Examensarbete

HÖGSKOLAN I SKÖVDE

Komfort Kontra Integritet:

Strukturerade litteraturstudier av IoT-enheter i hemmet

Comfort Versus Privacy:

Systematic reviews of IoT-devices in home environments

Examensarbete för kandidatexamen med huvudområdet informationsteknologi

Grundnivå 30 högskolepoäng

Vårtermin 2024

Studenter: Gustav Karlsson & Tobias Jacobsson

Handledare: Johan Zaxmy

Examinator: Thomas Fischer

Erkännanden

Vi vill uttrycka tacksamhet till handledaren Johan Zaxmy för det stöd som byggde grunden till detta arbete. Vidare vill vi tacka examinator Thomas Fischer för värdefull respons under arbetets gång och under opponering. Till sist vill vi även tacka David Halén, Filip Olsson och Rasmus Jonsson för att de tagit sig tid att läsa arbetet och gett värdefulla insikter till förbättring.

Sammanfattning

IoT-enheter inom hemmet blir allt vanligare och oron för hur användares integritet påverkas ökar i takt med att dessa enheter implementeras. Dessa enheter kan styras i hemmet eller på distans via tillhörande applikationer och har möjlighet att bidra med automatiserade funktioner och underhållning i en hemmiljö. Allt eftersom mer teknik implementeras i hemmet som kopplas upp mot internet kan detta utgöra risker för privatpersoners integritet. Detta arbete utförs i två separata strukturerade litteraturstudier. Den ena undersöker vilken typ av personuppgifter som kan komma att hämtas in av IoT-enheter i ett hem och den andra fokuserar på privatpersoners medvetenhet och inställning till insamlingen av dessa enheter. Båda studier använder sig av kvalitativa metoder för att undersöka respektive ämne för att nå en kombinerad slutsats om vilka personuppgifter som samlas in av IoT-enheter och privatpersoners medvetenhet om insamlingen.

Nyckelord: Internet of Things, IoT, Integritet, Datainsamling, Integritetsförlust, Medvetenhet, IoT-enheter inom hemmet

Abstract

Home IoT-devices are becoming more commonplace, and the concern about what this implies for users' privacy rises along with it. These devices can be managed locally, within the home, or remotely, with their companion apps, in order to enable automated functions and entertainment. As more technical devices are implemented with connection to the internet, more risks occur regarding the privacy of the user. This paper consists of two systematic reviews, where the first one focuses on what personal information is being collected by in-home IoT-devices. The second systematic review focuses on the individuals' awareness and attitude towards the collection of personal information by these devices. Both systematic reviews use a shared method that qualitatively investigates the data collected in order to reach a combined conclusion regarding what personal data is collected, and how aware users are about this collection.

Keywords: Internet of Things, IoT, Privacy, Data collection, Privacy loss, Awareness, Smart home

Innehållsförteckning

1 Introduktion

I det moderna hemmet blir det allt vanligare att enheter med benämning Internet of Things används i vardagen. Internet of Things- eller IoT-enheter består av enheter som via fjärrstyrning och molntjänster kontrolleras av en användare för specifika syften. Exempel på dessa enheter inkluderar luftkonditionering, smartklockor och röstassistenter. Enheterna kopplas upp till användarens lokala nätverk för att kunna kommunicera med andra enheter i hemmet, samt mot internet för att externt kunna hämta data och styras av användaren oavsett position. Exempelvis tillåter detta hemmets medlemmar möjligheten att öka värmen i hemmet via sin mobiltelefon innan deras arbetsdag är slut. Detta ökar användarens komfort i hemmet med hjälp av fjärrstyrda verktyg.

Tjänsterna som erbjuds involverar dock att användaren identifierar sig själv med ett konto som autentiserar användaren. Detta konto kan innehålla personuppgifter som användaren själv värnar om. Utöver detta hämtas även data in från användaren med hjälp av de IoT-enheter som existerar i hemmet. Exempel inkluderar enhetens position, information om övriga enheter inom nätverket och ljud upptaget från ständigt påslagna mikrofoner.

Detta bidrar till att IoT-enheter och deras funktion i hemmet snabbt kan bli en fråga om personlig integritet. Teknisk kunskap och utbildning kan avgöra om det blir svårt för användaren att förstå och vara medveten om vilka personuppgifter som samlas in om användaren. I detta arbete har två separata strukturerade litteraturstudier utförts där den första fokuserar på vilken data som IoT-enheter hämtar in om användaren, medan den andra utforskar hur medvetna användarna är om datainsamlingen.

2 Bakgrund

Syftet med följande kapitel är att beskriva de definitioner och termer som är förknippade med IoT-enheter för att förklara hur dessa fungerar i praktiken, samt definiera viktiga processer och termer relaterade till informationssäkerhet och insamling av personuppgifter.

2.1 Internet of Things

Dorsemaine et al. (2015) definierar Internet of Things (IoT) som grupper av infrastrukturer med objekt som är sammanlänkade vilket tillåter dem att styras och ha tillgång till den data de genererar. IoT används därmed som ett samlingsbegrepp för olika typer av hårdvara som är sammankopplade i ett nätverk och kopplas upp mot internet för att bidra med olika typer av tjänster till både individer och företag. IoT kan användas inom exempelvis industri, handel och sjukvård. Detta arbete fokuserar på IoT-enheter i privatpersoners hem, för att erbjuda olika möjligheter som bland annat fjärrstyrning, automatisering och mätning.

2.1.1 IoT inom hemmet

Smarta ekosystem har blivit allt vanligare i moderna hem. Kända varumärken som levererar dessa system inkluderar Google, Amazon och Apple. Även om konsumenten köper sig in i ett specifikt märke betyder detta nödvändigtvis inte att alla kompatibla enheter måste komma från samma leverantör. Googles utvecklingssida för Home-produkter (u. å) erbjuder instruktioner för leverantörer som önskar att låta sina enheter styras med hjälp av Google Home. Detta involverar en process där enhetens funktioner först skall testas internt och mot Googles tjänster. Lösningen skickas sedan in till Google för certifiering varpå tjänsterna kan erbjudas till kunder. Denna lösning är dock beroende av att enhetstillverkaren erbjuder ett separat kontosystem som sedan länkas till användarens Google-konto för att autentisera användaren till både Googles och enhetstillverkarens tjänster.

IoT-enheter styrs vanligtvis via applikationer på en mobil enhet som exempelvis en mobiltelefon eller surfplatta, för att låta användaren interagera med sina enheter. I vissa fall har kunden möjlighet att styra enheter från olika märken via en central applikation som exempelvis Google Home, förutsatt att leverantören erbjuder tjänsternas konton att länkas mellan varandras infrastrukturer. Ferraris et al (2020) skriver att IoT-lösningar som erbjuds av Amazon (Alexa), Google (Home) och Philips (Hue) kräver tre separata konton för att ge användaren kontroll över sina enheter. Vidare poängteras det att eftersom användning av IoT-enheter i hemmet ökar, kan detta innebära att ytterligare konton behöver skapas för att kontrollera andra enheter som införskaffas till hemmet.

Då IoT-enheter existerar för att förse kunder med specifika tjänster är hårdvarans design, för det mesta, simpel, med billiga komponenter som utvecklas för att vara energisnåla och utföra de beräkningar som tjänsten kräver.

IoT-enheter i hemmet är inte immuna mot potentiella säkerhetshål som uppdagas på grund av uteblivna uppdateringar. Acar et al. (2024) skriver att uppdateringar för produkter som använder Android och kommer från Google kan ha en snabbare uppdateringsprocess eftersom uppdateringar inte behöver finjusteras för en särskild tillverkare. Detta resulterar i fördröjda eller uteblivna uppdateringar beroende på hur länge tillverkaren planerar att underhålla produkten.

Utöver de tjänster som erbjuds av kommersiella leverantörer existerar även alternativ för IoT-lösningar med öppen källkod och valmöjligheter för användaren. Stiftelsen Open Home Foundation (u.å) skriver att de strävar efter en värld där äldre enheter kan användas för att minska klimatpåverkan, samtidigt som användaren kan kontrollera vilka personuppgifter som kan komma att samlas in och erbjuda möjligheten att få enheter att kommunicera med varandra, oavsett tillverkare. För dessa ändamål existerar lösningar som den öppna programvaran Home Assistant som kan installeras på ett flertal olika plattformar som enkortsdatorn Raspberry Pi, samt operativsystem som Windows och Linux (Home Assistant, u.å). Via Home Assistant finns det därför möjlighet för användaren att integrera IoT-enheter av olika märken förutsatt att dessa erbjuder funktioner för detta (Home Assistant, u.å). Denna lösning ger därmed användaren kontroll över vilka uppgifter som hämtas in då tjänsten i första hand kontrolleras i en hemmiljö.

2.1.2 Trådlösa tekniker

För att stödja sammankopplingen av IoT-enheter kan olika trådlösa teknologier användas. Dessa kan delas upp i två kategorier: långdistansteknologier, vilket inkluderar 5G, LTE samt LPWAN (Low-Power Wide-Area Network), och kortdistansteknologier, som inkluderar OWC (Optical Wireless Communications), Bluetooth, ZigBee och WiFi (Wireless Fidelity) (Ding et al., 2020). För användning i hem är det kortdistansteknologier som är av intresse, med undantaget av OWC som är ett nytt koncept som inte är lika beprövat på den kommersiella marknaden som Bluetooth, ZigBee eller WiFi.

Bluetooth LE (IEEE 802.15.1) är en utveckling av tidigare Bluetooth-teknologi för att tillåta överföring av data på frekvenser mellan 2.4 till 2.485GHz med en minskad strömkonsumtion (Samuel, 2016). Detta gör det möjligt för användare att styra andra enheter i hemmet genom en direkt anslutning.

ZigBee (IEEE 802.15.4) ämnar att stödja simpla funktioner där flera enheter kräver sammankoppling, vilket exempelvis kan vara sensorer, automatiska mätsystem eller säkerhetssystem (Hwang et al., 2010). Teknologin erbjuder kortdistanskommunikation samt låg strömkonsumtion.

WiFi (IEEE 802.11) är ett samlingsbegrepp för olika trådlösa nätverksprotokoll. Idag är det vanligt att moderna enheter som exempelvis smarta telefoner, bärbara datorer och surfplattor erhåller någon form av WiFi-teknik eftersom majoriteten av dessa enheters funktionalitet är beroende av en anslutning till internet. Ett protokoll som är skapat i syfte att vara anpassad till IoT enheter är WiFi HaLow (IEEE 802.11ah) då det stödjer längre räckvidd och har lägre strömkonsumtion samt använder frekvenser under 1GHz (Wi-Fi Alliance, u.å).

2.1.3 Insamling av data

Datainsamling är en vanligt förekommande marknadsstrategi för en leverantör där kunden godkänner insamlingen för att kunna använda tjänsten. Colbjørnsen (2020) skriver att data kan även komma att säljas till tredje parter för att sätta målgrupper för reklam till kunder på gratistjänster som erbjuds av leverantören. I en undersökning från 2015 svarade 71 procent av deltagarna att det nu var ett måste att dela med sig av sina personuppgifter för att följa med i det moderna samhället. Samtidigt hävdar 91 procent av deltagare i en annan studie att de har förlorat kontroll över hur deras personuppgifter samlas in och behandlas (Belli et al. 2017). Vidare har personuppgifter och data relaterade till hälsa nu introducerats på

alternativa plattformar via applikationer vilket kan öka riskerna mot rättigheter för hur personuppgifter behandlas.

Myndigheten för samhällsskydd och beredskap (MSB) har skapat en termbank för informationssäkerhet (u. å). Där beskrivs personuppgifter som information som rör en identifierad eller identifierbar levande enskild person. Även uppgifter som tillsammans kan leda till identifikation av en person räknas som personuppgifter. Exempel på giltiga personuppgifter inkluderar för- och efternamn, e-postadress, platsinformation och hemadress.

Google (2022) detaljerar vanligt förekommande frågor för Nest-produkter genom att redovisa de typer av data som samlas in när Nest-enheter används i ett hemnätverk. Information angående enhetens inställningar samlas in, vilket involverar data relaterat till kontot som enheten används med, enhetens namn, enhetens typ, samt information relaterad till användarens hem som exempelvis adress och vart enheten är placerad i hemmet. Utöver Nest-enhetens egen data inhämtas även information om övriga aspekter i användarens hemnätverk som exempelvis närliggande trådlösa nätverkspunkter, övriga enheter i nätverket och information om deras hård- och mjukvara (Google, 2022), data från sensorer som exempelvis temperatur, fuktighet och röknivåer.

Amazon Alexa hämtar in data från IoT-enheter i hemmet som exempelvis namn, typ av enheter, dess egenskaper och användningshistorik (Amazon, u. å). Data kan även komma att inhämtas om enheter under perioder där enheten inte direkt styrs via Alexa för att ge användaren möjlighet att få reda på enhetens status om så önskas.

I Europa har leverantörer krav att förhålla sig till dataskyddsförordningen. Europaparlamentets och rådets förordning ((EU) 2016/679) definierar dataskyddsförordningen via 99 artiklar. I kapitel II, artikel 6 specificeras sex stycken villkor där minst ett villkor måste vara uppfyllt för att lagligt få behandla personuppgifter. Exempelvis består det första villkoret av att den registrerade har samtyckt att dennes personuppgifter behandlas för ett eller flera specifika ändamål. Därefter existerar andra artiklar som definierar ytterligare krav. Artikel 7, punkt 1 förklarar att om behandlingen av personuppgifter grundar sig i samtycke ska den som behandlar personuppgifterna kunna bevisa att den registrerade har samtyckt till behandlingen.

I en undersökning publicerad av noyb (2024) hämtades svar in från 2173 individer mellan den 16 november och 4 december 2023 fokuserat på huruvida företag förhåller sig till dataskyddsförordningen eller inte. När deltagarna fick frågan om hur företag förhåller sig till artikel 5 till 11, vilket beskrivs som grundprinciperna för dataskyddsförordningen, svarade 42,1 procent att företag har problem med att förhålla sig till principerna. Medan 8 procent svarade att de flesta företag inte förhåller sig alls. Kombinerat innebär detta att totalt 50,1 procent beskriver någon form av problem för företag att förhålla sig till grundprinciperna. Undersökningen innehåller kommentarer från deltagare som beskriver under vilka förhållanden dataskyddsförordningen hanteras hos företag. Där citeras svårigheter, trots utbildning, att förstå sig på lagarna. Samtidigt är underbemanning ett vanligt problem. En deltagare beskriver också att de flesta vinstdrivande företagen anser att dataskyddsförordningen är ett marknadshinder.

Shayegh och Ghanavati (2017) skriver att användaravtal kopplade till datainsamling ofta är långa och komplicerade texter. Avtalen som Google Home och Amazon Alexa bidrar till sina kunder identifieras som att innehålla långdragna texter med innehåll som beskriver komplicerade juridiska processer. Ett vanligt problem som också noteras är att dessa texter

oftast dyker upp när tjänsten eller enheten installeras. Vilket kan innebära att kunden ignorerar avtalen.

I grund och botten bestämmer kunden själv vilka tjänster och enheter som används i hemmet, baserat på olika faktorer, vilket inkluderar användaravtal som kunden nödvändigtvis inte vill acceptera. Även om kunden förstår språket som används i avtalet räcker inte detta. Många användaravtal presenteras på ett sådant sätt att det mer eller mindre säger åt kunden att man måste acceptera avtalet för att använda en enhet eller applikation (Shayegh & Ghanavati, 2017). För Google Home och Amazon Alexa-enheter blir valet att skapa ett alternativt konto för enheten, stänga av enhetens mikrofon eller att regelbundet ta bort den data som samlas in. Detta förhindrar många funktioner som enheten bidrar med.

Zhang et al. (2023) skriver att inställningar som rör hantering av personuppgifter är komplicerade och blir därmed försummade av användare. Tidigare forskning påvisar även att appar som installeras på smarta telefoner hämtar in data som inte är nödvändiga för appens funktion. Kunder har också svårt att förstå, förhålla sig till och acceptera användaravtal eftersom språket i dessa är för tekniska.

2.1.4 Molntjänster

Då användarkonton som skapas hos olika leverantörer används för att styra IoT-enheter i hemmet blir dessa också en form av molntjänst. Molnet används för att bidra med tjänster som hyrs ut till kunden för att uppnå ett specifikt mål. Kunden behöver därmed inte köpa dyr hårdvara, utan kan istället utnyttja resurser som leverantören kan bidra med till kunden.

Biswas och Giaffreda (2014) skriver att molntjänster blir grundläggande för IoT-enheter då resurser molnet bidrar med förstärker och effektiviserar tjänsterna som enheterna bidrar med samtidigt som möjligheterna för skalbarhet blir större. Vidare är också molnlösningar tillgängliga till alla områden med en fungerande uppkoppling mot internet. Två byggstenar existerar för nätverk där IoT-enheter används: Ett lokalt moln där enheterna är sammankopplade och kan kommunicera med varandra och blir begränsade av vilka funktioner som lokala enheter bidrar med, samt ett globalt moln som beskrivs som “traditionellt” och ger användarna tillgång till ytterligare resurser för hantering av krävande processer och lagring av data (Biswas & Giaffreda, 2014).

2.2 Informationssäkerhet

MSBs termbank för informationssäkerhet (u. å) definierar *informationssäkerhet* som skydd av informationstillgångar i relation till konfidentialitet, riktighet och tillgänglighet. *Konfidentialitet* definieras som att enbart behöriga personer, processer och objekt har tillgång till informationstillgången. *Riktighet* avser att informationstillgången är skyddad mot oönskade förändringar, antingen med orsak eller av misstag. *Tillgänglighet* innebär att informationstillgången är åtkomlig inom förväntad tid. Informationstillgångar kan vara fysiska, exempelvis hårdvara, lokaler eller pappersdokument; alternativt logiska, där exempel inkluderar kunddatabaser, applikationer, samt anställdas kunskap om processer. Fysiska tillgångar har ofta ett mer konkret värde bundna till dem. Medan det kan vara svårt att sätta ett värde på de logiska tillgångarna. Båda typer av tillgångar löper risk att bli påverkade av cyberattacker.

Sharif och Mohammed (2022) skriver att antalet anmälda cyberattacker till organisationer

som Federal Bureau of Investigation, Federal Trade Commission och Kaspersky visar på en trend där antalet attacker har ökat kraftigt mellan 2010 och 2021 i USA.

2.2.1 Informationssäkerhet och IoT-enheter

Ur ett informationssäkerhetsperspektiv blir hantering av personuppgifter ett komplicerat ämne för leverantören, men även för kunden. Ziegeldorf et al. (2013) skriver att det blir lättare att identifiera en individ via IoT-enheter då dessa utnyttjar ett centralt system för att spara personuppgifter om kunden. Även om kunden godkänt insamlingen av uppgifterna blir det också svårt för kunden att kontrollera hur uppgifterna används då den centrala infrastrukturen inte är tillgänglig för kunden. Via kameraövervakning kan bilder användas för att samla ytterligare information på externa tjänster som exempelvis sociala medier. Vidare styrs också många IoT-enheter via röstkommandon som i sin tur använder sig av databaser för att känna igen talmönster och kan användas för att identifiera en person vilket ökar riskerna relaterade till integritet för kunden.

Geneiatakis et al. (2017) skriver att det finns möjligheter för en angripare att avlyssna trafiken som IoT-enheter skickar mellan kundens utgående anslutning och leverantör för att utläsa ytterligare information om kommunikationen. Då många IoT-enheter styrs av en applikation via kundens mobiltelefon eller andra enheter skapar detta en möjlighet för en angripare att infektera applikationen med skadlig kod, antingen via svagheter i enhetens operativsystem eller den aktuella applikationen. Flera tillverkare antar dessutom att den övriga infrastrukturen i kundens nätverk, exempelvis en router, kan ta hand om potentiella säkerhetsproblem.

I ett uppmärksammat fall skriver Norrgrann et al. (2022) att före detta anställda på företaget Verisure berättar om instanser där larm utlösts av olika anledningar. Detta resulterade i att anställda på företaget fick tillgång till bildövervakning för att kontrollera hur situationen sett ut. I dessa fall beskrivs situationen som att en medlem i hemmet lämnat fastigheten och larmat på medan övriga medlemmar i hemmet utlöst larmet. Det har resulterat i att företagets anställda har fått tag i explicita bilder på personer som klivit ur sängen på morgonen eller kommit ut ur badrummet utan deras samtycke. Bilderna har sedan spridits mellan anställda på företaget.

2.2.2 Konsekvenser av bristfällig datahantering

Företag har ett ansvar mot sina kunder när deras personuppgifter sparas på företagets system. För IoT-enheter kan ytterligare konsekvenser uppstå på grund av felaktig eller obehörig hantering av insamlade personuppgifter. Karale (2021) skriver att ett flertal etiska problem kan uppstå i relation till IoT-enheter och informationen som dessa samlar in. När flera IoT-enheter i ett hem inhämtar information om personer och enheter runt om dessa blir det svårt att identifiera enhetens ägare. Samtidigt blir det svårt för en IoT-enhet att avgöra vad som är privat och publik data då insamling sker genom olika typer av hårdvara.

Vidare kan enheter som kommunicerar med varandra potentiellt skapa oförutsedda beteenden, vilket kan göra att enheterna stör ut varandra och blir ett irritationsmoment för användaren, vilket i sin tur kan ge konsekvenser i form av förändringar i användarens schema och tidsplaner (Karale, 2021). I extrema fall kan intrång i IoT-system och informationen som förvaras skapa situationer som kan leda till fysisk eller psykisk skada för individen.

3 Problemställning

I dagens informationssäkerhetsklimat har lagar som dataskyddsförordningen upprättats i Europa som kontrollerar hur organisationer får hantera personuppgifter (Europaparlamentets och rådets förordning (EU) 2016/679). Detta har medfört att användare har fått rätt att kontrollera vilken typ av uppgifter som en organisation får samla in. Därför måste organisationen vara transparent med vilka personuppgifter som samlas in och till vilket syfte. Problem som kan uppstå under dessa förhållanden består bland annat av att användaren kan, av olika anledningar, ha svårt att ta till sig av denna information.

Problem att förstå avtal kan bli svåra då IoT-enheter introduceras i ekvationen eftersom dessa fungerar som en mellanhand där kunden får komforten av en lättanvänd enhet i utbyte mot kundens personuppgifter och långdragna avtal (Shayegh & Ghanavati, 2017). Detta arbete bedrivs därmed för att öka kunskapen för hur personuppgifter hanteras i en hemmiljö där IoT-enheter används och kundens medvetenhet av insamlingen och dennes inställning till detta.

Huvudproblemen i denna kontext består därför av:

- Vilka personuppgifter samlar IoT-enheter in?
- Vilken medvetenhet har kunden för personuppgifter som samlas in?
- Vilka personuppgifter är kunder bekväma att dela med sig av?

Problemen uppstår i relationen mellan kund och leverantör ur ett tekniskt datainsamlings-perspektiv, samt kundens medvetenhet för vilka personuppgifter som leverantören hämtar in.

Denna studie syftar till att informera privatpersoner som använder, eller överväger att använda IoT-enheter i hemmet angående hur deras personuppgifter hanteras. Inhämtade källor utgår från ett kundperspektiv avseende den information som leverantören presenterar gentemot kunden. Från ett leverantörsperspektiv, skulle den data som presenteras i arbetet även kunna ge insikt i hur kunder upplever personuppgiftshantering. Sammantaget skulle detta kunna användas som bas för diskussion och utveckling av en enhet som ger transparens över vilken information som hämtas in, och hur kunden kan hantera inställningarna på ett användarvänligt sätt.

3.1 Frågeställning

Arbetets syfte består av att skapa förståelse för vilka personuppgifter som samlas in av IoT-enheter i hemmet, samt undersöka vilken förståelse privatpersoner har för uppgifter som samlas in via dessa enheter. Med dessa mål i beaktning har en forskningsfråga formulerats för att besvara arbetets problemställning:
“Vilka personuppgifter samlas in av IoT-enheter i privatpersoners hem och vilken medvetenhet och inställning har privatpersoner till insamlingen?”

3.2 Avgränsningar

Detta arbete fokuserar endast på IoT-enheter som används i en hemmiljö och hur privatpersoner uppfattar den insamling av personuppgifter som sker genom dessa. Därmed behandlar inte detta arbete IoT-enheter i någon annan miljö än hemmet. Öppna lösningar för

integration av IoT-enheter i hemmet har även beskrivits kort i bakgrundskapitlet, men dessa har inte behandlats då kommersiella lösningar ligger i fokus.

4 Metod

Målet med arbetet är att undersöka vilka personuppgifter som samlas in av IoT-enheter samt att se hur medvetna privatpersoner är av insamlingen. Eftersom forskningsfrågan har definierats utifrån problemställning som beskrivits i föregående kapitel har arbetet delats upp i två delar. Den första fokuserade på den tekniska aspekten av vilken data som samlas in och vilket format denna data har. Den andra har undersökt privatpersoners perspektiv och val de gör gällande IoT-enheter kopplat till hur bekväma och medvetna de är gällande datainsamling. I detta kapitel presenteras den metod som användes i arbetet.

4.1 Val av metod

Detta arbete utfördes med två olika strukturerade litteraturstudier som utforskade de två olika infallsvinklarna. Ett alternativ istället för denna metod hade varit att genomföra en enkätstudie. Detta hade potentiellt lett till att undersökningen hade fått större underlag från en större mängd kvantitativa data. Dworkin (2012) menar att provstorleken inom kvalitativa forskningsmetoder oftast är mindre än de kvantitativa metoderna i syfte att ge en mer nyanserad bild av ämnet som undersöks. Ett annat alternativ hade varit att genomföra intervjuer. Detta hade öppnat för mer kvalitativ data till skillnad från en enkätstudie, då intervjudeltagarna haft möjlighet att uttrycka sig mer öppet och följdfrågor hade kunnat ställas för att ge ett mer detaljerat perspektiv. Intervjuer är däremot begränsade på tillgängligheten av människor som har kunskap inom området och har tillgång till relevant hårdvara för studien. Det är ett tidskrävande åtagande som inte nödvändigtvis garanterar att någon användbar data genereras. Kitchenham (2004) skriver att en av fördelarna med en strukturerad litteraturstudie är att sannolikheten ökar att hitta riktiga resultat som mindre studier inte alltid kan upptäcka i samma mån. Syftet med en strukturerad litteraturstudie är att samla in den existerande kunskapen inom det valda vetenskapliga området (Paré et al., 2015). Detta leder till att den existerande kunskapen kan sammanställas och därmed identifiera specifikt vad som har skrivits relaterat till ämnet. På så sätt kan även olika trender och mönster inom forskningen uppenbaras, samt tillåta utveckling av nya ramverk och teorier för framtida forskning. Kitchenham (2004) beskriver att en strukturerad litteraturstudie är mer tidskrävande än en litteraturstudie och kräver att en stor mängd data samlas in. Detta leder däremot till att arbetet kan bli verifierat, och ifall konsekventa resultat finns innebär det att inhämtad data är robust, och ifall det inte finns innebär det att källorna kan behöva varieras. Det finns även risk för att viss vetenskaplig bias kan uppkomma inom en strukturerad litteraturstudie (Kitchenham, 2004), vilket innebär att det är viktigt att åtgärder finns på plats för att motarbeta problemet.

I denna studie genomfördes två strukturerade litteraturstudier för att samla in existerande data inom ämnet. Ett alternativ mot detta hade varit att den ena studien utformades i exempelvis en intervju eller enkätstudie, i syfte att tillföra ett annat perspektiv. Istället valdes det att två likadana studier med olika infallsvinklar skulle genomföras för att samla in data som är likvärdiga och därmed leda till att resultaten är jämförbara.

4.2 Strukturerade litteraturstudier

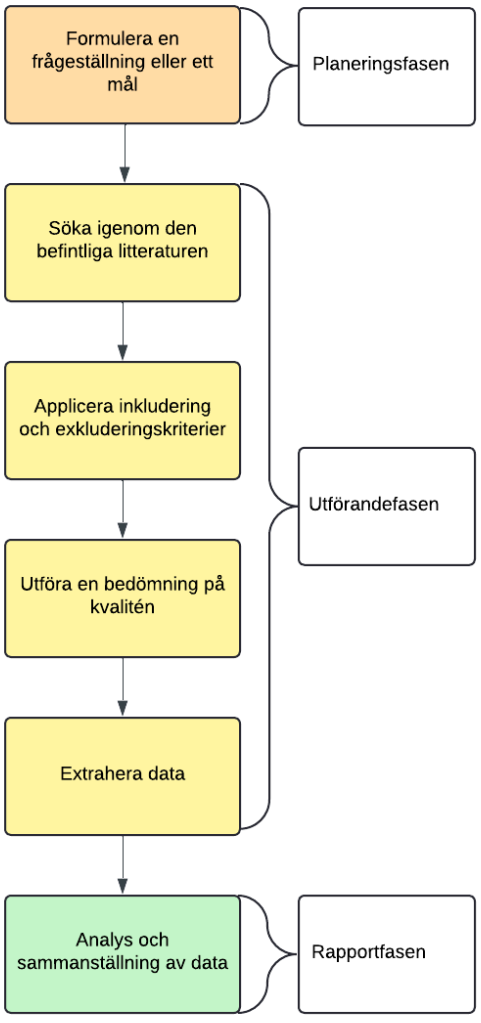
Det finns tre huvudsakliga faser som en strukturerad litteraturstudie följer, vilket är planeringsfasen, utförandefasen och rapportfasen (Kitchenham, 2004). Planeringsfasen

handlar om att redovisa behovet av studien och att definiera forskningsfrågan för att ge en tydlig grund för arbetet. Utförandefasen är det skede där en sökstrategi utvecklas och appliceras för att hitta så många primära källor som möjligt. Rapportfasen är arbetets slutliga moment och ämnar att dela med resultaten till potentiella intressenter.

Utförandet av en strukturerad litteraturstudie kan brytas ned till sex stycken steg enligt Paré och Kitsiou (2017). Dessa steg är som följande:

1. Formulera en frågeställning eller ett mål
2. Söka igenom den befintliga litteraturen
3. Applicera inkludering- och exkluderingskriterier
4. Utföra en bedömning på kvalitén
5. Extrahera data
6. Analys och sammanställning av data

Jämförs de tre huvudsakliga faser som Kitchenham (2004) föreslog med de sex stycken steg som presenteras av Paré och Kitsiou (2017) existerar överlappande moment. Genom att slå ihop dessa två tillvägagångssätt för strukturerade litteraturstudier skapades en ny modell som detaljeras i Figur 1.



Figur 1: Sex-stegsmetoden som baseras på metoder från Kitchenham (2004) samt Paré och Kitsiou (2017).

4.2.1 Formulera en frågeställning eller ett mål

Det första steget i en strukturerad litteraturstudie är att formulera en frågeställning eller ett mål för att bevisa att studien uppfyller ett behov samt att identifiera vilka koncept eller variabler som är viktiga (Paré & Kitsiou, 2017). En tydlig frågeställning blir därmed viktig för att veta exakt vad som undersöks för att effektivisera resten av arbetet.

4.2.2 Söka igenom den befintliga litteraturen

Kitchenham (2004) menar att målet med en strukturerad litteraturstudie är att hitta så många primära källor som möjligt med en opartisk sökstrategi. Vikten här är att definiera en sökstrategi som omfattar all relevant information till frågeställningen. Preliminära sökningar kan användas för att hitta liknande litteraturstudier inom området och därmed potentiellt hitta relevanta studier som kan användas. Genom att använda frågeformuleringen kan potentiella söktermer och nyckelord påträffas som är relevanta för sökningen. Data som inhämtas från artiklar bildar koder. Dessa koder sorteras in i kategorier som slutligen blir en del av ett övergripande tema (Graneheim & Lundman, 2004). I dessa arbeten skapades ett antal fördefinierade teman där data kategoriseras baserat på koderna som upptäcktes.

4.2.3 Inkluderings- och exkluderingskriterier

För att undvika vetenskaplig bias måste grundläggande inkluderings- och exkluderingskriterier upprättas. Dessa kriterier underlättar sökprocessen och medför att källor inhämtas med en objektiv process (Paré & Kitisou, 2017). Enligt Kitchenham (2004) bör inkluderings- och exkluderingskriterier baseras på forskningsfrågan och formuleras på ett sätt som klassificerar källan på ett korrekt vis.

4.2.4 Utföra en bedömning på kvalitén

För att säkerställa att insamlad data är relevant och kan tolkas på rätt sätt, är det viktigt att bedöma källans vetenskapliga kvalité (Paré & Kitsiou, 2017). Genom att bedöma innehållet i en artikel och utföra kvalitétsanalyser skapas möjligheter att tolka data och hur denna påverkar arbetets resultat. Detta möjliggör en diskussion om vilken data som anses möta arbetets kriterier. Överläggningar mellan arbetets författare kan skapa ytterligare inkluderings- och exkluderingskriterier för att undvika avvikelser från den valda metoden och underlätta att bedöma ytterligare data (Kitchenham, 2004).

4.2.5 Extrahera data

För att uppnå resultat som ger svar på arbetets problem- och frågeställning, samt underlag för arbetets slutsats och diskussion, måste relevant data extraheras. Detta inkluderar data angående källans metoder, såsom hur, vart och vem som utförde studien, samt vilka resultat som uppnåtts och om dessa varit kvalitativa eller kvantitativa (Paré & Kitsiou, 2017). Kitchenham (2004) skriver att det är viktigt att data inhämtas på ett konsekvent sätt. Detta kan exempelvis uppnås genom att låta övriga deltagare granska den data som extraheras.

4.2.6 Analys och sammanställning av data

Slutligen måste extraherade data sammanställas, summeras och presenteras på ett sätt som bidrar till nuvarande litteratur (Paré & Kitsiou, 2017). Arbetet bör därefter framställas via accepterade och relevanta kvalitativa eller kvantitativa metoder.

4.3 Tillämpning av metod

Baserat på forskningsfrågan söktes befintlig litteratur igenom med söktermer i kombination med booleska operatorer för skapa ett brett omfång med termer som kan formuleras på olika sätt men är möjligtvis synonyma, för att samtidigt inkludera relevanta termer för forskningsfrågan.

För båda arbeten etablerades generella inkluderings- och exkluderingskriterier som appliceras på båda studierna.

Inkluderingskriterier

- Endast artiklar skrivna på engelska
- Artiklar publicerade 2020 eller senare
- Artiklar endast publicerade i journaler

Exkluderingskriterier

- Artiklar bakom betalvägg
- Identiska artiklar

Artiklar fick endast vara skrivna på engelska för att säkerställa att den data dessa innehåller gick att tolka utan externa verktyg. Då IoT-enheters struktur och användaravtal kan utvecklas över tid har valet gjorts att endast inkludera data från 2020 och framåt. Vidare fick endast inkluderad data ha publicerats i vetenskapliga journaler. Detta val gjordes för att minska antalet resultat i tillämpning av inkluderings- och exkluderingskriterier och samtidigt uppnå resultat av kvalitet.

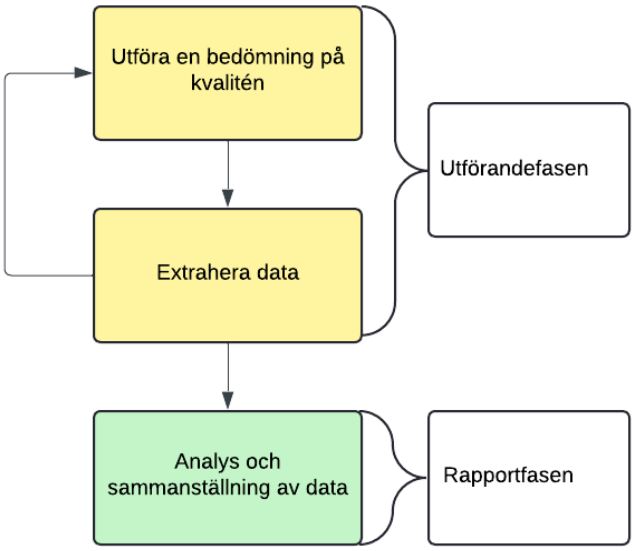
Identiska artiklar exkluderas för att undvika att data som redan inhämtats repeteras. Arbetets författare har genom Högskolan i Skövde fått tillgång till vetenskapliga databaser genom inloggning via institutionens infrastruktur. Detta innebär att vissa artiklar eventuellt kan vara bakom betalvägg, men att denna studie förbigår dessa med hjälp av resurser erhållna från Högskolan i Skövde. Inhämtad data har sedan evaluerats enligt metoden som beskrivs i kapitel 4.2.4. Källor har även evaluerats med hjälp av arbetets andra författare för att kontrollera källan från ett annat perspektiv och dess relevans till arbetet.

I planeringsfasen etablerades relevanta teman för att kategorisera den data som inhämtades. Dessa teman formade ett ramverk som avgjorde vilka källor och data som bedömdes relevanta till arbetets mål och forskningsfråga. Detta har resulterat i två strukturerade litteraturstudier som på egen hand kunnat besvara en del av forskningsfrågan. Detta gjordes för att på ett effektivt sätt kunna utforska problemet från två olika vinklar.

För att effektivisera metoden har verktyget Rayyan använts i båda litteraturstudier för att manuellt sortera artiklar efter inkluderings- och exkluderingskriterier. Genom att ladda upp exporterade artiklar i BibTeX och RIS-format till verktyget får båda deltagarna tillgång till en lista över alla artiklar som manuellt behöver sorteras när alla kriterier tillämpats på sökningen. Genom att läsa igenom titlar, sammanfattning och nyckelord sållades ytterligare

artiklar som inte var relevanta till arbetet bort.

För att besvara hela forskningsfrågan behövde resultaten av båda litteraturstudier kombineras. Data som inhämtats till gemensamma slutsatser behövde därför en ytterligare evaluering. Detta innebar att arbetets andra författare utförde en itererad evaluering med hjälp av modellen som beskrivits i kapitel 4.2, vilket detaljeras i Figur 2. Då den data som hämtades in separat för båda litteraturstudier inte räckte för att besvara arbetets forskningsfråga, fanns det därför anledning att genomföra de två sista stegen i utförandefasen för att kontrollera att slutsatsen som presenteras genomfördes korrekt. Därför har sex-stegsmetoden som detaljeras i Figur 1 modifierats i syfte att kunna utföra en omfattande kontroll för att hitta gemensamma nämnare i båda studier och därmed nå en kombinerad slutsats. Via interna överläggningar har arbetets författare gemensamt evaluerat artiklar genom bedömning från två perspektiv med kriteriet att båda deltagarna var överens om att artikeln bedömdes som relevant för ämnet.



Figur 2: Modifikation av sex-stegsmetoden som detaljeras i Figur 1. Syftet är att iterera de två sista stegen av utförandefasen.

4.3.1 Databaser

Databaser har valts gemensamt av arbetets båda författare då dessa innehåller material som är relevanta för forskningsfrågan genom artiklar som berör teknologi, datavetenskap och socialvetenskap.

- IEEE Xplore
- ACM Digital Library
- Web Of Science
- ScienceDirect

IEEE Xplore beskrivs som en ledande digital plattform där besökare får tillgång till vetenskapligt material publicerat av Institute of Electrical and Electronics Engineers (IEEE) och dess partners (IEEE, u.å.). ACM Digital Library beskrivs som världens mest omfattande databas med artiklar relaterade till informationsteknologi och uppmanar bland annat

forskare, lärare och professionella datavetare att använda plattformen för att ta del av vetenskapligt material (ACM, u.å.). Databasen Web of Science drivs av Clarivate, som stöder över 7000 forskningsorganisationer globalt (Clarivate, u.å.) och innehåller artiklar relaterade till ett flertal olika forskningsområden. ScienceDirect är en databas skapad för syftet att låta användaren ta del av vetenskapligt material publicerade av Elsevier som innehåller material relaterat till en rad ämnen och inkluderar exempel som datavetenskap, medicin och socialvetenskap (Elsevier, u.å.). Med dessa beskrivningar bedömdes databaserna vara relevanta till arbetets forskningsfråga.

4.3.2 Insamling av personuppgifter via IoT-enheter

Arbetets första strukturerade litteraturstudie genomfördes för att besvara forskningsfrågans inledande halva. Därmed består frågeställningen för studien av:

"Vilka personuppgifter samlas in av IoT-enheter i privatpersoners hem?"

En sökträng har etablerats med hjälp av åtta nyckelord för att inkludera artiklar som baseras på IoT i en hemmiljö. Termerna "IoT" eller "Internet of Things", samt "Personal" eller "Private" användes för att inkludera fler artiklar som kan syfta på ord som används synonymt. I kombination användes orden "Smart", "Home", "Data" och "Collection" separerade för att undvika omedveten exkludering. Den booleska operatorn "AND" användes för att kombinera IoT-enheter i hemmet med termer som inkluderar insamling av personuppgifter.

*(IoT **OR** "Internet of things") **AND** Smart **AND** Home **AND** (Personal OR Private) **AND** Data **AND** Collection*

Då studien fokuserade på insamling av personuppgifter från ett tekniskt perspektiv etablerades tre stycken teman innan analys och sammanställning av data: Datatyp, Molndata och lokal data. Syftet med detta var att sammanställa identifierade uppgifter och samtidigt visa om dessa sparades på molntjänster eller lokalt. Kategorier under dessa teman bildades under kodning då uppgifter som identifierades klassificeras efter vilken form dessa tog.

Initial sökning utan applicering av kriterier som journaler, årtal och artiklar utan betalvägg genererade totalt 11988 artiklar. Genom att filtrera artiklar publicerade år 2020 och framåt minskade resultaten till 8065. Därefter applicerades filter för att endast visa artiklar publicerade i journaler, vilket minskade det totala antalet artiklar till 2865. Sedan applicerades filter för att undvika artiklar med ytterligare betalväggar. Detta resulterade i totalt 1047 artiklar. Under det sista steget innan manuell sortering hittades en identisk artikel som sållades bort.

Kvarvarande artiklar konverterades till formaten BibTeX och RIS-format för att sedan laddas upp till verktyget Rayyan och sedan manuellt kategorisera dessa som: "Exkluderad", "Obestämd" och "Accepterad". Denna kategorisering skedde genom att läsa igenom titlar, sammanfattning och nyckelord. Under denna process sorterades 87 artiklar ut för vidare läsning. Slutligen bestod resultatet av 10 artiklar.

Inkluderings- och exkludringskriterier	Web of Science	ScienceDirect	IEEE	ACM	Total
Initial sökning	21	6432	78	5457	11988
Enbart engelska	21	6432	78	5457	11988
Artiklar från 2020 eller senare	13	4736	49	3267	8065
Journal	10	2243	11	601	2865
Artiklar utan betalvägg	6	437	3	601	1047
Identiska artiklar	5	437	3	601	1046
Utan tekniskt fokus på datainsamling med IoT-lösningar	0	6	0	4	10

***Tabell 1**: Resultat med söksträngen: (IoT **OR** "Internet of things") **AND** Smart **AND** Home **AND** (Personal **OR** Private) **AND** Data **AND** Collection*

4.3.3 Medvetenhet av insamling av personuppgifter

Arbetets andra strukturerade litteraturstudie genomfördes för att besvara forskningsfrågans andra halva. Därmed består frågeställningen för studien av:

"Vilken medvetenhet och inställning har privatpersoner till insamlingen [av personuppgifter med IoT-enheter]?"

Sökströngen som användes för studien inkluderar nyckelorden: "Personal OR Private data", "Awareness", "IoT OR Internet of Things", "Smart" och "Home". Det första nyckelordet är en översättning av "personuppgifter"där två olika variationer täcks med hjälp av den booleska operatorn "OR". Medvetenhet översätts och används i sökströngen, sedan skrevs IoT inom parentes tillsammans med "Internet of Things" för att fånga upp både förkortningen och hela ordet utskrivet. Till sist tillämpades orden "Smart" och "Home" till för att täcka användningen inom hemmet. Alla separata nyckelord binds samman med booleska operatorn "AND" för att garantera att allt inkluderas i sökningen. Den slutliga sökströngen var enligt följande:

*(Personal **OR** Private) **AND** data **AND** Awareness **AND** (IoT **OR** "Internet of Things") **AND** Smart **AND** Home*

För denna studie låg fokus kring privatpersoners medvetenhet och inställning till insamlingen av personuppgifter av IoT-enheter inom hemmet, och därför etablerades tre teman innan steg 6 i metoden, det vill säga analys och sammanställning av data. Dessa bestod av Bekvämlighet, Förtroende och Medvetenhet. Syftet var att identifiera de olika områden som kan bidra till att privatpersoner känner sig bekväma till att använda IoT-enheter och vilken inställning de har till insamlingen av personuppgifter. Under metodens slutgiltiga steg skapades kategorier baserat på de koder som fanns, för att vidare klassificera den data som identifierades.

När sökströngen användes på de olika databaserna utan några inkluderings- eller exkluderingskriterier blev resultatet 9753 artiklar. Dessa artiklar importerades till granskningsverktyget Rayyan för att underlätta processen. Genom att enbart ta med artiklar som publicerades 2020 eller senare resulterade det i att det återstod 6369 artiklar. Att enbart inkludera artiklar från journaler resulterade i 2923 artiklar. Artiklar som var låsta bakom ytterligare betalvägg togs bort, vilket resulterade i 962 artiklar. Sedan gjordes en granskning av artikelns titel, sammanfattning och nyckelord med hjälp av verktyget Rayyan för att

identifiera artikelns relevans till forskningsfrågan, vilket resulterade i 49 artiklar. De artiklar som var kvar analyserades baserat på deras kompletta innehåll, och resulterade i att det slutligen blev 21 artiklar som användes i studien.

Inkluderings- och exkluderingskriterier	Web of Science	ScienceDirect	IEEE	ACM	Total
Initial sökning	10	5799	51	3893	9753
Enbart engelska	10	5799	51	3893	9753
Artiklar från 2020 eller senare	3	4018	26	2322	6369
Journal	3	2362	1	535	2901
Artiklar utan betalvägg	2	402	1	535	940
Identiska artiklar	2	402	1	535	940
Artiklar utan fokus på privatpersoners medvetenhet gällande insamling av personuppgifter av IoT-enheter i hemmet	0	10	0	11	21

***Tabell 2**: Sökresultat med söksträngen: (Personal **OR** Private) **AND** data **AND** Awareness **AND** (IoT **OR** "Internet of Things") **AND** Smart **AND** Home*

5 Resultat

Denna del redovisar resultaten enskilt från båda strukturerade litteraturstudier. Resultaten av varje studie demonstreras separat via delkapitel för att strukturera upp arbetets resultat.

Kapitel 5.1, 5.2 och 5.3 redovisar resultaten från den första litteraturstudien med tre teman: Datatyp, Molndata och Lokal data. Teman, kategorier och deras tillhörande koder finns i appendix A-C.

Kapitel 5.4, 5.5 och 5.6 redovisar resultaten från den andra litteraturstudien med tre teman: Bekvämlighet, Förtroende och Medvetenhet. Dessa resultat detaljeras vidare i appendix D-F. Teman tillämpades för att hämta relevant data från artiklar utifrån vardera studies perspektiv.

5.1 Datatyp

Arbetets första strukturerade litteraturstudie ämnar att besvara frågeställningen:*"Vilka personuppgifter samlas in av IoT-enheter i privatpersoners hem?"*. För detta syfte skapades det första temat; Datatyp, som rör insamlad data oavsett var denna lagras. Tillhörande koder delades in i följande kategorier: Enhetsdata (7), Platsdata (4), Bilddata (5), Röstdata (5), Kroppsdata (4) och Sensordata (4). Teman, kategorier och tillhörande koder finns att läsa i appendix A.

5.1.1 Enhetsdata

Data som är mest vanligt förekommande består av enhetsdata. Dragonas et al. (2023) utförde en analys av HIKVISIONs applikation som används för kontroll av övervakningsenheter. Analysen utfördes på Android och iOS-versionen av applikationen där flera artefakter identifierades som potentiellt kan avslöja detaljer om användarens enheter och tillhörande nätverk när applikationen är aktiv. Vidare har filer identifierats som kan påvisa att applikationens användare har aktiverat fjärrhantering av övervakningsutrustning.

Wu et al. (2021) skriver i en separat undersökning av IoT-enheter från olika leverantörer som exempelvis Amazon, Google och Samsung där okrypterad enhetsdata som skickas över trådlösa nätverk och fångats upp via inspektion av nätverkspaket. En videokamera från Samsung skickade information utan kryptering som bär risk att identifiera enheten. I paketen som fångats upp kunde MAC-adress, serienummer, enhetens namn och ett användarnamn utläsas. Liknande data kunde även identifieras hos en annan övervakningskamera av märket Insteon där MAC-adress, IP-adress och en unik ID för kameran kunde identifieras. En högtalare från Triby kommunicerade även med okrypterade uppgifter och inkluderade MAC-adress, serienummer och användarnamn.

Servida et al. (2023) skriver att det via tillhörande mobilapplikationer finns möjlighet att hämta in diverse information om enheter baserat innehållet i mobilens lokala lagring. Xiaomi Home sparar information om enheterna och deras funktion, vilka rum som finns konfigurerade i hemmet och enheterna som återfinns i dessa. Applikationen Ikea Trådfri sparar data om enheternas ID, grupper, samt hur många totala enheter som finns i hemmet. I övrigt sparas diverse data om enheternas funktion, batterinivåer och testdata.

5.1.2 Platsdata

Via ett antal tidigare icke-dokumenterade API:er (Application Program Interface) kunde data läsas ut från en robotdammsugare tillverkad av Amazon. Med denna data fanns det möjlighet att kartlägga ägarens hem via detaljer som exempelvis hur länge dammsugaren städar, vilka hinder dammsugaren upptäcker i hemmet, bilder på hinder i krypterat format och koordinater (Onik et al, 2023). En smart våg tillverkad av Withings skickade okrypterade paket innehållande kroppsdata och användarens postnummer (Wu et al., 2021).

Tjänsten Ring Neighbours fungerar som ett socialt nätverk där användare har möjlighet att publicera bilder, video och tillhörande beskrivning. Uppgifter från dessa inlägg hämtades med hjälp av ett skript som kombinerades ihop med en användare för att snabbt byta hemadress och på så sätt få tillgång till inlägg över ett större område. Inlägg anonymiseras med hjälp av en närliggande geografisk vägkorsning (Calacci et al., 2022).

5.1.3 Bilddata

Utöver den platsdata som kan inhämtas av Amazons robotdammsugare kan användaren även få tillgång till bilder som dammsugaren tar på potentiella hinder. Bilderna är krypterade och deras filnamn beskriver objektet i bilden. Bilderna är åtkomliga i 36 timmar och länken till dessa försvinner om användaren kollar på dem (Onik et al., 2024). I kommunikationen för en kamera från D-Link och dess tillhörande applikation skickades delar av bilder i JPEG-format utan kryptering till applikationen.

Varje inlägg på Ring Neighbours har möjligheten att visa upp till fem bilder hämtade från användarens ringklocka. I flera fall inkluderas bilder från ringklockor vars kamera riktats mot allmän väg (Calacci et al, 2022). Likt bilder kan användare på Ring Neighbours även välja att bifoga upp till 5 videoklipp hämtade från ringklockan (Calacci et al., 2022).

En övervakningskamera av tillverkaren Xiaomi noterades kommunicera med molnet utan kryptering och inkluderade bland annat okrypterad video (Wu et al., 2021). Servida et al. (2023) skriver att det var möjligt att ladda ned videoinspelning från applikationen som används av QBee-kameror och noterar att dessa videoklipp har spelats in på grund av rörelsedetektion.

5.1.4 Röstdata

För Apple HomePod Mini, Google Nest Audio och Google Home Mini existerar inställningar för röstprofiler. Dessa profiler kontrollerar vem som pratar med enheten och matchar svaren till deras personliga kalender, meddelanden och påminnelser (Valero et al., 2023). Vidare hämtar Facebook Portal in data från konversationer för att visa reklam på Facebook. Denna data kan komma att delas vidare med Facebooks affärspartners (Valero et al., 2023).

Zhang et al. (2022) skriver att telefoner som använder Android upp till version 12 inte kräver några behörigheter för applikationer att få tillgång till telefonens rörelsesensorer. Dessa sensorer kan användas för att behandla mänskliga röstfrekvenser och därmed avlyssna telefonens användare.

5.1.5 Kroppsdata

Förutom postnummer skickar även vågen tillverkad av Withings detaljerad data om

användarens kropp utan kryptering. Detta inkluderar kön, ålder, höjd och vikt (Wu et al., 2021).

Smartklockan Fitbit Aria 2 besitter egenskaper för att mäta användarens vikt, kroppsfett och BMI. Medan Fitbit Charge 3 kan användas för att mäta hjärtrytm, sömntid och djup av sömn (Sei & Ohsuga, 2023).

5.1.6 Sensordata

Data från sensorer i applikationen Xiaomi Mi visar historik från temperatur- och luftfuktighetssensorer. Det noteras även att applikationen uppdaterar sig själv med historisk data från molnet som först kommit från rörelsesensorer, även om sensorn inte längre är ansluten till ett nätverk (Servida et al, 2023).

Zou et al. (2023) skriver att det med inspektion av nätverkspaket finns möjlighet att identifiera IoT-enheter och kartlägga boendes vanor genom att observera trafiken från sensorer mellan molnet och tillbaka.

5.2 Molndata

Arbetets första strukturerade litteraturstudie ämnar att besvara frågeställningen: *"Vilka personuppgifter samlas in av IoT-enheter i privatpersoners hem?"*. För detta ändamål har temat "Molndata" skapats för att sortera vilken data som identifierats skickas till molntjänster. Koder har delats in i följande kategorier: Enhetsdata (7), Bilddata (2), Röstdata (5), Användardata (4), Platsdata (3) och Sensordata (4). Teman, kategorier och tillhörande koder finns att läsa i appendix B.

5.2.1 Enhetsdata

Wu et al. (2021) skriver att kameror från Samsung, Insteon och Xiaomi skickar känsliga uppgifter som MAC-adresser, användarnamn, tidsstämplar, portnummer, IP-adresser, serienummer okrypterat mellan enhet och molnet. En högtalare från Triby identifierades också att skicka användarnamn, serienummer och MAC-address i klartext.

Onik et al. (2024) hade möjlighet att med odokumenterade API:er utläsa information om robotdammsugares olika aktiviteter, vilka Wi-Fi anslutningar dammsugaren använt sig av, hur lång tid dammsugaren laddas och aktiv städtid.

Tjänster och enheter från Meross sparar unik information om sammanlänkade telefoner och deras egentillverkade enheter i molntjänster (Servida et al, 2023).

5.2.2 Bilddata

Tjänsten för Amazons dammsugare erbjuder användare att ladda ned bilder som tagits av dammsugare för vidare granskning. Bilderna är krypterade men namnges efter det objekt som identifierats i bilden (Onik et al, 2024). En kamera från Xiaomi har identifierats att skicka okrypterad data som innehåller videomaterial till molntjänster (Wu et al, 2021). Inlägg på Ring Neighbours innehåller data som bilder och video tagna av privatpersoners ringklockor (Calacci et al, 2022).

5.2.3 Röstdata

Enheter som Apple HomePod Mini, Google Home Mini, Amazon Echo Dot 4 och Amazon Echo Show 5 sparar data om konversationer och röstkommandon i sina respektive molntjänster. Varje enhet erbjuder användaren att ta bort data som sparas, antingen genom automatisering eller genom att manuellt radera denna. Samtidigt noteras det att Facebook Portal använder Amazons rösttjänster, vilket gör att data skickas både till Facebook och Amazons infrastrukturer (Valero et al, 2023).

5.2.4 Användardata

Tjänster från Meross och Google Home sparar användarens e-postadresser. Vidare sparar Google även uppgifter om användningstid av applikationer i Android, vilka röstkommandon som använts av det aktuella kontot och dess Youtube-historik (Servida et al, 2023). Huang et al. (2020) skriver att enheter som används för TV-tjänster från Nvidia, Roku, TCL, Samsung, Sony och LG använder någon form av spårningstjänst. Via tjänsten Ring Neighbours har det funnits möjlighet att hämta unika identifierare för användare insamlade via inlägg på tjänsten (Calacci et al, 2022).

5.2.5 Platsdata

Anonymiserad platsdata som funnits i inlägg gjorda på Ring Neighbours har gått att ladda ner lokalt (Calacci et al, 2022). Genom Amazons tjänster för robotdammsugare går det via tidigare odokumenterade API:er att hämta ut koordinater och information om hinder för att kartlägga dammsugarens städyta från molntjänster (Onik et al, 2024).

5.2.6 Sensordata

Via sensordata i Google Home finns det möjlighet för användaren att hämta status för smarta lampor från IKEA. Genom molntjänsterna för Xiaomi Home, Netatmo och myStrom går det att hämta ut data som relaterar till temperatur, luftfuktighet, strömförbrukning och koldioxidhalter (Servida et al, 2023).

5.3 Lokal data

Arbetets första strukturerade litteraturstudie ämnar att besvara frågeställningen: *“Vilka personuppgifter samlas in av IoT-enheter i privatpersoners hem?”*. För detta har temat “Lokal data” skapats för att sortera den data som kunnat identifierats ligga lokalt på enheter eller i applikationer. Följande kategorier har upprättats för koder: Enhetsdata (5), Data mellan applikation och enhet (4), Kroppsdata (5). Teman, kategorier och tillhörande koder finns att läsa i appendix C.

5.3.1 Enhetsdata

Genom att undersöka Android- och iOS-versionen av applikationen för HIKVISION har lokala filer identifierats för att upptäcka aktiva kanaler och tillhörande namn som dessa har sparat i databasfiler. Utöver detta existerar databaser för vilka trådlösa nätverk telefonen har kopplat upp sig mot när applikationen varit i bruk, IP-adresser, användarkonton och vilka

funktioner som använts (Dragonas et al, 2023). På enheter som används med Nest Protect, Xiaomi Home, Ikea Trådfri och QBee Camera har information hämtats in genom att kopiera data som ligger på enheternas chip och innehåller unika identifierare, trådlösa nätverk och deras lösenord, serienummer, MAC-adresser, identifierare för användarkonton och konfigurationer (Servida et al, 2023).

5.3.2 Data mellan applikation och enhet

En kamera från D-Link har identifierats att kommunicera utan kryptering med sin tillhörande mobilapplikation. Information som insamlats innehåller bilddata från kameran som skickas i samband med liveströmning av video. Vidare identifieras en kamera av märket Victure skicka krypteringsnycklar för tillgång till API i klartext mellan applikation och enhet. Enheter från Vera Hub och Wansview identifierades att kommunicera mellan applikation och enhet i klartext, men ingen relevant data kunde utläsas från dessa (Wu et al, 2021).

5.3.3 Kroppsdata

Sei och Ohsuga (2023) har med hjälp av Fitbit Aria 2, Fitbit Charge 3 och kontrollen Joy-Con för spelkonsolen Nintendo Switch kunnat utmäta kroppsvärden och spara dessa lokalt. Denna data innehåller information om vikt, BMI, sömn, förbrända kalorier, hjärtrytm och steg.

5.4 Bekvämlighet

Bekvämlighet var det första temat i den andra strukturerade litteraturstudien som ämnar att besvara frågeställningen:

"Vilken medvetenhet och inställning har privatpersoner till insamlingen [av personuppgifter med IoT-enheter]?"

Totalt fanns sex kategorier tillsammans med deras respektive mängd koder, dessa är: Insamlingsmetod (6), Teknisk erfarenhet (4), Integritetsförlust (6), Interaktivitet (2), Komfort kontra integritet (3) och Minderårigas integritet (3) . Dessa kategorier detaljeras vidare i de följande kapitlen. Temat med kategorier och koder finns i appendix D.

5.4.1 Insamlingsmetod

Vilken typ av data och hur den samlas in inom hemmet påverkar hur bekväma privatpersoner är att dela med sig av informationen. Gøthesen et al. (2023) observerar i deras studie att många inte vill använda smarta högtalare då de är rädda att obehöriga ska lyssna på deras konversationer som kan innehålla känslig information. Även Lenhart et al. (2023) påtalar oron för enheter som spelar in ljud, och menar att många är oroliga för kameror som spelar in videomaterial inomhus. Windl och Mayer (2022) menar att privatpersoner är oroliga för enheter med ständigt påslagna mikrofoner och hur den data används och delas med tredje parter. Ahmad et al. (2022) menar att det existerar oro kring integritet relaterade till ljudinspelningar. Tabassum et al. (2020) påtalar även oro för ständigt påslagna mikrofoner och hur de lyssnar på konversationer.

5.4.2 Teknisk erfarenhet

Hur mycket eller lite teknisk erfarenhet visar på hur bekväma privatpersoner är med att använda IoT-enheter i hemmet. Ahmad et al. (2023) beskriver att användare antar att enhetens inbyggda mikrofon stängs av på en hårdvarunivå, även om tillverkaren nödvändigtvis har implementerat denna funktion. Deltagare i studien utförd av Lenhart et al. (2023) har noterat att teknisk kunskap och avancerad nätverksadministration krävs för att skydda sin integritet. Ifall en användare har tidigare erfarenhet av IoT-enheter inom hemmet leder det till mindre oro för integritetsförlust (Windl & Mayer, 2022; Tabassum et al., 2020).

5.4.3 Integritetsförlust

Oron för att användares integritet ska påverkas negativt korrelerar till hur bekväma de är att implementera och använda IoT-enheter inom hemmet. Lucia-Palacios och Pérez-López (2021) skriver att inkräktande funktioner mot integritet upplevs som ett bekymmer för användare. Adeyeye (2024) skriver att personer är mindre villiga att utsätta sig för potentiella integritetsintrång som påverkar deras underhållning, integritet och säkerhet inom hemmet. Albayaydh och Flechais (2024) menar att oron att förlora integritet relaterar till risker som dataläckor, datamissbruk och riktade inbrott. Major et al. (2021) påstår även att det finns stor oro för att integritetsförlust kan ske utan att personen är medveten om det, som exempelvis genom ständigt påslagna mikrofoner. Samtidigt existerar användare som förknippar IoT-enheter i hemmet med förbättrad säkerhet och anser att enhetssäkerhet ska hanteras av tillverkaren.

5.4.4 Interaktivitet

Desto mer användaren kan interagera med enheten och desto mer information som kommuniceras, bidrar till att produkten upplevs som mindre påträngade på deras integritet och att enheten upplevs som mer användbar (Lucia-Palacios & Pérez-López, 2021).

5.4.5 Komfort kontra integritet

Användare är ofta villiga att avstå integritet för att uppnå större nytta från deras IoT-enheter inom hemmet (Olabode et al., 2023; Scoccia et al., 2023; Lenhart et al., 2023). Scoccia (2023) skriver att många är villiga att ge upp känslig information för bekvämligheter oavsett potentiella problem som kan uppstå. Lenhart et al. (2023) beskriver att även om personerna påstår sig ha en hög medvetenhet om riskerna så väljer de ändå att uppoffra integritet för att nyttja fördelarna som enheterna erbjuder.

5.4.6 Minderårigas integritet

Det är viktigt att enheter ska kunna konfigureras så att minderåriga begränsas i deras interaktioner för att skydda dem från potentiella hot (Valero et al., 2023). Minderåriga förstår inte nödvändigtvis hur enheterna fungerar på samma sätt som vuxna (Valero et al., 2023; Turner et al., 2022). Studien av Turner et al. (2022) visar att minderåriga inte alltid förstår att IoT-enheter är uppkopplade till internet.

5.5 Förtroende

Förtroende var det andra temat i den andra strukturerade litteraturstudien som ämnar att besvara frågeställningen:

"Vilken medvetenhet och inställning har privatpersoner till insamlingen [av personuppgifter med IoT-enheter]?"

Totalt fanns tre kategorier tillsammans med deras respektive mängd koder, dessa är: Förtroende för märke (12) och Förtroende för teknologin (4). Dessa kategorier detaljeras vidare i de följande kapitlen. Temat med kategorier och koder finns i appendix E.

5.5.1 Förtroende för märke

Förtroendet som användaren har till märket visar sig ha en stor betydelse i hur bekväma de är att implementera IoT-enheter i hemmet (Lucia-Palacios & Pérez-López, 2021; Turner et al., 2023; Paupini et al., 2022; Gøthesen et al., 2023; Lenhart et al., 2023; Ogunniye & Kokciyan, 2023). En deltagare i studien som genomfördes av Paupini et al. (2022) menar att de inte litar på stora företag för att de inte vet vad de kommer att använda deras personuppgifter till, samt att de inte heller litar på småföretag för dessa troligen inte har implementerat tillräckliga säkerhetsprocesser. I undersökningen som genomfördes av Lenz et al. (2023) uttrycker deltagare större oro över hur personuppgifter lagras än hur dessa samlas in. I en separat studie hävdar flera deltagare att det existerar för lite information om produkternas funktioner för att kunna lita på leverantören (Turner et al., 2022). Privatpersoner anser att företag bör förhålla sig till relevanta lagar för datahantering och att regeringar ska involvera sig i frågan (Albayaydh & Flechais, 2024).

5.5.2 Förtroende för teknologin

Huruvida användaren har förtroende för hur teknologin bakom en produkt fungerar är en faktor som påverkar hur villiga de är att använda IoT-enheter i hemmet. Förtroendet i sin tur är ofta baserat på deras kunskap och oro för integritetsförlust (Adeyeye, 2024; Scoccia et al., 2023; Ahmad et al., 2022). Scoccia et al. (2023) menar att privatpersoner som har högre oro för att deras integritet skulle påverkas, sannolikt inte implementerar IoT-enheter i deras hem. Personer som är villiga att införskaffa billiga produkter förstår inte nödvändigtvis riskerna med att använda dessa i hemmet (Turner et al., 2022).

5.6 Medvetenhet

Förtroende var det andra temat i den andra strukturerade litteraturstudien som ämnar att besvara frågeställningen:

"Vilken medvetenhet och inställning har privatpersoner till insamlingen [av personuppgifter med IoT-enheter]"

Totalt fanns fem kategorier tillsammans med deras respektive mängd koder, dessa är: Integritetsmedvetenhet (4), Datahanteringsmedvetenhet (3), Konfigurationsmedvetenhet (5), Likgiltighet (7) och Gästmedvetenhet (3). Dessa kategorier detaljeras vidare i de följande kapitlen. Temat med kategorier och koder finns i appendix F.

5.6.1 Integritetsmedvetenhet

Medvetenhet om hur privatpersoners integritet kan påverkas spelar in på vilka risker som användarna utsätts för gällande IoT-enheter i hemmet (Al Muhander et al., 2023; Turner et al., 2022; Ogunniye & Kokciyan, 2023; Tabassum et al., 2020). Tabassum et al. (2020) skriver att risker mot integritet är en motiverande faktor för användare när det gäller att införskaffa röstassistenter som har ständigt påslagna mikrofoner. Att tillverkarna av IoT-enheter inom hemmet meddelar de potentiella riskerna som uppstår mot användares integritet är en viktig faktor för att tillåta dem att göra mer informerade beslut kring införskaffandet av dessa enheter (Ogunniye & Kokciyan, 2023). Al Muhander et al. (2023) menar att kommunikationen kring de potentiella riskerna måste göras på ett sätt som är enkelt för användaren att förstå.

5.6.2 Datahanteringsmedvetenhet

Turner et al. (2022) skriver att de individer som intervjuades har en viss förståelse för hur IoT-enheter ökade insamlingen av data i hemmet och hur detta kan leda till potentiella risker. Meng et al. (2021) visar även i deras studie privatpersoners oro för hur data hanteras och otillräcklig transparens utövas av företagen. En av deltagarna i studien av Chhetri och Genaro Motti (2022) beskriver att de hade önskat att det fanns något sätt att kontrollera den data som överförs och vart den lagras.

5.6.3 Konfigurationsmedvetenhet

Hur IoT-enheter i hemmet kan konfigureras för att skydda deras integritet upplevs ofta som krångligt av många användare, medan andra inte vet att möjligheten finns alls (Major et al., 2021). I sin studie fann Chhetri och Genaro Motti (2022) att deltagarna förespråkade för instruktioner för att konfigurera sina enheter så att de slipper be om hjälp från någon professionell. Saura et al. (2021) skriver att de standardinställningar som finns på IoT-enheter inom hemmet bör prioritera en balans mellan tjänstens kvalitet och skydd för personuppgifter. Ahmad et al. (2022) beskriver att fysiska kontroller för att stänga av enheters avlyssningsfunktion var något som visade på att öka användarens uppfattning av pålitligheten av enheten, och därmed öka dess förtroende för den.

5.6.4 Likgiltighet

Adeyeye (2024) skriver att många deltagare i deras studie känner att deras personliga information redan finns tillgänglig för andra och att de därmed inte har någon kontroll över den. I en studie av Scoccia et al. (2023) observerades recensioner av applikationer för att kontrollera IoT-enheter i hemmet, fann de att väldigt få var fokuserade kring integritet eller säkerhet. Oavsett hur användarna känner kring hur deras integritet hanteras, måste de acceptera användarvillkoren som kan inkludera datainsamling för att kunna utnyttja enheterna (Turner et al., 2022).

5.6.5 Gästmedvetenhet

När det kommer till gäster i hemmet har de inte samma kontroll som ägaren av IoT-enheterna, vilket gör att deras möjligheter att påverka de risker som de kan utsättas för

minskar (Chhetri & Genaro Motti, 2022; Albayaydh & Flechais, 2024). Privatpersoner använder oftast ett enda konto för att styra enheterna i hemmet, istället för att göra separata konton för övriga i hushållet (Albayaydh & Flechais, 2024).

6 Diskussion

Detta kapitel diskuterar arbetets processer, resultat och slutsatser. Samt presenterar en diskussion för vilka ämnen som är av intresse för fortsatt arbete.

De två strukturerade litteraturstudierna gjordes i syfte att besvara frågeställningen:

"Vilka personuppgifter samlas in av IoT-enheter i privatpersoners hem och vilken medvetenhet och inställning har privatpersoner till insamlingen?"

Utifrån den kvalitativa analysen hittades sex stycken teman: Datatyp, Molndata, Lokal data, Bekvämlighet, Förtroende och Medvetenhet. Syftet med två studier var att frågeställningen var tvåfaldig, och med denna metod kan de två olika infallsvinklarna utforskas separat, för att sedan triangulera den data som uppstått.

6.1 Datainsamling

Resultaten som presenterats i flera artiklar tyder på att en mängd smarta enheter som kan existera i ett hem kan hämta in olika data om användaren och spara dessa lokalt eller på molntjänster. I den första litteraturstudiens alla tre teman var enhetsdata mest förekommande och inkluderar detaljer som MAC- och IP-adresser, serienummer och enhetsnamn (Dragonas et al, 2023; Wu et al, 2021; Servida et al, 2023). I denna kontext är det dock viktigt att belysa att dessa uppgifter inte nödvändigtvis klassas som personuppgifter av gemene person. Däremot kan privatpersoner utsättas för ytterligare risker om uppgifterna hanteras med illvilja. Exempelvis genom att via identifierad enhet hitta ytterligare hål i hemnätverket för att få tillgång till personuppgifter. Detta möjliga hot ligger därmed i parallell med Geneiatakis et al. (2014) påstående att flera leverantörer delegerar säkerhet till nätverkets övriga enheter som exempelvis en router.

Bilddata var även en återkommande kategori som innefattar både still- och rörliga bilder. Dessa uppgifter ser ut att främst användas för navigation och övervakning i olika former (Onik et al, 2024; Calacci et al, 2022; Wu et al, 2021; Servida et al, 2023). I vissa fall har bilddata skickats utan kryptering. I ett fall identifierades krypterade bilddata där filnamn har beskrivit objekt i bilden. Data i dessa former kan möjligtvis användas för att kartlägga privatpersoners hem och de objekt som finns där i, samt personer som lever i hushållet. Utöver detta existerar data som tyder på att det finns en vilja från privatpersoner att delta i övervakning om de anser att detta gör deras grannskap säkrare. Via tjänster som Ring Neighbours kan personuppgifter inte bara sparas om enhetens ägare, utan data som härstammar från förbipasserande eller besökare. Samtidigt är det enhetens ägare som i slutändan gör bedömning om vilka uppgifter som laddas upp på plattformen. För förbipasserande kan det därför vara omöjligt att veta vilka bilder som laddas upp på tjänsten.

För röstassistenter sparas data relaterat till konversationer och röstprofiler i molnet av enheter från diverse märken (Valero et al., 2023). Ett löpande tema i denna kategori av data tyder på att bestå av att användaren antingen behöver ställa in automatisk borttagning av den data som sparas, alternativt att manuellt ta bort den data som sparas regelbundet. En möjlig fråga för hur denna typ av data behandlas av leverantören och privatpersoner är huruvida regelbundna interaktioner via skärmar spelar roll. Eftersom en röstassistent sällan besitter en egen skärm är det möjligt att den enda interaktionen via skärm sker vid initial konfiguration av assistenten med hjälp av mobiltelefon eller surfplatta. Vidare är det möjligt att det kan för gemene användare vara svårt att kontrollera ytterligare inställningar relaterade till integritet

på en röstassistent utan en extern enhet eller skärm.

6.2 Medvetenhet och inställning

Av de studerade artiklarna framkommer det att användarens bekvämlighet, förtroende och medvetenhet gällande datainsamling varierar utifrån flera faktorer. Vilken typ av data och hur de hanteras har en viss effekt. Ljud- och bilddata var något som noterades extra känsligt för användarna. Windl och Mayer (2022) skriver om hur privatpersoner är oroliga att enheter med ständigt påslagna mikrofoner spelar in deras konversationer och delar denna data med tredje parter. Detta är av särskild vikt när det gäller data rörande minderåriga. Huruvida personen är medveten om själva datainsamlingen spelar även in, då det finns stor oro för att data spelas in utan deras medvetenhet (Major et al., 2021). De risker som personer utsätts för gällande integritet är något som influerar huruvida de vill implementera och använda IoT-enheter i hemmet. Den här effekten mildras dock till viss del av användarens förtroende för företaget och teknologin som ligger till grund för IoT-enheten. Användare väljer att lägga sin tillit till företaget för att upprätthålla en säker hantering av integritet och säkerhet, dock utan att utföra några metoder för att säkerhetsställa att detta faktiskt sker. Det ska även poängteras att privatpersoner som visar högre oro för integritetsförlust kommer möjligtvis inte att implementera IoT-enheter i deras hem (Scoccia et al., 2023). Detta kan eventuellt visa på ett mörkertal, då dessa personer inte representeras i tillgänglig data. Även hur interaktiv enheten är kan ha en positiv effekt på bekvämligheten, då privatpersonen upplever att denna kan skapa sin egen upplevelse.

En annan faktor som påverkar upplevelsen av IoT-enheter är tidigare erfarenhet av dessa produkter. Oron för integritetsförlust sjunker i samband med den tid en person spenderar med IoT-enheter i hemmet (Windl & Mayer, 2022; Tabassum et al., 2020). Detta visar att mer tidigare erfarenhet inte nödvändigtvis innebär att användarna implementerar mer skyddsåtgärder. De som redan äger enheter kommer även med större sannolikhet att tillåta fler enheter, vilket potentiellt kan leda till ytterligare risker för integriteten. Utöver erfarenhet är även teknisk kompetens en viktig faktor. Deltagare i studien gjord av Lenhart et al. (2023) noterar att teknisk erfarenhet är ett krav för att skydda sig inom hemmet. Detta kan tyda på att oerfarna användare upplever teknologin som komplicerad och därmed löper risker genom att använda den. Det finns tecken på att användare inte har full förståelse för hur deras personuppgifter behandlas och därmed löper risken att utsättas för integritetskränkning. Detta tillsammans med att användare visar större oro för hur data faktiskt lagras av företag visar på att det potentiellt är ett mångfacetterat problem. Detta är på grund av att både inspelning, överföring och lagring är något som upplevs som diffust hos användare. Även om det finns inställningar i syfte att skydda integriteten hos användaren är det inte nödvändigtvis så att de vet om det, eller att de vill lägga tiden för att sätta sig in i det.

Komfort kontra integritet är titeln på denna studie och även detta är en viktig aspekt att diskutera utifrån privatpersoners medvetenhet och inställning till IoT-enheter. Studien av Olabode et al. (2023) visar att användare bortser deras integritet för att istället främja deras komfort och ha större nytta av de enheter de använder. Detta gäller även för personer som påstår sig ha högre medvetenhet om vilka risker mot integritet som finns (Lenhart et al., 2023). Detta visar på att användare medvetet väljer bort sin egen integritet för att ta del av olika bekvämligheter som de IoT-enheter kan erbjuda. I kontrast visar studien av Adeyeye (2024) att användare upplever en konflikt då de blir mindre villiga att utsätta sig för integritetsintrång när det påverkar deras underhållning, integritet och säkerhet. Skillnaden i

dessa studier kan potentiellt förklaras utifrån typ av produkt. Användaren väger deras behov samt nyttan av enheten gentemot deras integritet. Slutligen är det många användare som upplever en likgiltighet till huruvida deras personuppgifter samlas in. Detta då de känner att deras personliga information redan finns tillgänglig på platser och därmed upplever att deras individuella förmåga att hantera detta redan är förbrukad (Adeyeye, 2024).

6.3 Sammanställning

"Bilddata" är den näst mest förekommande typen av insamlad data, där bild och video har kunnat inhämtas lokalt eller från molnet tagna av enheter som robotdammsugare, övervakningskameror och ringklockor (Onik et al, 2024; Calacci et al, 2022; Wu et al, 2021; Servida et al, 2023). Vid användningen av många enheter är det upp till användaren om bild- och videodata ska delas ut på tjänster som fungerar likt sociala nätverk. Ring Neighbours, till exempel, är en tjänst som bidrar med en plattform där användare själva väljer att delta i videoövervakning där detta potentiellt delas till rättsmyndigheter (Calacci et al, 2022). Många IoT-enheter erbjuder möjligheten att konfigurera alternativ för insamlande av personuppgifter. Dessa konfigurationsmöjligheter är dock inte användarna nödvändigtvis medvetna om, eller så upplevs dessa inställningar som komplicerade (Major et al., 2021). Samtidigt existerar enheter som kommunicerar bilder och video mellan applikation och enhet utan kryptering (Wu et al., 2021). Bild- och videodata som lagras av IoT-enheter i hemmet utgör ett orosmoment för privatpersoner (Lenhart et al., 2023). Denna kombinerade insamlade data tyder på att de orosmoment som existerar är grundade i det sätt som data faktiskt hanteras. Möjligheten att påverka sin situation finns på vissa enheter, men är inte alltid en självklarhet. Även om det finns, ställer det ofta tekniska krav på användaren att skydda sig mot potentiella risker. Hur dessa krav förmedlas till användaren är dock ofta komplicerade. Albayaydh och Flechais (2024) beskriver hur de användaravtal som är kopplade till datainsamling är fördelaktiga för leverantörer och lägger mindre fokus kring användaren, vilket leder till acceptans av påträngande villkor. Oavsett hur de ser på användarvillkoren och hur deras förståelse av hur personuppgifter kan användas måste de dessutom acceptera dessa användarvillkor för att utnyttja enheterna (Turner et al., 2022). I slutändan spelar det alltså ingen roll hur medvetna eller tekniskt kunniga personerna är. Teknisk erfarenhet skapar därmed en barriär för användare att kunna utnyttja IoT-enheter inom hemmet på ett säkert sätt som inte innebär risker för deras integritet.

Vidare existerar data för en enhet som använder odokumenterade kommandon för att hämta ut information som kan användas för att kartlägga en persons hemmiljö (Onik et al., 2024). Ett orosmoment för användare är hur data kan läcka och hur det kan leda till datamissbruk och riktade inbrott (Albayaydh & Flechais, 2024). Detta är potentiellt problematiskt då många användare lägger tillit till tillverkaren att upprätthålla säkerheten och integritetsskydd i enheterna (Scoccia et al., 2023), medan det inte finns något som tyder på att användare själva verifierar detta.. Detta kan upplevas bli än mer komplicerat när användaren själv blir ansvarig för att regelbundet ta bort data från molntjänster (Valero et al., 2023). Särskilt då många inte förstår att data sparas permanent och delas externt. Det existerar även indikationer på att användare nödvändigtvis inte förstår vilka personuppgifter som IoT-enheter behandlar och hur de lagras (Meng et al., 2021). Då olika former av data sparades både på molntjänster och lokalt hittades ingen tydlig korrelation. Insamlade uppgifter ser ut att framstå mestadels av enhetsdata, det vill säga, exempelvis MAC-adresser, IP-adresser och serienummer (Wu et al., 2021; Servida et al., 2023; Dragonas et al., 2023; Onik et al., 2024). Avsaknad av data på huruvida privatpersoner anser att dessa uppgifter är

kritiska eller inte tyder på att användare inte anser dessa som viktiga, eller att ett mörkertal existerar. Än en gång ställs det tekniska krav på användaren för att skydda sig själv.

6.4 Etiska- och samhällsaspekter

Då arbetets syfte bestått av att kartlägga nuvarande teknologi finns det möjlighet för aktörer med oetiska mål att utnyttja den data som har kartlagts för att hitta och utnyttja tekniska misstag och säkerhetshål i produkter som används i hemmet. Detta kan potentiellt användas för ekonomiska vinster, integritetsintrång och kartläggning av privatpersoner.

6.5 Begränsningar i arbetsprocessen

Under arbetsprocessen där källor identifierades noterade arbetets författare en avvikelse i antalet artiklar som fanns tillgängliga till respektive strukturerade litteraturstudie. Detta ledde till att mängden koder som samlades in till vardera studie även skilde i mängd. Detta gör att den andra litteraturstudien erhåller större vetenskaplig basis än den första. Valet av databaser för båda strukturerade litteraturstudier var: ACM, ScienceDirect, IEEE Xplore och Web of Science. Det var stor skillnad i mängden resultat för båda studier gällande antalet träffar, där både ACM och ScienceDirect hade anmärkningsvärt större mängd artiklar till skillnad från IEEE Xplore och Web of Science. Något som båda arbetets författare upplevde som märkligt var att slutresultaten inte inkluderade någon träff hos IEEE Xplore eller Web of Science. Utifrån personlig erfarenhet har IEEE Xplore tidigare varit en återkommande källa till arbeten gällande IT och informationssäkerhet, vilket upplevdes som förvånande då en låg resultatmängd erhölls. Då arbetets författare har haft tillgång till resurser från Högskolan i Skövde medförde det tillgång till artiklar som potentiellt kan vara bakom betalvägg. Därför har valet att använda Open Access använts på de databaser där det varit applicerbart. IEEE Xplore, Web of Science och ScienceDirect låter användaren applicera sådana filter. Detta kan ha medfört att antalet artiklar som inkluderats har minskat vilket kan ha resulterat i en reducerad provstorlek.

Efter att inkluderings- och exkluderingskriterier applicerades på sökningarna, importerades resultaten till verktyget Rayyan. Båda hade liknande mängd resultat att manuellt gå igenom, 1046 respektive 940, vilket gjorde den manuella sorteringen likvärdig för båda. Detta genomfördes med att läsa igenom titlar, sammanfattning och nyckelord från artiklar och välja ut ifall de skulle inkluderas, exkluderas eller vara obestämda utifrån de förutbestämda kriterierna. Genom att i första hand gå på titlar och sammanfattning har detta kunnat resultera i exkludering då dessa inte nödvändigtvis representerar artikeln i sin helhet. De artiklar som var obestämda granskades efteråt noggrannare med en fullständig genomläsning.

Under arbetets gång har arbetets författare föreslagit och implementerat förbättringar som har effektiviserat särskilda arbetsprocesser. Arbetets författare har evaluerat och bidragit med perspektiv på varandras källor och gjort en kvalitetsgranskning av materialet. Med metoden som detaljeras i Figur 2, har de två sista stegen i utförandefasen itererats av den andre personen i syfte att utföra en bedömning på kvalitén och analysera den data som samlats. Enligt Kitchenham (2004) är det viktigt att den data som inhämtas hanteras på ett konsekvent sätt och att den granskas av en annan person. Detta valde vi att tolka som att den andra författaren i arbetet utförde detta, men processen hade kunnat förbättras om ytterligare personer fanns tillgängliga för evaluering. Evalueringsprocessen hade potentiellt

kunnat förbättras med användandet av en reliabilitetsmetod som exempelvis Cohens Kappa. Detta hade lett till att en mer standardiserad process för hur artiklar evaluerades och valdes ut för de strukturerade litteraturstudierna och redovisat processen för läsaren på ett mer transparent sätt.

6.6 Resultat jämfört med tidigare forskning

Ogonji et al. (2020) har genom en strukturerad litteraturstudie identifierat ett flertal utmaningar relaterade till integritet och nätverkssäkerhet i relation till IoT-enheter. Platsdata identifieras som ett problem när uppgifterna inte hanteras på ett säkert sätt, eller när användaren inte har möjlighet att kontrollera den platsdata som hämtas in, vilket är en trend som observeras i detta arbete. Vidare identifieras uppgifter som sparas på enheten av personer i anslutning till denna som problematiskt. Eftersom enheten kan delas mellan flera individer eller säljas begagnade kan också uppgifterna som lagras på denna bli tillgänglig för obehöriga. I detta arbete har data inhämtats som stöder denna trend, då ett flertal enheter har identifierats som sparar uppgifter om användaren på lokal nivå.

Olabode et al. (2023) utförde en strukturerad litteraturstudie med syftet att kartlägga forskningen som finns kring olika risker och svagheter inom IoT-enheter i hemmet. Integritet, säkerhet och välmående för privatpersoner är de huvudområden som täcks, och de teman som identifieras som framväxande är “risker”, “svagheter” och “skador” i relation till smarta enheter inom hemmet. De noterar att den litteratur som finns gällande smarta hem fokuserar mycket på teknologi, medan det finns ett underskott på artiklar som undersöker detta från ett beteendevetenskapligt eller humanitärt perspektiv. Denna trend stöds inte av detta arbete då den första studien erhöll en lägre mängd data än den andra. Denna artikel användes i den andra strukturerade litteraturstudien i detta arbete, då den visade på hur IoT-enheter upplevs från ett användarperspektiv, istället för enbart att lista olika tekniska detaljer.

6.7 Fortsatt arbete

Ytterligare arbete bör bedrivas för att samla in mer information om vilka personuppgifter IoT-enheter samlar in från ett tekniskt perspektiv. Detta arbete bör också involvera var uppgifterna sparas, hur de transporteras och vilken form uppgifterna tar. Vidare bör det också bedrivas arbeten som fokuserar på vilka uppgifter som privatpersoner anser är känsliga, då det i dagsläget finns svårigheter att avgöra om uppgifter om enheter betraktas som kritiska för privatpersoner.

Under arbetets gång dök flera artiklar upp angående insamling av personuppgifter kombinerat med AI-lösningar som exempelvis ansiktsigenkänning och för att förutse vissa hälsorisker som potentiellt kan läsas ut med hjälp av smarta klockor. Då artificiell intelligens byggs med hjälp av insamlade uppgifter skulle framtida arbete kunna utforska IoT-enheters insamling av personuppgifter, kombinerat med AI-lösningar för att kontrollera huruvida dessa påverkar insamlingen och privatpersoners medvetenhet om teknologin som används för att behandla insamlad data.

Med tanke på att allt fler minderåriga använder IoT-enheter i hemmet är det viktigt att profiler med begränsad funktionalitet skapas för att skydda dem (Valero et al., 2023). Även om det finns konfigurationsmöjligheter för detta, är det helt upp till målsmäns tekniska förmåga att begränsa detta (Valero et al, 2023) och därmed kan det behövas mer klarhet i hur

minderåriga kan skyddas ytterligare.

Det finns en obalans mellan ägaren av IoT-enheter och de som är bosatta med personer när det gäller att konfigurera integritetsinställningar av enheter (Albayaydh & Flechais, 2024). Detta är något som skulle kunna utforskas vidare för att se hur personer som bor i samma hem kan gemensamt styra över den data som samlas in. Ytterligare kan påverkan på gäster i ett hem undersökas för att få bättre uppfattning av hur omfattande integritetsförlust är.

Till sist kan det finnas skäl att genomföra en studie som berör de ämnen som detta arbete belyser via alternativa metoder. Då en strukturerad litteraturstudie är beroende av data som redan existerar kan fortsatt arbete därför bestå av exempelvis intervjustudier eller enkätstudier som inhämtar ytterligare data från personer angående deras medvetenhet och inställning till de personuppgifter som inhämtas av IoT-enheter i hemmet. Detta kan bidra med ytterligare perspektiv och tillåta att mer specifika frågor kan ställas för att samla in mer data inom forskningsämnet.

7 Slutsats

Utifrån de studier som har genomförts i detta arbete kan vissa slutsatser dras. IoT-enheter samlar in en rad olika typer av data, där personuppgifter kan vara inkluderade. Huvudsakligen gäller det “Enhetsdata”, “Bilddata”, “Röstdata” och “Kroppsdata”. Gällande privatpersoners medvetenhet och inställning till denna insamling är resultaten mer komplexa. Oro för integritetsförlust är brett förekommande hos användare, dock varierar tyngden av denna oro utifrån vad som orsakar den, till exempel typ av data, om minderåriga omfattas i insamlingen och hur det delas med tredje parter. Möjligheten att skydda sin integritet framstår direkt relaterad till erfarenhet och teknisk kompetens. Det kan avse till att kunna konfigurera sin enhet eller förstå användarvillkor. Detta kan potentiellt medföra ett problem, då teknisk kompetens inte enkelt kan kvantifieras eller generaliseras. IoT-enheter är djupt integrerade i vårt samhälle och fortsätter att öka. Med robotdammsugare, smarta klockor och säkerhetskameror i allt fler hem har vi svårt att kontrollera vilka uppgifter som insamlas, vare sig det är data gällande en själv, sitt barn eller grannen som hälsar på.

Referenser

Acar, A., Tuncay, G. S., Luques, E., Oz, H., Aris, A., & Uluagac, S. (2024). 50 shades of support: A device-centric analysis of Android Security updates. *Proceedings 2024 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2024.24175

ACM. (u.å.). *ACM Digital Library An Archive of Original Research*. Hämtad 25 maj, 2024, från https://www.acm.org/publications/digital-library

Adeyeye, K. (2024). Controlling the 'elephant in the room': A new protocol for sharing data from Home Performance Monitoring Systems. *Technology in Society*, *76*, 102478. https://doi.org/10.1016/j.techsoc.2024.102478

Ahmad, I., Akter, T., Buher, Z., Farzan, R., Kapadia, A., & Lee, A. J. (2022). Tangible privacy for smart voice assistants: Bystanders' perceptions of physical device controls. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1–31. https://doi.org/10.1145/3555089

Albayaydh, W., & Flechais, I. (2024). "Innovative technologies or Invasive Technologies?": Exploring design challenges of privacy protection with smart home in Jordan. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 1–54. https://doi.org/10.1145/3637353

Al Muhander, B., Wiese, J., Rana, O., & Perera, C. (2023). Interactive Privacy Management: Toward enhancing privacy awareness and control in the internet of things. *ACM Transactions on Internet of Things*, *4*(3), 1–34. https://doi.org/10.1145/3600096

Amazon. (u. å.). *Alexa and Alexa Device FAQs*. Help & Customer Service. Hämtad 10 april, 2024, från https://www.amazon.com/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=G201602230

Belli, L., Schwartz, M., & Louzada, L. (2017). Selling your soul while negotiating the conditions: From notice and consent to data control by design. *Health and Technology*, *7*(4), 453–467. https://doi.org/10.1007/s12553-017-0185-3

Biswas, A. R., & Giaffreda, R. (2014). IOT and cloud convergence: Opportunities and challenges. *2014 IEEE World Forum on Internet of Things (WF-IoT)*. https://doi.org/10.1109/wf-iot.2014.6803194

Calacci, D., Shen, J. J., & Pentland, A. (2022). The cop in your Neighbor's doorbell: Amazon Ring and the spread of participatory mass surveillance. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1–47. https://doi.org/10.1145/3555125

Chhetri, C., & Genaro Motti, V. (2022). User-centric privacy controls for Smart Homes. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1–36.

https://doi.org/10.1145/3555769

Clarivate. (u.å.). *About us*. Hämtad 25 maj, 2024, från https://clarivate.com/webofsciencegroup/about-us/

Colbjørnsen, T. (2020). The streaming network: Conceptualizing distribution economy, technology, and power in streaming media services. *Convergence: The International Journal of Research into New Media Technologies*, *27*(5), 1264–1287. https://doi.org/10.1177/1354856520966911

Ding, J., Nemati, M., Ranaweera, C., & Choi, J. (2020). IOT connectivity technologies and applications: A survey. *IEEE Access*, *8*, 67646–67673. https://doi.org/10.1109/access.2020.2985932

Dorsemaine, B., Gaulier, J.-P., Wary, J.-P., Kheir, N., & Urien, P. (2015). Internet of Things: A Definition & Taxonomy. *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*. https://doi.org/10.1109/ngmast.2015.71

Dragonas, E., Lambrinoudakis, C., & Kotsis, M. (2023). IOT forensics: Analysis of a HIKVISION's mobile app. *Forensic Science International: Digital Investigation*, *45*, 301560. https://doi.org/10.1016/j.fsidi.2023.301560

Dworkin, S. L. (2012). Sample size policy for qualitative studies using in-depth interviews. Archives of Sexual Behavior, 41(6), 1319–1320. https://doi.org/10.1007/s10508-012-0016-6.

Elsevier. (u.å.). *ScienceDirect: Elsevier's premier platform of peer-reviewed scholarly literature*. Hämtad 25 maj, 2024, från https://www.elsevier.com/products/sciencedirect

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 94/46/EG (allmän dataskyddsförordning). *Europeiska unionens officiella tidning*, L 119/1, 4 maj 2016, s. 1-88. https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32016R0679

Ferraris, D., Bastos, D., Fernandez-Gago, C., & El-Moussa, F. (2020). A trust model for popular Smart Home Devices. *International Journal of Information Security*, *20*(4), 571–587. https://doi.org/10.1007/s10207-020-00519-2

Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017). Security and privacy issues for an IOT based Smart Home. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. https://doi.org/10.23919/mipro.2017.7973622

Google. (u. å). *Cloud-to-cloud | Google home developers*. Cloud-to-cloud. Hämtad 5 April, 2024, från https://developers.home.google.com/cloud-to-cloud

Google. (2022, 11 maj). *FAQs on privacy: Google Nest*. Google Nest Help. Hämtad 5 april, 2024, från https://support.google.com/googlenest/answer/9415830?hl=en&ref_topic=7173611&sjid=7865583226551762728-EU

Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today*, *24*(2), 105–112. https://doi.org/10.1016/j.nedt.2003.10.001

Gøthesen, S., Haddara, M., & Kumar, K. N. (2023). Empowering homes with intelligence: An investigation of smart home technology adoption and usage. *Internet of Things*, *24*, 100944. https://doi.org/10.1016/j.iot.2023.100944

Home Assistant. (u.å..). *Installation*. Home Assistant. Hämtad 25 maj, 2024, från https://www.home-assistant.io/installation/

Home Assistant. (u.å.). *Integrations*. Home Assistant. Hämtad 25 maj, 2024, från https://www.home-assistant.io/integrations/

Huang, D. Y., Apthorpe, N., Li, F., Acar, G., & Feamster, N. (2020). IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *4*(2), 1–21. https://doi.org/10.1145/3397333

Hwang, K., Choi, B.-J., & Kang, S. (2010). Enhanced self-configuration scheme for a robust Zigbee-based home automation. IEEE Transactions on Consumer Electronics, 56(2), 583–590. https://doi.org/10.1109/tce.2010.5505974

IEEE. (u.å.). *About IEEE Xplore*. IEEE Xplore Resources and Help. Hämtad 25 maj, 2024, från https://ieeexplore.ieee.org/Xplorehelp/overview-of-ieee-xplore/about-ieee-xplore

Karale, A. (2021). The challenges of IOT addressing security, ethics, privacy, and laws. *Internet of Things*, *15*, 100420. https://doi.org/10.1016/j.iot.2021.100420

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33(2004), 1–26.

Lenhart, A., Park, S., Zimmer, M., & Vitak, J. (2023). "You shouldn't need to share your data": Perceived privacy risks and mitigation strategies among privacy-conscious smart home power users. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW2), 1–34. https://doi.org/10.1145/3610038

Lenz, J., Bozakov, Z., Wendzel, S., & Vrhovec, S. (2023). Why people replace their aging Smart Devices: A push–pull–mooring perspective. *Computers & Security*, *130*, 103258. https://doi.org/10.1016/j.cose.2023.103258

Lucia-Palacios, L., & Pérez-López, R. (2021). Effects of home voice assistants' autonomy on instrusiveness and usefulness: Direct, indirect, and moderating effects of

interactivity. *Journal of Interactive Marketing*, *56*, 41–54. https://doi.org/10.1016/j.intmar.2021.03.005

Major, D., Huang, D. Y., Chetty, M., & Feamster, N. (2021). Alexa, who am I speaking to?: Understanding users' ability to identify third-party apps on Amazon alexa. *ACM Transactions on Internet Technology*, *22*(1), 1–22. https://doi.org/10.1145/3446389

Meng, N., Keküllüoğlu, D., & Vaniea, K. (2021). Owning and sharing. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW1), 1–29. https://doi.org/10.1145/3449119

Myndigheten för samhällsskydd och beredskap. (u, å) *Termbanken för informationssäkerhet*. Hämtad 21 februari, 2024, från https://termbanken.informationssakerhet.se/

Norrgrann, K., Mohlin, L., Aschberg, R. (2022, 31 mars). "Ingen ska behöva bli filmad så i sitt eget hem". Aftonbladet. https://www.aftonbladet.se/nyheter/a/rEJX38/tidigare-anstallda-pa-verisure-berattar-bilder-av-nakna-kunder-cirkulerade-internt-200-sekunder-granskar

noyb. *GDPR: A culture of non-compliance?*. GDPR: a culture of non-compliance? (2024, 28 januari). Hämtad 15 april, från https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance.pdf

Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of internet of things. *Computer Science Review*, *38*. https://doi.org/10.1016/j.cosrev.2020.100312

Ogunniye, G., & Kokciyan, N. (2023). A survey on understanding and representing privacy requirements in the internet-of-things. *Journal of Artificial Intelligence Research*, *76*, 163–192. https://doi.org/10.1613/jair.1.14000

Olabode, S., Owens, R., Nijia Zhang, V., Copilah-Ali, J., Kolomeets, M., Wu, H., Malviya, S., Markeviciute, K., Spiliotopoulos, T., Neesham, C., Shi, L., & Chambers, D. (2023). Complex online harms and the Smart Home: A scoping review. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4377201

Onik, A. R., Alsmadi, R., Baggili, I., & Webb, A. M. (2024). So fresh, so clean: Cloud forensic analysis of the Amazon iRobot Roomba Vacuum. *Forensic Science International: Digital Investigation*, *48*, 301686. https://doi.org/10.1016/j.fsidi.2023.301686

Open Home Foundation. (u.å.). *About the Open Home Foundation*. About the Open Home Foundation – Open Home Foundation. Hämtad 25 maj, från https://www.openhomefoundation.org/about/

Paré, G., Kitsiou, S. (2017) Methods for Literature Reviews, Handbook of eHealth Evaluation: An Evidence-based Approach, *University of Victoria*. Hämtad 3 Mars,

2024, från https://www.ncbi.nlm.nih.gov/books/NBK481583/

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, *52*(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008

Paupini, C., Van der Zeeuw, A., & Fiane Teigen, H. (2022). Trust in the institution and privacy management of internet of things devices. A comparative case study of Dutch and Norwegian households. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4031364

Samuel, S. S. (2016). A review of connectivity challenges in IOT-Smart Home. *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*. https://doi.org/10.1109/icbdsc.2016.7460395

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2021). Setting privacy "by default" in social IOT: Theorizing the challenges and directions in Big Data Research. *Big Data Research*, *25*, 100245. https://doi.org/10.1016/j.bdr.2021.100245

Sei, Y., & Ohsuga, A. (2023). Data collection of biomedical data and sensing information in Smart Rooms. *Data in Brief*, *47*, 108922. https://doi.org/10.1016/j.dib.2023.108922

Servida, F., Fischer, M., Delémont, O., & Souvignet, T. R. (2023). OK google, start a fire. IOT devices as witnesses and actors in fire investigations. *Forensic Science International*, *348*, 111674. https://doi.org/10.1016/j.forsciint.2023.111674

Sharif, H. U., Mohammed, M. A. (2022). A literature review of financial losses statistics for Cyber Security and future trend. *World Journal of Advanced Research and Reviews*, *15*(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0573

Shayegh, P., & Ghanavati, S. (2017). Toward an approach to privacy notices in IOT. *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*. https://doi.org/10.1109/rew.2017.77

Scoccia, G. L., Eramo, R., & Autili, M. (2023). Studying users' perception of IOT mobile companion apps. *Pervasive and Mobile Computing*, *92*, 101786. https://doi.org/10.1016/j.pmcj.2023.101786

Tabassum, M., Kosiński, T., Frik, A., Malkin, N., Wijesekera, P., Egelman, S., & Lipford, H. R. (2020). Investigating users' preferences and expectations for always-listening voice assistants. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *3*(4), 1–23. https://doi.org/10.1145/3369807

Turner, S., Pattnaik, N., Nurse, J. R. C., & Li, S. (2022). "You just assume it is in there, I guess": Understanding UK families' application and knowledge of Smart Home Cyber Security. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1–34. https://doi.org/10.1145/3555159

Turner, S., Tanczer, L., & Neubauer, L. (2023). *In Principle vs in Practice: User, Expert and Policymaker Attitudes towards the Right to Data Portability in the Internet of Things*. https://doi.org/10.2139/ssrn.4486266

Valero, C., Pérez, J., Solera-Cotanilla, S., Vega-Barbas, M., Suarez-Tangil, G., Alvarez-Campana, M., & López, G. (2023). Analysis of security and data control in smart personal assistants from the user's perspective. *Future Generation Computer Systems*, *144*, 12–23. https://doi.org/10.1016/j.future.2023.02.009

Wi-Fi Alliance. (u.å). Wi-Fi CERTIFIED HaLow. Hämtad 29 februari 2024, från https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-halow

Windl, M., & Mayer, S. (2022). The skewed privacy concerns of bystanders in Smart Environments. *Proceedings of the ACM on Human-Computer Interaction*, *6*(MHCI), 1–21. https://doi.org/10.1145/3546719

Wu, T., Breitinger, F., & Niemann, S. (2021). IOT network traffic analysis: Opportunities and challenges for forensic investigators? *Forensic Science International: Digital Investigation*, *38*, 301123. https://doi.org/10.1016/j.fsidi.2021.301123

Zhang, K., Qian, Y., Motti, V. G., & Fung, C. (2023). A study on the privacy concerns of the internet of things. In *2023 7th cyber security in networking conference (csnet)*. IEEE. https://doi.org/10.1109/csnet59123.2023.10339706

Zhang, S., Liu, Y., & Gowda, M. (2022). I Spy You: Eavesdropping Continuous Speech on Smartphones via Motion Sensors. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *6*(4), 1–31. https://doi.org/10.1145/3569486

Zou, Q., Li, Q., Li, R., Huang, Y., Tyson, G., Xiao, J., & Jiang, Y. (2023). Iotbeholder: A Privacy Snooping Attack on User Habitual Behaviors from Smart Home Wi-Fi Traffic. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *7*(1), 1–26. https://doi.org/10.1145/3580890

Appendix A - Datatyp

Artikel	Kategori	Kod
IoT forensics: Analysis of a HIKVISION's mobile app (Dragonas et al., 2023)	**Enhetsdata**	Details about added CCTV system's active channels and their friendly names are saved within the “channelinfo” table of the “database.hik” database.
IoT forensics: Analysis of a HIKVISION's mobile app (Dragonas et al., 2023)	**Enhetsdata**	Details about Wi-Fi networks that the mobile device was connected to while the application was used are populating the “hc.realm” database.
IoT forensics: Analysis of a HIKVISION's mobile app (Dragonas et al., 2023)	**Enhetsdata**	The presence of the “videoGo_device_info.xml” file indicates that the user has enabled access to the CCTV system's “Remote Configuration” operations.
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Enhetsdata**	The first is the Samsung camera that sent unencrypted HTTP POST requests to the cloud, which exposed unique identifiers including, MAC address, username, serial number, timestamp and user specific device name (e.g. ‘smarthomeunsw’)
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Enhetsdata**	The second camera an Insteon also displayed cleartext information such as port numbers, MAC address, public IP address and unique ID
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Enhetsdata**	An unexpected finding was when the Triby speaker15 communicated with the cloud during an update, the HTTP GET request is displayed in cleartext and included information such as MAC address, username and serial number as shown in Fig. 3
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Enhetsdata**	There are two files of interest: events.csv and sensors.csv. On one hand, the events file, stores logs about the proper functioning of the device, such as a speaker or buzzer tests, network connection or battery state.
So fresh, so clean: Cloud forensic analysis of the Amazon iRobot	**Platsdata**	objects: Types of Objects and their coordinates Roomba detected.

Roomba vacuum (Onik et al., 2024)		
So fresh, so clean: Cloud forensic analysis of the Amazon iRobot Roomba vacuum (Onik et al., 2024)	**Platsdata**	Information regarding Roomba's navigational coordinates to reconstruct the map
The Cop In Your Neighbor's Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance (Calacci et al., 2022)	**Platsdata**	a location, anonymized to a nearby street intersection
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Platsdata**	postcode/zipcode etc. All this data is sensitive and helpful not just in identifying the user but also their physical characteristics.
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Platsdata**	postcode/zipcode etc. All this data is sensitive and helpful not just in identifying the user but also their physical characteristics.
So fresh, so clean: Cloud forensic analysis of the Amazon iRobot Roomba vacuum (Onik et al., 2024)	**Bilddata**	The Roomba Obstacle Detection API provides information that can help in investigations. In JSON response, some files have encrypted images. All images are labeled with the name of the object in them
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Bilddata**	We found that when the Xiaomi camera detected motion, the unencrypted video, MAC address and timestamp were sent in cleartext through a HTTP PUT request packet, a snippet of this is shown in Fig. 1. The access key ID and signature are also present in the header, this can provide an investigator access to the AWS account.
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Bilddata**	We also found that when the mobile app for the D-Link camera was activated, cleartext was present between the device and the mobile app during live streaming where partial JPEG images were present in the HTTP header.

Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Bilddata**	Through manual interaction with the QBee Camera application, we were able to download video recorded during the event; interestingly as videos were triggered by motion detection, the camera recorded not only the accelerant spill at 11:01, but was also triggered by the flames and smoke at 11:02:30.
The Cop In Your Neighbor's Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance (Calacci et al., 2022)	**Bilddata**	Each post also contains a title, description, up to five photos or videos
Analysis of security and data control in smart personal assistants from the user's perspective (Valero et al., 2023)	**Röstdata**	The data extracted from conversations identified by Facebook Portal is used to display advertising across Facebook. The company may also share specific demographic and audience engagement data with advertisers and analytics partners.
Analysis of security and data control in smart personal assistants from the user's perspective (Valero et al., 2023)	**Röstdata**	On the Apple HomePod Mini, Google Home Mini, and Google Nest Audio the personal responses are related to the selected voice recognition setting. If the user has the voice profile saved and voice recognition is active, when the SPA is asked for information such as calendar events, messages, or reminders, among other examples, it will check which user initiated the query, to provide an answer according to that person's data.
I Spy You: Eavesdropping Continuous Speech on Smartphones via Motion Sensors (Zhang et al., 2022)	**Röstdata**	Unlike microphones which require explicit permissions from the user for access by app developers, motion sensors (accelerometer and gyroscope) have unrestricted access, thus providing a side channel for eavesdropping speech
I Spy You: Eavesdropping Continuous Speech on Smartphones via Motion Sensors (Zhang et al., 2022)	**Röstdata**	In particular, recent android smartphones such as OnePlus 9 Pro, Samsung S20 and Huawei P20 provide unrestricted access to sensor data with sampling rates up to 500 Hz when sampled in

		SENSOR_DELAY_FASTEST mode . This covers a key range of human speechfrequencies, thus allowing a malicious app developer to eavesdrop speech content and compromise the privacy of users.
I Spy You: Eavesdropping Continuous Speech on Smartphones via Motion Sensors (Zhang et al., 2022)	**Röstdata**	By setting the sensor delay as *SENSOR_DELAY _FASTEST* in the Android SensorManager API [4], we extract data at a sampling rate of 500HzProc without any special permission from the user. With the improvement in CPU and battery performance, higher sampling rates might be possible in the future, thus increasing the privacy threat
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Kroppsdata**	The remaining 3 devices were smart health care devices that required personal data such as height, weight, postcode/zipcode etc. All this data is sensitive and helpful not just in identifying the user but also their physical characteristics.
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Kroppsdata**	The 3 devices manufactured by Withings (Sleep, baby monitor and scales) all sent cleartext data through HTTP POST requests. Although the Withings baby monitor and sleep did not contain any sensitive cleartext information, the Withings smart scales displayed considerable amount of user information, e.g., weight, height, as shown in Fig. 2.
Data collection of biomedical data and sensing information in smart rooms (Sei & Ohsuga, 2023)	**Kroppsdata**	Fitbit Aria 2 was used. The data of body weight, BMI, and body fat were measured.
Data collection of biomedical data and sensing information in smart rooms (Sei & Ohsuga, 2023)	**Kroppsdata**	Fitbit Charge3 and Withings Sleep were used. Fitbit Charge3 can measure the sleep level (awake, light, REM, and sleep), and Withings Sleep can measure the sleep level (awake, light, deep, and REM) and sleep events (heart rate, respiration rate, and snoring time.)

Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Sensordata**	For the first scenario, the most interesting findings related to the Xiaomi Mi app: a history of sensor values both for temperature and humidity as well as the motion detection is present, stored in an XML file for each configured sensor
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Sensordata**	Of interest is the difference in the handling of motion sensor logs, which are refreshed with the historical values from the cloud, even if the sensor is not connected anymore
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Sensordata**	From this file, it is observed that two emergency alerts were triggered at 11:02. The first one, titled “HeadsUp Smoke2”, is a warning about an increase in the level of smoke.8 The second one, titled “Emerg Smoke”, due to the fact that the emergency smoke values have been reached.
IoTBeholder: A Privacy Snooping Attack on User Habitual Behaviors from Smart Home Wi-Fi Traffic (Zou et al., 2023)	**Sensordata**	Among them, event 31 and event 39 come from the data collected from user C. Event 31 probably corresponds to the behavior of user C when getting up. User C first turns on the bedlight, then the LED in the living room through the app and enters the living room. Later, user C turns on the light of the bath heater and starts to wash. After that, user C turns off the light of the bath heater and walks out. An interesting observation is that user C tends to turn off the bed light via the app after washing up.

Appendix B - MoIndata

Artikel	Kategori	Koder
So fresh, so clean: Cloud forensic analysis of the Amazon iRobot Roomba vacuum (Onik et al., 2024)	**Enhetsdata**	https://disc-prod.iot.irobotapi.com/v1/discover/endpoints?country_code=US - Configuration details about the iRobot IoT platform - Provides insight into the infrastructure and potential data storage locations.
So fresh, so clean: Cloud forensic analysis of the Amazon iRobot Roomba vacuum (Onik et al., 2024)	**Enhetsdata**	https://auth3.prod.iot.irobotapi.com/v1/robotid/missionhistory?filterType=app_id - Comprehensive dataset about Roomba's activities - Offers insights into Roomba's operations, including Wi-Fi connections, charging times, and cleaning durations. This can help establish timelines and identify anomalies.
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Enhetsdata**	Samsung Smart Cam - MAC address, username, serial number, timestamp and user specified device name
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Enhetsdata**	Insteon Camera(wired) - Port numbers, MAC address, public IP address, unique ID
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Enhetsdata**	Triby speakers - Username, serial number, MAC address
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Enhetsdata**	Xiaomi camera - URL and timestamp of captured motion, MAC address
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Enhetsdata**	Meross - UUID and model of the linked smartphone - UUID and MAC address of the gateway - Login and Google tokens (expired)
So fresh, so clean: Cloud forensic analysis of the Amazon iRobot Roomba vacuum (Onik et al., 2024)	**Bilddata**	https://auth1.prod.iot.irobotapi.com/v1/robots/340EE4928078487E853BF9F3180A3898/imageupload/imagesurl - Link to download Encrypted Images captured by Roomba -

		Images to see the Obstacles presented in an Environment.
The Cop In Your Neighbor's Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance (Calacci et al., 2022)	**Bilddata**	Each post also contains a title, description, up to five photos or videos
So fresh, so clean: Cloud forensic analysis of the Amazon iRobot Roomba vacuum (Onik et al., 2024)	**Användardata**	Our analysis discovered an Account Provider API to access account management information. Roomba uses gigya, a customer identity management platform. The JSON data provided by this API includes first and last name, email address, country, account registration timestamp, last login timestamp, user preferences, and account status.
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Användardata**	Meross - Registered email
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Användardata**	Google Home - Google Account ID - Registered email - Android app usage - Voice commands history - YouTube history
IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale (Huang et al., 2020)	**Användardata**	The top 10 vendors with the highest fraction of devices that communicated with at least one tracking domain are all associated with smart TVs. In particular, 57.9% (highest fraction across the vendors) of Nvidia devices (which correspond to Nvidia Shield TV) communicated with tracking domains, and 47.1% (next highest fraction) of Roku devices communicated with tracking domains. The remaining 8 vendors in the top 10 include TCL, Samsung, Sony, and LG, among others
Analysis of security and data control in smart personal assistants from the user's perspective (Valero et al., 2023)	**Röstdata**	The protection of minor users through simple and quick settings is practically non-existent in the conditions analysed (see Table 2), whereas this has already been included in other related applications, such as streaming platforms like Netflix, which already includes a specific default profile for

		them. In the case of SPAs, however, it is necessary to go through the entire set of device settings, even having to switch between different configuration menus, to disable all features that may be unsafe for an unsupervised minor user.
Analysis of security and data control in smart personal assistants from the user's perspective (Valero et al., 2023)	**Röstdata**	The options for interacting with the conversation history are different for each of the devices. The Apple HomePod Mini offers the least possibilities, only being able to send a request to delete the conversation recordings stored on Apple's servers.
Analysis of security and data control in smart personal assistants from the user's perspective (Valero et al., 2023)	**Röstdata**	The Google Home Mini offers a full privacy settings section for viewing and deleting voice recordings, as well as setting up automatic deletion of recordings and pausing the storage of recordings.
Analysis of security and data control in smart personal assistants from the user's perspective (Valero et al., 2023)	**Röstdata**	The options that Amazon incorporates into the Amazon Echo Show 5 and Amazon Echo Dot 4 are similar to those of Google, offering a full set of options for reviewing conversations with the SPA, deleting them, and setting up automatic deletion of data
Analysis of security and data control in smart personal assistants from the user's perspective (Valero et al., 2023)	**Röstdata**	In the case of Facebook Portal, since it uses Amazon Alexa as a voice agent, something similar happens. In fact, Facebook Portal records voice clips when the users activate the Smart Assistant by saying "Hey portal" and it sends back to Facebook these clips. Also, these voice clips are recorded and sent back to Amazon
So fresh, so clean: Cloud forensic analysis of the Amazon iRobot Roomba vacuum (Onik et al., 2024)	**Platsdata**	https://auth3.prod.iot.irobotapi.com/v1/robotid/pmaps/pmap_id/versions/pmapv_id/ - Information regarding Roomba's navigational coordinates to reconstruct the map - Offers a digital footprint, enabling the reconstruction of events, verification of objects, detection of

		environmental changes.
So fresh, so clean: Cloud forensic analysis of the Amazon iRobot Roomba vacuum (Onik et al., 2024)	**Platsdata**	https://auth1.prod.iot.irobotapi.com/v1/robots/340EE4928078487E853BF9F3180A3898/imageupload/metadata - Details about the type of obstacle - Forensically relevant in reconstructing events, understanding environmental dynamics, and establishing potential evidence in investigations.
The Cop In Your Neighbor's Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance (Calacci et al., 2022)	**Platsdata**	The resulting date range of posts ranges from October 2016 to February 2020 because the earliest post on the platform appears in October 2016, and scraping was performed in March 2020. Each alert includes a unique ID, a user ID of the account the alert was posted by, a user-provided title, description, and category, as well as a timestamp and geocoded location
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Sensordata**	Google Home - IKEA bulbs state information
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Sensordata**	Nest Protect - Sensors measurements history
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Sensordata**	Xiaomi Home - Measurements of Temperature and Humidity
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Sensordata**	Netatmo - Measurements of - temperature - humidity - CO_2
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Sensordata**	myStrom - Measurements of - consumption - power - energy - temperature

Appendix C - Lokal Data

Artikel	Kategori	Koder
IoT forensics: Analysis of a HIKVISION's mobile app (Dragonas et al., 2023)	**Enhetsdata**	Details about added CCTV system's active channels and their friendly names are saved within the “channelinfo” table of the “database.hik” database.
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Enhetsdata**	Nest Protect - Account ID - Structure ID (Home ID) - SSID and WiFi PSK
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Enhetsdata**	Xiaomi Home - Serial Number - Model - MAC Address - SSID and WiFi PSK - References to some sensors
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Enhetsdata**	Ikea Trådfri - Serial Number - Room Configuration - Device Configuration or Logs
Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations (Servida et al., 2023)	**Enhetsdata**	QBee Camera - Serial Number - Model - SSID and WiFi PSK
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Data mellan applikation och enhet**	D-Link camera - JPEG images
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Data mellan applikation och enhet**	Victure camera - API access key, access token
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Data mellan applikation och enhet**	3 devices used no encryption between the mobile app-to-device. We found LE LampUX lightbulb and the iBlockcube plug used Internet Protocol Device Control (IPDC), which is unusual as this is typically used for Voice Over IP (VoIP).
IoT network traffic analysis: Opportunities and challenges for forensic investigators? (Wu et al., 2021)	**Data mellan applikation och enhet**	D-Link camera communicated to the mobile app in cleartext.

Data collection of biomedical data and sensing information in smart rooms (Sei & Ohsuga, 2023)	**Kroppsdata**	Fitbit Aria 2 was used. The data of body weight, BMI, and body fat were measured.
Data collection of biomedical data and sensing information in smart rooms (Sei & Ohsuga, 2023)	**Kroppsdata**	Fitbit Charge3 was used. This watch is waterproof, but some subjects remove it when showering. The heart rate during sleep is also included in the sleep data measured by Withings Sleep.
Data collection of biomedical data and sensing information in smart rooms (Sei & Ohsuga, 2023)	**Kroppsdata**	Fitbit Charge3 was used. Energy expenditure per hour, number of steps taken per hour, distance traveled per hour, number of floors climbed per hour, and elevation gain per hour were measured.
Data collection of biomedical data and sensing information in smart rooms (Sei & Ohsuga, 2023)	**Kroppsdata**	Fitbit Charge3 and Withings Sleep were used. Fitbit Charge3 can measure the sleep level (awake, light, REM, and sleep), and Withings Sleep can measure the sleep level (awake, light, deep, and REM) and sleep events (heart rate, respiration rate, and snoring time.)
Data collection of biomedical data and sensing information in smart rooms (Sei & Ohsuga, 2023)	**Kroppsdata**	Joy-Con is a controller for Nintendo Switch. Joy-Con is equipped with an accelerometer and gyro-sensor; one Joy-Con is stored in Ring-Con, and the other Joy-Con is stored in the leg strap. The user holds the Ring-Con in his or her hand and wraps the leg strap around the thigh to enjoy the game. Joy-Con measures the calories burned during play, playtime duration, and distance traveled during running exercises.

Appendix D - Bekvämlighet

Artikel	Kategori	Kod
Empowering homes with intelligence: An investigation of smart home technology adoption and usage (Gøthesen et al., 2023)	**Insamlingsmetod**	CON4 stated that this factor was the main reason they did not use any SHT today and especially pointed out that smart speakers were problematic due to the possibility of them listening to personal conversations and accessing sensitive information.
"You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users (Lenhart et al., 2023)	**Insamlingsmetod**	Overall, participants were most concerned about interior cameras (video data collected in private spaces), followed by some concerns with devices that collected audio data.
The Skewed Privacy Concerns of Bystanders in Smart Environments (Windl & Mayer, 2022)	**Insamlingsmetod**	In line with previous work [6,8,45], we found that devices with microphones and cameras were perceived as especially privacy-concerning.
Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls (Ahmad et al., 2022)	**Insamlingsmetod**	Although people can be assured of their privacy by physically covering or obscuring cameras, no clear solutions exist to assure people that embedded microphones are indeed 'off' and not listening.
The Skewed Privacy Concerns of Bystanders in Smart Environments (Windl & Mayer, 2022)	**Insamlingsmetod**	In contrast, by far, the most concerns were raised by the smart security camera, followed by the smart speaker. Our qualitative findings provide reasoning. Here, several participants mentioned feeling surveilled by both devices, either by constantly being watched or listened to without consenting to either

Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants (Tabassum et al., 2020)	**Insamlingsmetod**	Indeed, many participants raised privacy concerns associated with the continuous listening of their conversations.
Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls (Ahmad et al., 2022)	**Teknisk erfarenhet**	Thus, a major design implication is that a large amount of responsibility lies on device manufacturers. Device manufacturers need to ensure their designs do indeed disconnect the microphones at a hardware level to be in line with people's expectations, since this functionality appears to be assumed
The Skewed Privacy Concerns of Bystanders in Smart Environments (Windl & Mayer, 2022)	**Teknisk erfarenhet**	Finally, as already suggested by Apthorpe et al. [4], we could also confirm our fifth hypothesis (H5), that participants assign fewer privacy concerns to devices they own, i.e., devices they are already experienced with.
Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants (Tabassum et al., 2020)	**Teknisk erfarenhet**	We found that current owners of voice assistants were more likely to allow an always-listening device to use a recorded conversation than non-owners, thus making them more likely to adopt even more privacy-invasive future devices
"You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users (Lenhart et al., 2023)	**Teknisk erfarenhet**	Participants also noted that some of their strategies required technical skills and advanced network management to achieve meaningful results that protected their privacy—something they worried most people wouldn't be willing or able to do.

"Innovative Technologies or Invasive Technologies?": Exploring Design Challenges of Privacy Protection With Smart Home in Jordan (Albayaydh & Flechais, 2024)	**Integritetsförlust**	Users recognized that privacy threats in the smart home exist on two fronts: external threats originating from outside the home, such as companies, hackers, criminals, and curious individuals, and internal threats posed by users who have control over the devices within the home and target individuals with limited device usage, including passive family members and bystander domestic workers [U06].
Controlling the 'elephant in the room': A new protocol for sharing data from home performance monitoring systems (Adeyeye, 2024)	**Integritetsförlust**	The participants were less inclined to take privacy risks that could have direct impact on their enjoyment, privacy, and safety in their home.
Effects of Home Voice Assistants' Autonomy on Instrusiveness and Usefulness: Direct, Indirect, and Moderating Effects of Interactivity (Lucia-Palacios & Pérez-López, 2021)	**Integritetsförlust**	Together with privacy risk, intrusiveness is one of the main consumer concerns about the new connected products or those with Internet of things technologies.
Alexa, Who Am I Speaking To?: Understanding Users' Ability to Identify Third-Party Apps on Amazon Alexa (Major et al., 2021)	**Integritetsförlust**	These findings suggest that a user may accidentally invoke an unintended skill without being aware of this mistake; regardless of whether the skill is malicious or benign, the unintended third party may obtain sensitive user information, thus giving rise to privacy risks.
Empowering homes with intelligence: An investigation of smart home technology adoption and usage (Gøthesen et al., 2023)	**Integritetsförlust**	On the other hand, our findings suggest that those who used some SHT solutions did not have particular security and privacy concerns, and some also felt that SHT enabled better home security [23]
Empowering homes with intelligence: An investigation of smart home technology adoption and usage (Gøthesen et al., 2023)	**Integritetsförlust**	Another explanation might be, as suggested by EXP5, that SP concerns mainly apply to the vendors and should therefore

		not be a concern to the consumers.
Effects of Home Voice Assistants' Autonomy on Instrusiveness and Usefulness: Direct, Indirect, and Moderating Effects of Interactivity (Lucia-Palacios & Pérez-López, 2021)	**Interaktivitet**	The results show that improving and increasing the level of interactivity have positive effects, not only reducing intrusiveness but also increasing the perceived usefulness of the voice assistant.
Effects of Home Voice Assistants' Autonomy on Instrusiveness and Usefulness: Direct, Indirect, and Moderating Effects of Interactivity (Lucia-Palacios & Pérez-López, 2021)	**Interaktivitet**	Our findings show that the higher the interactivity, the lower the perceived intrusiveness of the product.
Complex online harms and the smart home: A scoping review (Olabode et al., 2023)	**Komfort kontra integritet**	From a user perspective, the research shows that users generally cede their agency, independence, and autonomy in the smart home in favour of increased benefits of technology, which then augments risks and vulnerabilities.
Studying users' perception of IoT mobile companion apps (Scoccia et al., 2023)	**Komfort kontra integritet**	However, this also highlights that most consumers do not pay special attention to privacy-related aspects of IoT devices, or are willing to accept compromises in this regard, trading privacy in exchange for more advanced features.
"You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users (Lenhart et al., 2023)	**Komfort kontra integritet**	And while many participants described themselves as privacy-conscious and made purchasing decisions based on their desire to minimize data collection, they recognized that they sometimes had to sacrifice some privacy to get benefits from the devices.

Analysis of security and data control in smart personal assistants from the user's perspective (Valero et al., 2023)	**Minderårigas integritet**	Since SPAs are more and more used by minors [28], it is of major importance the possibility to set up profiles for minors that limit some functionalities and protect them from inappropriate content and from potential stalkers and fraudsters.
Analysis of security and data control in smart personal assistants from the user's perspective (Valero et al., 2023)	**Minderårigas integritet**	As a result, the access of minors to inappropriate content or actions in the case of SPAs rely heavily on the technical knowledge and skills of their guardians, which is unfair for minors and may entail not fulfilling current security and data regulation that is typically more strict in their case.
"You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security (Turner et al., 2022)	**Minderårigas integritet**	In addition, children may not perceive devices in the same way that adults do, not only, as our interviews showed, failing to understand they are connected to the Internet, but also in understanding how they work [71,73].

Appendix E - Förtroende

Artikel	Kategori	Koder
Why people replace their aging smart devices: A push–pull–mooring perspective (Lenz et al., 2023)	**Förtroende för märke**	These results suggest that respondents were more concerned about the motivation or ability of manufacturers to securely store personal information collected by older smart devices (i.e., storing of collected data) than about the data collection itself.
Why people replace their aging smart devices: A push–pull–mooring perspective (Lenz et al., 2023)	**Förtroende för märke**	Alternatively, users of smart devices may become more concerned about how the collected personal information is stored with the increasing amount of accumulated personal information in manufacturers' databases.
Effects of Home Voice Assistants' Autonomy on Instrusiveness and Usefulness: Direct, Indirect, and Moderating Effects of Interactivity (Lucia-Palacios & Pérez-López, 2021)	**Förtroende för märke**	Intrusiveness involves a lack of trust in the service provider or brand (Benlian et al., 2019, Wueest, 2017, Yang et al., 2017), so trust is an important condition to reduce privacy risk or intrusiveness.
In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things (Turner et al., 2022)	**Förtroende för märke**	This, in turn, results in users not having enough information to assess their trust in these products and the respective vendors, which interviewees frequently alluded to.
Trust in the institution and privacy management of Internet of Things devices. A comparative case study of Dutch and Norwegian household (Paupini et al., 2022)	**Förtroende för märke**	If you look at big companies like Facebook, Google, Apple. No. I don't trust them at all - I'm more afraid of those big companies that they will use or sell it themselves or I don't know what.
Trust in the institution and privacy management of Internet of Things devices. A comparative case study of	**Förtroende för märke**	And those small businesses probably don't have their safety and security in order.

Dutch and Norwegian household (Paupini et al., 2022)		
Empowering homes with intelligence: An investigation of smart home technology adoption and usage (Gøthesen et al., 2023)	**Förtroende för märke**	Furthermore, EXP5 emphasized that privacy and security-related concerns should, by principle, mainly apply to the vendors and not so much to the consumer, as the vendors should ensure to follow the highest possible security and privacy measures in their technologies.
"You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users (Lenhart et al., 2023)	**Förtroende för märke**	Nonetheless, numerous participants commented that they were willing to pay more for HomeKit devices and/or deal with less functionality because of concerns that companies who made cheaper devices routinely collected and/or sold user data.
A Survey on Understanding and Representing Privacy Requirements in the Internet-of-Things (Ogunniye & Kokciyan, 2023)	**Förtroende för märke**	The example above shows that Bob is willing to share data with different agents with varying degrees of trust.
"Innovative Technologies or Invasive Technologies?": Exploring Design Challenges of Privacy Protection With Smart Home in Jordan (Albayaydh & Flechais, 2024)	**Förtroende för märke**	They have also emphasized the need for government intervention through the enactment of explicit data protection laws to protect users' privacy, highlighting the need for companies to ensure compliance with existing laws to avoid the consequences of non-compliance [D05].
"Innovative Technologies or Invasive Technologies?": Exploring Design Challenges of Privacy Protection With Smart Home in Jordan (Albayaydh & Flechais, 2024)	**Förtroende för märke**	Moreover, some participants expressed the view that companies prefer an opaque regulatory environment to continue exploiting users' data [L05].

"You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security (Turner et al., 2022)	**Förtroende för märke**	We found that even with these users' advanced research, knowledge, and technical skills, their comfort with SHDs still depended heavily on trust in the companies who manufacture and support the devices
Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls (Ahmad et al., 2022)	**Förtroende för teknologin**	Thus, a major design implication is that a large amount of responsibility lies on device manufacturers. Device manufacturers need to ensure their designs do indeed disconnect the microphones at a hardware level to be in line with people's expectations, since this functionality appears to be assumed
Controlling the 'elephant in the room': A new protocol for sharing data from home performance monitoring systems (Adeyeye, 2024)	**Förtroende för teknologin**	Acceptance factors within the context of citizen attitudes and participation were found to include cost, trust, benefit, and performance expectancy. However, hedonic factors, and social influence were not proven.
"You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security (Turner et al., 2022)	**Förtroende för teknologin**	People who receive a smart speaker as a gift or just want the cheapest smart doorbell to track package delivery might not fully understand the privacy risks inherent in such devices, know what questions to consider when deciding to use them, or possess the skills to take meaningful action
Studying users' perception of IoT mobile companion apps (Scoccia et al., 2023)	**Förtroende för teknologin**	A possible explanation for this phenomenon is that the more privacy-concerned individuals refrain from adopting smart-home IoT devices, driven by their privacy concerns.

Appendix F - Medvetenhet

Artikel	Kategori	Koder
Interactive Privacy Management: Toward Enhancing Privacy Awareness and Control in the Internet of Things (Al Muhander et al., 2023)	**Intergritetsmedvetenhet**	Throughout the device development cycle, IoT developers and manufacturers must consider the device's privacy and how it may impact users. This information must be communicated to users in an understandable manner by using, for example, the three-step design shown in Figure11(a)
A Survey on Understanding and Representing Privacy Requirements in the Internet-of-Things (Ogunniye & Kokciyan, 2023)	**Intergritetsmedvetenhet**	Explanations are important to improve users' understanding of privacy preferences and expectations to help them make informed decisions
Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants (Tabassum et al., 2020)	**Intergritetsmedvetenhet**	As with current voice assistants, privacy issues remain a key concern that may limit users' willingness to even consider an always-listening voice assistant
"You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security (Turner et al., 2022)	**Intergritetsmedvetenhet**	People who receive a smart speaker as a gift or just want the cheapest smart doorbell to track package delivery might not fully understand the privacy risks inherent in such devices, know what questions to consider when deciding to use them, or possess the skills to take meaningful action
User-Centric Privacy Controls for Smart Homes (Chhetri & Genaro Motti, 2022)	**Datahanteringsmedvetenhet**	"If there is any kind of app or anything that might help me to control the monitoring of data myself and the data being transferred to somewhere else, so I can see like what happened to my data." (P20)

"You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security (Turner et al., 2022)	**Datahanteringsmedvetenhet**	The adults and children interviewed had some level of understanding of how having home IoT devices increased the collection of personal data, and that misuse of such data by someone with malicious intent could be bad.
Owning and Sharing: Privacy Perceptions of Smart Speaker Users (Meng et al., 2021)	**Datahanteringsmedvetenhet**	Similar for all groups, participants have concerns about how their data is handled and a lack of control and transparency over the data processes.
Setting Privacy “by Default” in Social IoT: Theorizing the Challenges and Directions in Big Data Research (Saura et al., 2021)	**Konfigurationsmedvetenhet**	To conclude, the direction of setting privacy ‘by default’ in SioT should seek to achieve a satisfactory balance between: (i) quality of service and protection of user data privacy; (ii)
Tangible Privacy for Smart Voice Assistants: Bystanders’ Perceptions of Physical Device Controls (Ahmad et al., 2022)	**Konfigurationsmedvetenhet**	Our first major finding is that a tangible, physical control to mute/unmute devices provides a statistically significant increase in people’s perceptions of reliability, trust (and reduced risk), usability, and control of the device.
Alexa, Who Am I Speaking To?: Understanding Users’ Ability to Identify Third-Party Apps on Amazon Alexa (Major et al., 2021)	**Konfigurationsmedvetenhet**	Participants often did not have clear intuitions regarding what can and cannot be done with Alexa verbally (rather than through the app or with physical buttons on the device
User-Centric Privacy Controls for Smart Homes (Chhetri & Genaro Motti, 2022)	**Konfigurationsmedvetenhet**	Participants desired user training and simplistic design of devices so that users can configure themselves, without the need for professional help.

"You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security (Turner et al., 2022)	**Konfigurationsmedvetenhet**	People who receive a smart speaker as a gift or just want the cheapest smart doorbell to track package delivery might not fully understand the privacy risks inherent in such devices, know what questions to consider when deciding to use them, or possess the skills to take meaningful action
Controlling the 'elephant in the room': A new protocol for sharing data from home performance monitoring systems (Adeyeye, 2024)	**Likgiltighet**	Most of the participants recognised that a lot of their personal information is already "out there", and they have little or no control over that.
Studying users' perception of IoT mobile companion apps (Scoccia et al., 2023)	**Likgiltighet**	we can observe that a limited amount of reviews express privacy-related concerns, identified in only 6 Android and 11 iOS reviews.
Studying users' perception of IoT mobile companion apps (Scoccia et al., 2023)	**Likgiltighet**	However, this also highlights that most consumers do not pay special attention to privacy-related aspects of IoT devices, or are willing to accept compromises in this regard, trading privacy in exchange for more advanced features.
Empowering homes with intelligence: An investigation of smart home technology adoption and usage (Gøthesen et al., 2023)	**Likgiltighet**	On the other hand, our findings suggest that those who used some SHT solutions did not have particular security and privacy concerns, and some also felt that SHT enabled better home security [23].
"You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security (Turner et al., 2022)	**Likgiltighet**	Regardless of their feelings about this, if individuals want to use such devices, they have to accept the terms of use, which often requires full data collection to be turned on for complete device functionality.

"You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security (Turner et al., 2022)	**Likgiltighet**	The interviews and the survey showed that families were happy to use and integrate home IoT devices in their homes, and did not take particular steps to inform themselves as to how to make these devices more secure”
"Innovative Technologies or Invasive Technologies?": Exploring Design Challenges of Privacy Protection With Smart Home in Jordan (Albayaydh & Flechais, 2024)	**Likgiltighet**	They expressed that the terms and conditions in privacy policies tend to favor service providers, leaving users feeling compelled to accept and agree to them [U03].
User-Centric Privacy Controls for Smart Homes (Chhetri & Genaro Motti, 2022)	**Gästmedvetenhet**	About 5% (n=11) of the codes fell in this category, which included desired features, such as add/remove users, anonymize collected data, optimize privacy settings, do not share (with other users), multi-user privacy settings, option to give permission to family members, schedule SHD operation, display data only for authenticated user, and segregate data by users
"Innovative Technologies or Invasive Technologies?": Exploring Design Challenges of Privacy Protection With Smart Home in Jordan (Albayaydh & Flechais, 2024)	**Gästmedvetenhet**	Furthermore, users mentioned that they use a single account for their devices, without creating individual accounts for each household member

"Innovative Technologies or Invasive Technologies?": Exploring Design Challenges of Privacy Protection With Smart Home in Jordan (Albayaydh & Flechais, 2024)	**Gästmedvetenhet**	Consequently, the consent provided by the account owner applies to all users within the device's range, including family member sand bystanders, which represents a privacy protection challenge in multi-user settings where no restrictions are placed on how the account owner (the administrator) uses others' data.