized privacy-preserving healthcare blockchain for IoT sensors

Den lösning som bäst tillfredsställer de krav som ställts är en lösning baserad på en decentraliserad blockkedja. Problemet med denna teoretiska lösning, likt många andra blockkedjelösningar, är att det saknas fungerande praktiska exempel som påvisar att detta kan implementeras. Även om det inte inte finns några praktiska implementeringar av den decentraliserade blockkedjan är protokollen och användandet av de olika teknikerna däremot väl beskrivna.

I och med oförmågan att ta bort data ur en blockkedja, uppstår även risken att all denna data kan exponeras och kopplas till en specifik identitet. Händer detta röjs inte bara data kopplad till framtida transaktioner med blockkedjan utan även all historiska data. Utöver detta måste dessutom den insamlade data skickas till blockkedjan vilket blir en ytterligare attackvektor. Detta leder till bedömningen i tabell 5.

Kriterier	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Poäng	1	4	3	2	4

Tabell 5 - Bedömning Decentraliserad blockkedja för IoT inom hälso- och sjukvård

5.2.2 An edge-based architecture to support efficient applications for healthcare industry

BodyEdge använder en dedikerad lokal enhet som kan ha ökad säkerhetskapacitet. Det är däremot orimligt att varje individuell enhet skulle kunna ta till samma säkerhetsåtgärder som en central databas. Detta skulle kunna göra intrång lättare att genomföra på enskilda personer, men mycket svårare att göra i stor skala. Detta är en följd av att den enskilda datainsamlaren får ansvaret att hålla datan säkert lagrad.

Både hårdvaran och mjukvaran som författarna bakom bodyedge tar fram är väl beskrivna i funktion och syfte, samt dess förutsättningar. Däremot finns det oklarheter

kring kompabiliteten bland deras mjukvara och olika IoT-enheter både i nuläget och för framtiden. Bodyedge har dessutom blivit testad med olika förutsättningar för att se hur pass väl den fungerar, vilket gör den relativt tekniskt mogen. Utifrån studiens fallbeskrivningen möjliggör bodyedge hemtjänst på distans, förutsatt att IoT-enheten är kompatibel. Utifrån dessa argument framgår betygen i tabell 6.

Kriterier	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Poäng	2	4	3	2	3

Tabell 6 - Bedömning BodyEdge

5.2.3 Smart homecare system for health tele-monitoring

Lösningen som presenteras av Leijdekkers, Gay, & Lawrence (2007) beskrivs tydligt och läsaren erhåller en klar bild av hur enheterna kopplas samman, samt av hur data samlas in och skickas. Att lösningen baseras på existerande tekniker såsom sensorer kopplade till en edge-enhet som synkroniserar mot en central enhet visar på lösningens implementerbarhet. Även om denna modell framstår som produktionsredo är den, i den form som presenteras i konferenspappret, endast en prototyp och har därmed ej påvisats fungera i praktiken. Utan en fungerande prototyp kan inte heller modellen anses ha en hög mognadsgrad.

Funktionaliteten framstår som lovande och författarna beskriver användarvänlighet som ett fokus. Det är dock oklart huruvida detta system verkligen kommer att vara applicerbart även för äldre patienter, eller patienter med funktionsnedsättning, då dessa kan ha svårare att ta till sig tekniken.

Modellen saknar även en grundlig utvärdering av systemets säkerhet. Den tidiga prototyplösningen förutsätter kompabilitet mellan systemets olika sensorer, kameror och aktörer utan att säkerhetsgranska dessa anslutningar, och gör genom rapporten ingen nödvändig kritisk säkerhetsgranskning som skulle krävas för att påvisa lösningens implementerbarhet ur denna synvinkel. Sammantaget leder detta till bedömningen i tabell 7.

Kriterier	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Poäng	3	3	2	1	3

Tabell 7 - Smart Homecare System for Health Tele-monitoring

5.2.4 Diskussion

Även om det redan finns ett antal implementeringar av blockkedjor inom andra fält, saknas det ett tydligt försök inom hälso- och sjukvården. Då denna teknik är väldigt avancerad är detta ingen lätt implementering. Till skillnad från blockkedjor är lokal beräkning en tekniskt sett mer simpel och lättförståelig lösning. Vidare beskriver de två artiklarna kring lokal beräkning mer tydligt hur den praktiska tillämpningen ska gå till, vilket talar för att de har en högre teknisk mognadsgrad. Om hälso- och sjukvårdspersonalen dessutom ska förstå systemet underlättas detta när lösningen är mer lättförståelig.

Utöver en blockkedjelösning finns det flera lösningar som bygger på lokal beräkning. Fördelen med detta är att rådatan stannar lokalt hos insamlaren istället för att delas med en tredje part, vilket därmed leder till att ansvaret att hålla datan säker stannar hos insamlaren. En eventuell attack mot den tredje parten exponerar alltså inte varje enskild användares data. Då endast den för vårdgivaren relevanta informationen delas medför detta även att ett intrång i en central databas ej blir lika skadligt, då mycket av den känsliga informationen aldrig lämnat patientens ägo.

Nackdelen som de lokala lösningarna medför är att även om patienten blir mer skyddad mot ett centralt intrång hos vårdgivaren eller tjänsteleverantören så kvarstår möjligheten för intrång i patientens privata enhet. En sådan enhet har ett mindre rigoröst säkerhetssystem och skulle kunna kompromettеras av till exempel ett digitalt virus. Risken för detta ökar dessutom markant när lösningen inte använder sig av en dedikerad edge-enhet, utan utav till exempel en mobiltelefon. Detta då en dedikerad edge-enhet kan ha ökad säkerhet då den är byggd för syftet, samt att den inte exponeras genom användning utanför syftet. Denna potentiellt lägre säkerhet medför även en större sårbarhet mot riktade attacker när man lagrar känslig data i en privat uppkopplad enhet.

Av största vikt vid denna typ av system är att patientens data inte heller missbrukas av de som tar del av informationen. Detta är svårt att säkerställa då en viss nivå av förtroende måste tillskrivas vårdgivaren, men detta perspektiv saknas i den beskrivna lösningen. Exempelvis presenteras möjligheten att upprätta videolänk med patienten i hemmet då en nödsituation uppstår. Det diskuteras dock inte hur det kan säkerställas att detta ej kan missbrukas. Se fallet om *Ring security systems* som beskrivs i inledningsavsnittet.

IT-infrastruktur är föränderlig, och att alla system utvecklas parallellt och av olika utvecklare. Detta innebär att även om en lösning som du utvecklat är säker idag, så kan den göras sårbar imorgon när en annan programvara eller tjänst du förlitar dig på uppdateras av andra utvecklare. Detta betyder att IT-säkerhet är ett löpande arbete, och att dilemmat är oundvikligt med internetuppkopplade mjukvarulösningar.

Vad gäller den övergripande funktionaliteten framstår en lokal lösning i kombination med en blockkedjelösning som den mest heltäckande lösningen. På detta vis kan fördelarna med att inte dela mer än de nödvändiga insikterna, tillsammans med att lagra denna data i en blockkedja. Detta bygger dock på att blockkedjelösningen fungerar enligt förhoppningarna. Detta bedöms i dagsläget inte vara nära produktionsstadiet, vilket kan göra en ren lokal lösning till en mer realistisk modell tills det att en blockkedjelösning ligger närmare i tiden.

5.3 Fall 3 – Digital röstning

Att skapa ett system för säker digital röstning är ingen lätt uppgift givet de höga kraven. De tidigare lösningarna har säkerhetsbrister, men kan också komplettera varandra tillsammans med ytterliggare tekniker för att skapa en säkrare lösning.

5.3.1 I-voting: Lessons from Estonia

Det röstningssystem som används i Litauen idag, I-voting, är fullt tekniskt moget, eftersom det redan idag är i rullning. De tekniska beskrivningar och specifikationer som finns lämnar dock en del tekniska detaljer obesvarade, vilket gör att systemets transparens brister något. Hela röstningsresultatet tillsammans med alla identiteter och krypterade röster går genom ett system vilket skapar enskilda kritiska attackvektorer. Detta gör systemet sårbart om en attack skulle ske, med tanke på en

nationell röstnings omfattning. En följd av att systemets transparens är låg är att röster kan återkopplas till enskilda personer om arbetet bakom kulisserna inte utförs som utlovat. Detta gör att deltagarnas integritet inte nödvändigtvis kan garanteras. Funktionen som I-voting erbjuder går att likställa med ett vanligt analogt röstningssystem, men det saknar möjligheten för enskilda röstare att spåra sin röst i efterhand vilket är viktigt för att erhålla tillit av folket. Betygssättningen framgår i tabell 8.

Kriterier	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Poäng	4	2	2	1	3

Tabell 8 - Bedömning I-voting

5.3.2 Short Linkable Ring Signatures For E-Voting, E-cash and Attestation

Användandet av länkade ringsignaturer är teoretiskt möjligt, men inga prototyper eller exempel finns för att visa detta i praktiken. Det gör det svårt att bedöma om en implementering är möjlig i framtiden, och i så fall när. Systemet är konstruerat med hög transparens, ingenting avses hållas hemligt. Det finns en tydlig specifikation med matematiska beskrivningar. Länkade ringsignaturer erbjuder också mycket god konfidentialitet och integritet, men är endast en del av lösningen på problemet som fallet beskriver, och kan inte ses som en helhetslösning. Systemet är en byggsten som gör det möjligt att gömma en individ utan att låta denne rösta flera gånger. Betygssättningen framgår i tabell 9.

Kriterier	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Poäng	2	4	4	4	1

Tabell 9 - Bedömning Short linkable ring signatures

5.3.3 Diskussion

Eftersom röstning är en central del i den demokratiska processen är det viktigt att system som implementeras är pålitliga och transparenta. Estland är ett av de första länder att implementera ett digitalt röstningssystem, men det innefattar ett flertal brister. Spårbarhet av rösterna är något som inte är möjligt i Estlands nuvarande röstningssystem men som kan anses viktigt för tilliten av systemet. Om transparens är

bristande är det svårt att bedöma graden av integritet och konfidentialitet i praktiken eftersom man inte kan säkerställa att systemet beter sig som det utger sig för att göra. Därför kan transparens väga tyngre i praktiken än övriga kriterier, eftersom det är en förutsättning för att övriga kriterier ska kunna bedömmas korrekt.

De tekniska beskrivningarna för I-voting visar uppenbara säkerhetsbrister på grund av att protokollen är av typen closed source, och därmed att de publika beskrivningar som finns inte noggrant förklarar hur den tekniska lösningen faktiskt fungerar. Den största osäkerheten är steget där identiteten separeras från den krypterade rösten. Den litteratur som finns beskriver endast att rösten vidarebefordras i processen och att personligheten slängs, utan en teknisk beskrivning på hur. Detta gör det omöjligt för den röstande befolkningen att säkerställa att detta faktiskt genomförs, eller att det görs korrekt. Det är också omöjligt att kontrollera att den enskilde individens röst blev räknad.

Ett problem med den befintliga litteraturen är att den inte tar hänsyn till rösternas spårbarhet. I I-voting används public key cryptography, vilket gör det omöjligt att avläsa rösternas innehåll när de lämnat röstaren.

En variant av återidentifikation av data skulle kunna användas för att låta den som röstat säkerställa i efterhand att rösten räknats. Detta skulle fungera genom att en identifierare som är unik för varje röstberättigad person, och som endast är känd för den individ identifieraren tillhör, associeras med individens röst. När rösterna sedan räknats anonymt kan en lista med alla röster och deras unika identifierare publiceras. En individ kan då kontrollera att den röst som är associerad med dennes unika identifierare verkligen var den röst som lades. Publicering av anonyma röster möjliggör också en kontroll av huruvida ytterligare röster har lagts till i efterhand, eftersom det totala antalet röstberättigade är känt på förhand. Detta tillåter en rimlighetsanalys av röstlängden. Eftersom varje röst är associerad med en identifierare går det inte heller att byta ut röster utan riskera att detta upptäcks.

Att Estland använder sig av ett centraliserat system har flera nackdelar, då en attack mot den centrala aktören kan få stora konsekvenser. Detta gäller både digitala och fysiska intrång, samt missbruk av förtroende och misstag av de ansvariga. Dessutom

implicerar detta att en privat nyckel dekrypterar alla inskickade röster. Även detta utgör en stor sårbarhet, och är således en attackvektor.

Multifaktorautentisering är en väl beprövad metod, och den metod vi anser lämpar sig bäst för att säkerställa att rätt person ligger bakom en registrerad röst. Denna metod kräver att det finns en BTP som sparar autentiseringsdata i syftet att verifiera röstaren. Detta kan bli ett problem i länder som saknar digital infrastruktur motsvarande svenskt BankID och svenska bankdosor. Om inte denna infrastruktur finns, och autentiseringen kan förfalskas skulle det vara möjligt att skicka röster i någon annans namn.

Linkable ring signatures löser inte detta problem då tekniken endast säkerställer att en röst kan läggas utav varje registrerad individ, samtidigt som individens identitet hålls dold bland ringens medlemmar. Autentiseringen är ett tidigare steg i processen som måste vara säker med avseende på konfidentialitet och integritet för att ringsignaturen ska vara användbar.

Linkable ring signatures är ett bra sätt att säkerställa att identiteter hålls gömda bland en kvalificerad grupp. Detta gör den till ett passande alternativ för ett digitalt röstningssystem där individerna ska kunna säkerställas som röstberättigade samtididgt som deras identiteter ska hållas gömda i själva röstningsprocessen. Möjligheten att verifiera en rösts ursprung till en grupp ringmedlemmar är ett integritetsbevarande sätt att säkerställa att rösten kommer från en röstberättigad person.

6 Resultat av studien

Utifrån analysen kan en sammanfattad föreslagen lösning som är bättre ur konfidentialitets- och integritetssynpunkt tas fram för varje enskilt fall.

6.1 Fall 1 – Nyckeltalsjämförelse

I analysen av tidigare förskningen framgår att prototypen av Sobati-Moghadam & Fayoumi (2019) är den som bäst uppfyller de uppställda kriterierna. Med de tekniker som rapporten har behandlat finns heller inga tydliga möjligheter till förbättringar.

Att uppnå fullständig konfidentialitet förefaller med befintliga tekniker vara mycket svårt, och det gäller att göra avvägningar beroende på vilket specifikt problem man vill lösa. Framförallt handlar avvägningarna kring om nyckeltalsberäkningen ska göras tillsammans i grupp med tekniken SDB, vilket röjer gruppstorleken, eller om homomorfisk kryptering ska användas, vilket introducerar en något större risk i form av en BTP.

Mot bakgrund av detta lämnas inget förslag på lösning för detta fall utan istället fastslås att Sobati-Moghadam & Fayoumis lösning är den bästa som med de tekniker som har behandlats i denna rapport kan uppnås vilket framgår i tabell 10.

Lösning	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Kerschbaum	2	4	2	2	3
COBE	3	1	3	2	3
S-M & F	1	3	3	4	4

Tabell 10 - Sammanställning nyckeltalsjämförelse

6.2 Fall 2 – Hemtjänst

Den föreslagna lösningen är en kombination av lokal beräkning och smarta kontrakt, vilket inte de funna tidigare praktiska implementeringarna använt. I och med detta bör föreslaget få låg poäng under kriteriet mognadsgrad.

Eftersom den föreslagna lösningen använder sig av smarta kontrakt kommer enbart vissa data sparas, exempelvis data kring när ett blodtryck överskridit ett värde. Till följd av detta kommer en attack enbart att kunna komma åt blodtrycksdatan och inte annan data. På så vis bör användarnas integritet bevaras.

Vi föreslår en lösning som kombinerar lokal beräkning med smarta kontrakt då detta ger störst möjlighet att säkerställa datans konfidentialitet. Detta medför att patienterna endast delar de insikter om sitt hälsotillstånd som är nödvändiga för att vårdgivaren ska kunna leverera sina tjänster. På så vis minimeras risken för både missbruk och läckor av känslig data. Vi bedömer fördelarna som erhålls av lokal beräkning som större än nackdelarna, jämfört med centraliserad lagring av data.

Vi föreslår att man använder sig av en dedikerad, syftesbygd, enhet för lagring och beräkningar av den känsliga datan, då detta är den säkraste möjliga lösningen för lokal beräkning.

Funktionellt bör denna lösning kunna vara allmänt tillämpbar för leverans av hälsoövervakning i hemmet. Samma problem som diskuterades i avsnitt 5.2.4 angående lättanvändning kan dock uppstå, men detta handlar i stort om design av användargränssnitt, snarare än om lösningen i sig.

Det finns en avvägning mellan funktionalitet och konfidentialitet då tillräckligt mycket data måste skickas för att vårdtjänsten ska kunna levereras, men det måste samtidigt säkerställas att ingen kritisk information om patientens hälsotillstånd inte når läkaren. Hur detta kalibreras avgörs av hur implementationen av denna lösning görs, men denna problematiken orsakar att full konfidentialitet och full funktion ej kan uppnås i samma lösning. En sammanfattad betygsättning framgår i tabell 11.

Lösning	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
Blockkedja	1	4	3	2	4
BodyEdge	3	4	3	2	3
Smart Homecare	2	3	2	1	3
Förslag	2	4	4	3	3

Tabell 11 – Sammanställning hemtjänst

6.3 Fall 3 – Digital röstning

Följande föreslagna lösning är inte praktiskt implementerad och testad, vilket minskar dess bedömda mognadsgrad.

En central myndighet kan med fördel användas för att säkerställa att alla deltagare är röstberättigade. Att ersätta denna funktion med en digital motsvarighet är inte ett alternativ enligt litteraturstudie och analys. Denna myndighet måste arbeta transparent för att erhålla tillit från befolkningen. Hela systemet ska dokumenteras för alla att ta del av för att övertyga befolkningen om att valet sker på ett säkert sätt.

Användning av public key cryptography med ett stort antal krypteringsnycklar minskar konsekvenserna av att en nyckel skulle hamna i fel händer, och förbättrar därmed konfidentialiteten. Multifaktorautentisering bör även användas.

Genom att använda länkade ringsignaturer med mindre gruppstorlekar kan man dölja ursprungsröstarnas identitet, samtidigt som de kan konstateras legitima. Detta är en klar förbättring av integriteten, eftersom den med tekniska resonemang kan säkerställas.

Återidentifikation av data kommer möjliggöra spårning av röster i efterhand, vilket möjliggör verifikation av att valet gick rätt till i efterhand. Detta ökar funktionaliteten eftersom systemet blir enklare att lita på för medborgare.

En sammanfattad betygsättning framgår i tabell 12.

Lösning	**Mognadsgrad**	**Transparens**	**Konfidentialitet**	**Integritet**	**Funktion**
I-voting	4	2	2	1	3
Ringsign	2	4	4	4	1
Förslag	3	4	3	4	3

Tabell 12 – Sammanställning digital röstning

7 Slutsats

En naturlig och oundviklig följd av den fortsatta digitaliseringen i samhället är att frekvensen och omfattningen på datautbyten växer. Denna tillväxt innebär ett ökat antal attackvektorer, och därmed medför den ett större behov för säkra datautbyten och användning av säkra tekniker.

I analysen av tre skilda fall har det tydligt framkommit att användningen av säkra tekniker för att bevara konfidentialitet och integritet kräver ett omfattande arbete för att helhetslösningen ska kunna anses säker. Detta säkerhetsarbete är avgörande för att de inblandade aktörerna ska kunna delta, och för att de ska kunna lita på övriga inblandade aktörer.

Studien visar att det inte finns några universallösningar som leder till säkerhet i alla datautbyten, och därmed måste varje säkerhetslösning anpassas efter den unika situationen. En övergripande slutsats från studien är alltså att alla säkerhetssystem måste vara situationsanpassade. Dessutom framgår det att mindre delad data innebär mindre riskerad data, och därför är studiens andra övergripande slutsats att datadelningen bör minimeras ur säkerhetssynpunkt.

I dagens digitala tjänster förekommer ett flertal säkerhetsbrister, och beroende på vilken säkerhetsaspekt som prioriteras och vilka uppoffringar man är redo att göra innebär lösningen implementation av olika tekniker. Exempel på några av dessa har redogjorts för i denna rapport, och resultatet indikerar att fortsatt forskning på och utveckling av tekniker som tillåter säker distribuering av data är viktigt för att vi ska nå en uppkopplad och avancerad framtid utan att göra avkall på befolkningens rätt till integritet.

8 Hållbarhetsperspektiv

Världens ledare har enats omkring 17 globala mål för hållbar utveckling som ska uppnås till 2030 (United Nations Development Programme, 2020). Dessa mål handlar om både miljö och sociala aspekter och är därmed relevanta för alla typer av projekt oavsett ämne. Då rapporten utreder säkra digitala informationsöverföringar ligger tyngdpunkten på de sociala aspekterna och berör inte miljöfrågor.

Något som saknas bland de globala målen är dock människors rätt till att skydda sin personliga integritet vilket i allra högsta grad är en social aspekt. I allt mer digitaliserade samhällen försvåras människors möjlighet att själva ha kontroll över sina egna data vilket blottar dem för integritetskränkande aktiviteter. Dokument som tidigare låg i en skrivbordslåda eller inlåst ligger numer på en hårddisk som är uppkopplad mot internet. För att säkerställa att data är säker hos den enskilda och vid överföringar krävs nya tekniska lösningar på området.

Denna aspekt anser rapportens författare är något som borde integreras i de globala målen i framtiden. Vidare finns ett antal sociala aspekter för hållbar utveckling med i målen och fem av dessa har valts ut för att de på något vis berör de tre fall som har valts för att åskådliggöra problematik med dataöverföringar. Dessa fem mål eller delmål diskuteras nedan kopplat till fallen som de berör. Diskussionen fokuserar på hur de olika lösningarna kan möjliggöra att målen uppnås.

8.1 Fall 1 – Nyckeltalsjämförelse

Delmål 8.2 syftar till att *"Främja ekonomisk produktivitet genom diversifiering, teknisk innovation och uppgradering"*. Detta mål kan möjliggöras i fallet nyckeltalsjämförelse då den tekniska innovationen eller uppgraderingen är att kunna genomföra konfidentiell nyckeltalsjämförelse. Hela syftet med nyckeltalsjämförelse är att företag eller andra aktörer utifrån jämförande ska kunna identifiera förbättringsmöjligheter i verksamheten och på så vis öka sin ekonomiska produktivitet. I dagsläget hämmas denna möjlighet av brist på lösningar som säkerställer att de involverade parterna själva kan vara anonyma och de nyckeltal de bidrar med. Konfidentiell nyckeltalsjämförelse har också potential att möjliggöra partnerskap mellan offentliga och privata sektorn då det förekommer branscher där

de båda agerar. Delmål 17.17 syftar till att *”Uppmuntra och främja effektiva offentliga och offentlig-privata partnerskap samt partnerskap inom det civila samhället vilka bygger på erfarenheterna från andra partnerskap och deras finansieringsstrategier”*, vilket rimmar väl med vad det skulle kunna bidra med.

8.2 Fall 2 – Hemtjänst

Delmål 3.4 stipulerar *”Minska antalet dödsfall till följd av icke smittsamma sjukdomar och främja mental hälsa”*. Den första delen av detta mål berörs på så vis att det förekommer dödsfall till följd av exempelvis hjärtfel som potentiellt hade kunnat undvikas vid konstant övervakning av en persons medicinska värden. En sådan övervakning kommer i dagsläget med ett stort inkräktande i en persons privatliv vilket kan tänkas påverka patienter att välja bort en sådan lösning. En teknisk lösning som möjliggör övervakande av en patient i hemmet utan denna negativa bieffekt skulle kunna få fler att överväga den och på så vis minska dödsfall. Effekten av rapporten hade således kunnat hjälpa till att nå detta mål.

8.3 Fall 3 - Digital röstning

Att varje medborgare får möjligheten att påverka samhället den lever i är en grundpelare till att ett demokratiskt samhälle ska fungera. Att minoritetsgruppers röster väger lika tungt som övrigas, samt att alla oavsett utbildningsnivå eller geografisk lokalisering får delta på samma villkor bidrar till att ett land känner enighet och gemenskap trots de inbördes skillnader som finns. Delmål 10.2 syftar till att *“[…] möjliggöra och verka för att alla människor, oavsett ålder, kön, funktionsnedsättning, […], blir inkluderade i det sociala, ekonomiska och politiska livet”*. Delmål 16.7 syftar till att *“Säkerställa ett lyhört, inkluderande, deltagandebaserat och representativt beslutsfattande på alla nivåer”*.

Projektet har ett effektmål att bidra till högre integritetsbevarande och medverkande i till exempel röstningsprocesser, och hjälper därför till att möjliggöra att alla, oavsett grupptillhörighet, blir inkluderade och rättvist representerade i ett demokratiskt val. Det leder även till ett mer lyhört och inkluderande beslutsfattande genom ökad transparens. En digital röstningslösning skulle, om den implementeras lyckat, leda till

att fler fick möjlighet att delta i valen samt säkerställa att resultatet inte manipuleras på de platser där noggrann valövervakning inte sker idag.

Referenser

Delfs, H., & Knebl, H. (2007). *Introduction to cryptography: Principles and applications*. Springer Science.

Gilbert, S., & Lynch, N. (2002). Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. *ACM SIGACT News*, pp 51-59.

University of Minnesota. (u.d.). Hämtat från https://www.lib.umn.edu/datamanagement/whatdata

Internetstifltelsen. (2019). *Svenskarna och internet*.

Hedin, A. (2011). Hämtat från Liten lathund om kvalitativ metod med tonvikt på intervju: https://studentportalen.uu.se/uusp-filearea-tool/download.action/nodeId/459535/toolAttachmentId/108197&usg=AOvVaw2yDelaH-c6IKFlVVw_YXAC

Ejvegård, R. (2003). *Vetenskaplig metod*. Lund: Studentlitteratur.

Valmyndigheten. (den 20 Feb 2020). *Valmyndigheten*. Hämtat från Rösta i din vallokal på valdagen: https://www.val.se/att-rosta/var-rostar-jag/rosta-pa-valdagen-i-din-vallokal.html

E-Estonia. (u.d.). *E-Governance*. Hämtat från i-Voting - E-estonia: https://e-estonia.com/solutions/e-governance/i-voting/

Tsahkna, A.-G. (2013). E-voting: lessons from Estonia. *European View*. Hämtat från https://journals.sagepub.com/doi/pdf/10.1007/s12290-013-0261-7

Tynan, D. (den 19 Augusti 2019). *HealthTech*. Hämtat från Healthtechmagazine: https://healthtechmagazine.net/article/2019/08/will-edge-computing-transform-healthcare

Yli-Huumo, J., Ko, D., Choi, S., & Sooyong Park, K. S. (2016). Where is current research on blockchain technology? *PLOS One*.

Datainspektionen. (u.d.). *GDPR*. Hämtat från Datainspektionen: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/

National research council. (1994). *Academic careers for experimental computer scientists and engineers*. Washington: The national academic press.

Davis, G. (den 2 Januari 2018). *Mcafee*. Hämtat från Mcafee.com: https://www.mcafee.com/blogs/consumer/key-findings-from-our-survey-on-identity-theft-family-safety-and-home-network-security/

Cimpanu, C. (den 10 February 2020). *Software error exposes the ID numbers for 1.26 million Danish citizens*. Hämtat från ZDNet:

https://www.zdnet.com/article/software-error-exposes-the-id-numbers-for-1-26-million-danish-citizens/

Bashir, I. (2018). *Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition*. Packt Publishing Ltd.

Cao, J., Zhang, Q., & Shi, W. (2018). *Edge computing: A primer*. Cham: Springer.

Toyota. (den 10 Augusti 2017). *Industry leaders to form consortium for network and computing infrastructure of automotive big data*. Hämtat från Toyota website: https://global.toyota/en/detail/18135029/

Buschmann, J. (2004). *Introduction to cryptography*. New York: Springer Science+business media.

Chapple, M. (den 18:de April 2019). *Fact or fallacy: Is edge computing poised to disrupt healthcare?* Hämtat från healthtechmagazine.net: https://healthtechmagazine.net/article/2019/04/fact-or-fallacy-edge-computing-poised-disrupt-healthcare

Cox, J. (den 8 January 2020). *Ring fired employees for watching customer videos*. Hämtat från Vice: https://www.vice.com/en_us/article/y3mdvk/ring-fired-employees-abusing-video-data

Dasgupta, D., Roy, A., & Nag, A. (2017). Multi-factor authentication. i *Advances in user authentication* (ss. 185-233). Springer.

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors*, Volume 19.

Fan, J., & Vercauteren, F. (2012). *Somewhat practical fully homomorphic encryption*. Citeseer.

Frostling-Henningsson, M. (2017). *Kvalitativa metoder*. Lund: Studentlitteratur AB.

Gentry, C. (2009). *Fully homomorphic encryption scheme using ideal lattices*. ACM.

Gilbert, S., & Lynch, N. A. (2012). Perspectives on the CAP theorem. *Computer*, 30-36.

Goldreich, O. (2004). *Foundations of cryptography: basic techniques*. Cambridge University Press.

Hamilton, E. (den 27 December 2018). *What is edge computing: The network edge explained*. Hämtat från Cloudwards web site: https://www.cloudwards.net/what-is-edge-computing/

Kerschbaum, F. (2008). Practical privacy-preserving benchmarking. *IFIP international federation for information processing, Volume 278; Proceedings of the IFIP TC 11 23rd International Information Security Conference*, 17-31.

Kesan, J. P., Majuca, R. P., & Yurcik, W. J. (2004). *The economic case for cyberinsurance*. Chicago: University of Illinois. Hämtat från http://law.bepress.com/uiuclwps/art2

Leijdekkers, P., Gay, V., & Lawrence, E. (2007). *Smart homecare system for health tele-monitoring*. Sydney: Faculty of IT, University of Technology Sydney.

Pace, P., Aloi, G., Raffaele, G., Calicuri, G., Fortino, G., & Liotta, A. (2018). An edge-based architecture to support efficient applications for healthCare industry 4.0. *IEEE Transaction on Industrial Informatics*, 481-489.

Rivest, R. L., Shamir, A., & Tauman, Y. (2001). How to leak a secret. *International Conference on the Theory and Application of Cryptology and Information Security* (ss. 552-565). ASIACRYPT.

Savelyev, A. (2017). Contract law 2.0: "'Smart" contracts as the beginning of the end of classic contract law. *Information & communications technology law*, 116-134.

Sobati-Moghadam, S., & Fayoumi, A. (2019). Private collaborative business benchmarking in the cloud. *Intelligent computing*, 1359-1365.

Trochim, W. M. (den 22 Jan 2020). *Deduction & induction*. Hämtat från Research methods knowledge base: https://socialresearchmethods.net/kb/deduction-and-induction/

Wei, P., Tsang, P., & Victor, K. (2004). *Short linkable ring signatures for e-Voting, e-cash and attestation**. Hämtat från https://eprint.iacr.org/2004/281.pdf

Witte, J. H. (den 6 December 2016). The blockchain: a gentle four page introduction. Ithaka, New York, United States: Cornell University.

MyData. (den 05 05 2020). *MyData 101*. Hämtat från https://mydata.org/mydata-101/

ESSIF. (den 05 05 2020). Hämtat från About ESSIF: https://essif-lab.eu/

United Nations Development Programme. (den 12 March 2020). Hämtat från https://www.globalamalen.se/om-globala-malen/

Johnson, R. (den 17 August 2016). *Greenwich Associates*. Hämtat från Greenwich: https://www.greenwich.com/fixed-income-fx-cmds/securing-blockchain

The GWG task team on privacy preservation techniques. (den 1 August 2019). UN handbook on privacy-preserving computation techniques.

The Alexandra Institute. (den 2 March 2020). *Compare confidential information while keeping it secret!* Hämtat från https://alexandra.dk/uk/cases/cobe-confidential-benchmarking

INSTITUTIONEN FÖR TEKNIKENS EKONOMI OCH ORGANISATION

CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige 2020
www.chalmers.se

CHALMERS