

DIGITAL LAGRING OCH
ANVÄNDNING AV PRIVAT
INFORMATION I SMARTA HEM
– EN STUDIE MED ANVÄNDARPERSPEKTIV

Kandidatuppsats i Informatik

André Hamberg
Fredrik Lundgren

VT 2020:KANI14



HÖGSKOLAN
I BORÅS

Svensk titel: Digital lagring och användning av privat information i smarta hem

Engelsk titel: Digital storage and use of private information in smart homes

Utgivningsår: 2020

Författare: André Hamberg och Fredrik Lundgren

Handledare: Anders Hjalmarsson Jordanius

Abstract

The dream of a fully automated smart home is soon no longer a dream. Connected devices can adapt to their surroundings and the given situations, allowing the kitchen lamps to light up when the garage door is opened. Furthermore, smart homes can increase the quality of life for users by adapting to their habits and behaviours. If the devices are to be able to adapt to the users and their environment, much information is required, which in the wrong hands could have devastating consequences for the user. However, there are deficiencies in the security of devices, and some of these are produced without security in mind. There are several security risks with smart homes and the study has focused on security risks with a focus on authentication and behavioural adaptation, with a user perspective, as this is something that is missing in existing literature. The question addressed in the study is:

"How do users of connected devices in Smart homes view security based on authentication and behavioural adaptation?"

To answer this question a quantitative method has been applied. A web survey was designed and tested in a pre-pilot study and then in a pilot study before it was published. The questions in the survey have been generated from the theory presented in the theoretical framework. The result shows that users have high confidence in the security of their devices and that a majority are not worried about security risks linked to authentication. Respondents are more concerned about security risks associated with behavioural adaptation rather than with authentication. Those with high confidence tend to be more willing to disclose more private information than those with low confidence. A majority are also favourably positioned to provide more information for increased convenience and for the units to use stored information for increased convenience.

Keywords:

Internet of Things, Smart homes, User perspective, Authentication, Behaviour adaptation, Security

Sammanfattning

Drömmen om ett smart hem som är helt automatiserat är snart inte en dröm längre. Uppkopplade enheter kan anpassa sig efter sin omgivning och efter givna situationer, vilket exempelvis gör det möjligt för kökslamporna att tändas när garageporten öppnas. Vidare har smarta hem möjligheten att öka livskvaliteten för användare genom att anpassa sig efter deras vanor och beteenden. Om enheterna ska kunna anpassa sig efter användarna och sin omgivning krävs det oerhört mycket information, som i fel händer skulle kunna få förödande konsekvenser för användaren. Dock finns det brister i säkerheten bland enheter och vissa produceras utan säkerhet i åtanke. Det finns flertalet säkerhetsrisker med smarta hem och studien har fokuserat på säkerhetsrisker med fokus på autentisering och beteendeanpassning, med ett användarperspektiv, då det är något som saknas i befintlig litteratur. Frågeställningen som behandlas i studien är:

”Hur ser användare av uppkopplade-enheter i smarta hem på säkerhet utifrån autentisering och beteendeanpassning?”.

För att kunna besvara denna frågeställning har en kvantitativ metod tillämpats. En webbenkät utformades och testades i en pre-pilot studie och sedan i en pilotstudie innan den publicerades. Frågorna i enkäten har utvecklats från den teori som presenteras i det teoretiska ramverket. Resultatet visar på att användarna har en hög tilltro till säkerheten hos sina enheter och att en majoritet inte är oroliga över säkerhetsrisker kopplat till autentisering. Respondenterna är mer oroliga över säkerhetsrisker associerade med beteendeanpassning än med autentisering. De respondenterna med hög tillit tenderar att vara villiga att ge ut mer privat information än de med låg tillit. En majoritet är också positivt inställda till att lämna ut mer information för ökad bekvämlighet samt att enheterna använder lagrad information för ökad bekvämlighet.

Nyckelord:

Internet of Things, Smarta hem, Användarperspektiv, Autentisering, Beteendeanpassning, Säkerhet.

Förord

Först och främst vill vi tacka alla de som tog sig tiden att besvara vår enkät. Studien hade inte varit möjlig att genomföra utan ert engagemang och deltagande.

Vi vill även tacka våra familjer och vänner som har ställt upp och korrekturläst, gett oss tips på hur vi borde presentera olika delar i studien, samt agerat som stöttepelare de dagar när vi behövt extra stöd för att ta oss vidare.

Vi vill slutligen även rikta ett stort tack till vår handledare Anders Hjalmarsson Jordanius som hjälpt oss genom hela uppsatsarbetet. Utan din vägledning hade denna studie inte varit möjlig.

Borås 2020-06-04

André Hamberg och Fredrik Lundgren

Innehållsförteckning

1 Introduktion	1
1.1 Bakgrund	1
1.2 Tidigare forskning	2
1.3 Problemdiskussion	4
1.4 Syfte och problemformulering	5
1.5 Intressenter	5
1.6 Avgränsning	6
2 Metod	7
2.1 Metodansats	7
2.2 Forskningsstrategi	7
2.3 Litteraturstudie	8
2.4 Enkätundersökning	9
2.4.1 Utformning av enkät	9
2.4.2 Pilotstudie	11
2.5 Urval	11
2.6 Validitet	13
2.7 Reliabilitet	14
2.8 Etik	14
2.9 Analysmetod	15
2.10 Metoddiskussion	16
3 Teoretiskt ramverk	17
3.1 Smarta Hem	17
3.2 Säkerhetsrisker	18
3.2.1 Autentisering	19
3.2.2 Beteendeanpassning	20
4 Resultat	22
4.1 Resultat av univariat data	22
4.2 Resultat av bivariat data	- 32 -
5 Analys och diskussion	- 40 -
5.1 Smarta hem	- 40 -
5.2 Säkerhetsrisker	- 41 -
5.3 Autentisering	- 42 -
5.4 Beteendeanpassning	- 44 -
6 Slutsats och utvärdering	- 46 -
6.1 Slutsats	- 46 -
6.2 Värdering av studien	- 47 -

6.3 Förslag på framtida forskning	- 48 -
7 Referenser	- 49 -
<i>Bilaga. Enkätundersökning</i>	<i>- 54 -</i>

1 Introduktion

1.1 Bakgrund

Världen är på väg in i en ny teknologisk era, Internet of Things (IoT). IoT innebär att vardagliga föremål som försetts med intelligens kan kommunicera med varandra via inbäddade system (Vinel, Wang, Xia & Yang 2012). Skiljelinjen mellan våra egna, mänskliga handlingar och de som utförs av de uppkopplade enheterna i vår omgivning blir konsekvent mer diffusa. Enheterna kan via sina system ta emot och överföra data, samt initiera operationer hos andra enheter (Mendez, Papapanagiotou & Yang 2017).

Drömmen om att ett hem skulle kunna vara helt automatiserat är inte längre bara en dröm, utan är på väg att bli en verklighet med uppskattningsvis 50 miljarder uppkopplade enheter i världen år 2020 (Nilsson 2018). Uppkopplade enheter kan anpassa sig efter den givna situationen, en form av beteendeanpassning. Detta möjliggör bland annat att lamporna i köket kan tändas när garageporten öppnas, då det signalerar att någon är hemma (Liu, Gong, Shea & Sun 2018). Smarta hem har som syfte att göra livet mer bekvämligt eftersom vi behöver göra mindre, på grund av att enheterna i hemmet sköter det åt användarna (Miller 2015). Detta eftersom de smarta enheterna automatiskt kan samla in data från dess användare med minimal interaktion mellan dem (Kim & Wong 2014).

I och med att ny teknologi för smarta hem konstant kommer ut på marknaden för detta med sig säkerhetsrisker (Awad & Bako 2018). När stora mängder data lagras och genereras om dess användare, dyker osäkerheter upp kring hur denna data används. Detta beror på att det inte finns något tydligt implementerat integritetsskydd som dessa tar hänsyn till (Kim & Wong (2014). Vem som äger all data och har ansvaret för den tenderar därmed att vara otydligt (Andonova, Milne, Hajjat & Weinberg 2015). Företag som Apple, Amazon och Google har bland annat hamnat i blåsväder när de har lagrat och använt konversationer mellan användare och dess enheter i hemmen för olika syften (Jacobson 2019).

Med tanke på att en markant del av den information som lagras och används av enheterna i smarta hem är av den privata karaktären, bör det väsentliga vara att beskydda den från

otillbörlig användning, annars riskerar enheterna i hemmen att inte bevara och vädja om integriteten hos dess användare (Brill 2015).

1.2 Tidigare forskning

Forskning och studier som berör uppkopplade enheter i hemmet och smarta hem som helhetsgrepp har framförallt haft fokus på två områden, nämligen på vilka sätt de kan underlätta för människor i deras vardag, samt säkerhetsaspekter - positiva som negativa associerade med dessa.

Pau, Salerno, Sharma & You (2019) menar att smarta hem har kapaciteten att öka välmående hos människor. Enheterna kan lära sig vilka nödvändigheter varje person i hemmet är i behov utav genom att de kan lära sig personers vanor och beteenden, vilket förbättrar livskvalitén. Människors hälsa och välmående förbättras som följd (Cook & Rashidi 2009). Även Alam, Ali & Reaz (2012) hävdar att smarta hem har förmågan att förbättra individers livskvalité genom att enheterna kan automatisera diverse handlingar, samt erbjuda assistanstjänster. Exempel på detta kan vara att bli påmind via mejl att kylskåpsdörren står öppen, eller att ugnen skickar ett sms när maten är klar (Miller 2015). Genom att utforma användarkontext (hur användarna beter sig samt deras vanor) kan enheterna skapa sig förståelse för användarnas olika förhållanden mellan olika enheter och människor (Pau et al. 2019).

Vidare har smarta hem inte bara förmågan att förbättra livskvalitén för dess användare, utan de kan även användas för att få en mer verkningsfull energieffektivisering (Cook & Rashidi 2009). Genom att lära sig residenternas beteende kan exempelvis termostater anpassa temperaturen inomhus beroende på om någon är hemma, eller befinner sig i en särskild del av hemmet, för att exempelvis öka deras bekvämlighet (Miller 2015). Eftersom fjärrstyrning är en av grundpelarna i smarta hem (Alam, Ali & Reaz 2012; Mashal & Shuhaiber 2019) kan användarna utföra diverse tidigare manuella handlingar på distans, vilket ytterligare kan bidra till att öka bekvämligheten.

När det kommer till säkerhet i smarta hem finns det flera sätt att hjälpa och underlätta för användarna. Bland annat kan övervakningsfunktioner och åtkomstkontroll generera varningar och slå larm om det skulle bli nödvändigt (Alam, Ali & Reaz 2012). Ett implementerat säkerhetssystem i ett smart hem skulle ha möjlighet att automatiskt låsa upp hemmets dörrar

och meddela larmcentralen vid en eventuell brand, utan att de som bor i hemmet behöver göra det själva (Kim & Robles 2010).

Dock påstår Liu et al. (2018) att människor tenderar att förbise konsekvenserna av att ha ett flertal enheter använda och skicka data, och som påföljd skapar sig illusioner om att de är säkra. Atzori, Iera & Morabito (2010) anser att när ny teknologi konstant kommer ut på marknaden är det svårt att få en överblick över vad som faktiskt lagras, och vem som kan använda den informationen. Maras (2015) menar vidare att hetsen att få ut ny IoT-teknologi på marknaden har lett till att flertalet av enheterna inte bara brister när det gäller säkerhetsåtgärder, utan att flertalet av dem har producerats utan säkerhet i åtanke överhuvudtaget. Bergman & Lin (2016) påstår att orsaker till detta kan vara att det inte finns någon motivation hos företagen att uppdatera säkerheten för enheter som inte kostar så mycket, samt att hushåll idag hanterar och sköter en stor del av säkerheten själva.

Fernandes, Jung, Prakasch & Rahmati (2017) menar i sin studie att användarna inte har kontroll över informationen och argumenterar för detta genom att hävda att 42 procent av ett urval av 499 applikationer på plattformen ”SmartThings” tilldelades åtkomst och tillgång till olika funktioner och information hos användarnas enheter, som de inte hade fått tillstånd från användaren att använda. Hargreaves, Hauxwell-Baldwin & Wilson (2015) åsyftar att den främsta utmaningen för smarta hem och dess enheter inte är förbättringar av reliabiliteten, funktionaliteten, synen på tillförlitligheten, användarvänligheten och integritet. Det är i själva verket att erkänna dessa problemområden som delar utav en utmaning att omdefiniera vad begreppet ”smart” egentligen innebär. Det är termer som måste framträda i människors vardag och samexistera med teknologin, och inte ses som något som endast finns inbyggt i själva teknologierna. Detta samspekar med det faktum att användare förväntar sig att rätten till integritet, eller funktioner som främjar det, inte ska kosta extra, samt att de inte är villiga att ge ut sin data för andra typer av ändamål än den de har godkänt (Barbosa, Park, Yao, Wang & Yao 2019).

Eftersom användare av uppkopplade enheter riskerar att bli hackade (You et al. 2019) finns risken att de får sin autentiseringsdata manipulerad och/eller förlorad som följd. Det räcker för en obehörig att skapa sig åtkomst till ett konto som tillhör användaren för att sedan komma åt andra konton kopplade till hen (Awad & Bako 2018). Användare är i behov att öka säkerheten

i processen att säkerställa deras identitet gentemot enheterna (Borgohain, Borgohain, Kumar & Sanyal 2015).

Chen, Huang, Yi & Zhu (2016) menar att enheter tenderar att inte operera som användare föreställt sig och förlorar därefter tilltro till dem på grund av att säkerhetsfunktioner inte tagits på det allvar det borde. Detta bygger Balta-Ozkan, Bicket, Davidson & Whitmarch (2013) vidare på, och menar att några av de största sociala barriärerna för att anamma konceptet ”smarta hem” hos användare är att förlora kontroll, integritet och tillförlitlighet. För att kunna öka bekvämlighet och användarvänlighet behöver enheterna information om beteendemönster, vilket leder till en svår balansgång mellan vad enheterna ska hjälpa användarna med och vad användarna är beredda att ge upp i utbyte (Miller 2015). Förbättring av en funktion för en person kan innebära en förlust av integritet hos en annan (Hargreaves, Hauxwell-Baldwin & Wilson 2015).

1.3 Problemdiskussion

Det går att se från tidigare forskning att det finns olika användningsområden för uppkopplade enheter i smarta hem (You, et. al. 2019; Alam, Ali & Reaz 2012; Miller 2015; Cook & Rashidi 2009; Mashal & Shuhaiber 2019). Enheterna kan bidra med att förhöja livskvalitén, förbättra energieffektiviseringen och säkerheten genom till exempel automatisering genom att enheterna lär sig användarnas beteendemönster och vanor. Dock är inte allt som tas upp positivt. Det finns flertalet säkerhetsaspekter förknippade med uppkopplade enheter i smarta hem, där bland annat (Atzori, Iera & Morabito 2010; Maras 2015) menar att användare saknar kunskap och kontroll över vilken information som lagras och används av enheterna.

På grund av att fjärrstyrning är en väsentlig del av konceptet smarta hem (Alam, Ali & Reaz 2012; Mashal & Shuhaiber 2019) finns det risk för användarna att utomstående genom hackning kommer åt autentiseringsdata, och kan därmed få tillgång till flertalet olika enheter i hemmet, samtidigt som de kan manipulera den (Awad & Bako 2018). Personerna kan därmed blockera åtkomst till enheterna. Detta skulle även kunna få ödesdiga konsekvenser när enheterna har lagrad information som på flertalet sätt kan beskriva vem ägaren är som person, genom hens vanor och beteenden (Miller 2015).

Det finns emellertid relativt lite forskning och litteratur som belyser användarperspektivet. Det har gjorts viss forskning på området som beskriver de sociala barriärerna och balansgången mellan integritet och mängden information som enheterna får tillgång till (Balta-Ozkan, Bicket, Davidson & Whitmarch (2013; Hargreaves, Hauxwell-Baldwin & Wilson 2015; Miller 2015).

Det existerar trots detta ett tomrum på forskning som helt utgår från användarnas perspektiv och som inte har sin utgångspunkt i något annat än hur dessa ser på den genererade informationen som lagras och används av enheterna, samt säkerhetsaspekterna som är associerade till detta.

1.4 Syfte och problemformulering

Med bakgrund mot tidigare forskning och problemdiskussionen har denna studie som syfte att undersöka hur användare ser på säkerhet kring lagring och användning av privat information av uppkopplade enheter i smarta hem, med fokus på autentisering och beteendeanpassning. Detta på grund av att majoriteten av tidigare forskning som gjorts på området fokuserar på säkerhet och användningsområden, men den tenderar att utesluta användarna.

Det är på grund av detta faktum det är relevant att genomföra en studie som har användarna som utgångspunkt för att bredda och komplettera den forskning och de studier som redan gjorts.

Frågeställningen som kommer bearbetas i denna studie:

- Hur ser användare av uppkopplade-enheter i smarta hem på säkerhet utifrån autentisering och beteendeanpassning?

1.5 Intressenter

Intressenterna som denna studie kommer rikta sig mot är de som idag använder sig utav uppkopplade enheter i sina hem. Individer som funderar på att införskaffa enheter och bygga upp ett smarthem i framtiden är inte av intresse i enkätundersökningen. Detta på grund av att den riktar sig till redan befintliga användare, men tillhör ändå gruppen av intressenter på grund av att den ger existerande användares perspektiv på säkerhet, och ger därmed en överblick på hur dessa förhåller sig till ämnet. Förutom privatpersoner är även olika företag som behandlar, utvecklar och producerar mjuk- och hårdvara för enheter i smarta hem

intressenter i studien. Eftersom det finns en brist på forskning kring användares syn på digital lagring och användning av information är det essentiellt att producenternas kunskap och medvetenhet om användarna ökar.

1.6 Avgränsning

Studien är riktad till svenska privatpersoner som innehar minst en uppkopplad enhet utöver en smartphone, läsplatta eller dator. En enhet i denna studie är definierad som att den är uppkopplad med hjälp av ett nätverk för att ha möjlighet att kommunicera med andra enheter och användaren. Studien är inte inriktad på enheter som används inom det dagliga arbetet hos olika institut. Den kommer endast rikta sig till personer som är 18 år eller äldre, då vi tror att valet att införskaffa enheten/enheterna är högre då snittåldern för att flytta från föräldrahemmet i Sverige ligger på strax över 18 år (Haglund 2015). Respondenterna har som en konsekvens av detta hunnit bilda sig en egen uppfattning, istället för att tagit till sig någon annans.

Det finns flertalet olika perspektiv som en studie kring ämnet hade kunnat ha sin utgångspunkt ifrån. Studien kommer dock endast att utgå från användarperspektivet, det vill säga hur användarnas syn och åsikter på ämnet denna studie behandlar.

2 Metod

2.1 Metodansats

För att undersöka hur användare av uppkopplade enheter i smarta hem ser på säkerhet utifrån autentisering och beteendeanpassning har en kvantitativ metod tillämpats. En kvantitativ metod innebär att empiri som samlas in är standardiserad och kan analyseras på ett statistiskt sätt, vanligtvis genom någon form av enkät eller standardiserade intervjuer (Jacobsen 2017). En kvantitativ metod börjar med insamling av information för att utveckla en teori/-er kring ett eller flera fenomen som sedan testas utifrån den insamlade empirin (Recker 2013).

När empirin var insamlad så sammanställdes den statistiskt för att möjliggöra generalisering av svaren utifrån den undersökta populationen. Både Recker (2013) och Jacobsen (2017) menar att en kvantitativ metod är att föredra vid generalisering när ett större antal enheter undersöks. Den kvantitativa metoden är fokuserad på siffror och mängd, och då siffror kan ses som ett starkt belägg på hur fenomen fungerar, styrker det valet av metod (Recker 2013).

Kvalitén på en kvantitativ studie beror på tillförlitligheten i den insamlade informationen. Författarna måste säkerställa att de har god validitet samt reliabilitet för att uppnå detta (Davidson & Patel 2019). Dessa två aspekter går att läsa i avsnittet (” 2.6 Validitet”) respektive (”2.7 Reliabilitet”).

Den kvalitativa metoden ansågs irrelevant för studien då den inte baseras på mätning, utan lägger vikten vid ord (Jacobsen 2017; Recker 2013).

2.2 Forskningsstrategi

Vanligtvis tillämpas en deduktiv ansats när en kvantitativ metod används (McCartan & Robson 2016) vilket gjordes i denna studie. En deduktiv ansats innebär att studien börjar med att samla in information, teori, och slutligen empiri (Recker 2013; Jacobsen 2017). Studien började med en litteraturgranskning där teori inhämtades. Utifrån den drogs slutsatsen att det fanns en brist på undersökningar och forskning med användarperspektiv. De flesta undersökningar som gjorts inom området hade haft fokus på existerande säkerhetsrisker och användningsområden. Detta ledde till att empiri samlades in för att undersöka hur användarna ser på säkerhetsrisker kring digital lagring och användning av privat information, med fokus

på autentisering och beteendeanpassning. Detta gjordes för dels ökad kunskap, samt testa slutsatser som den tidigare forskningen presenterat.

Motsatsen till deduktiv ansats är induktiv, vilket innebär att empirin samlas in först och sedan formas teorier utifrån empirin (Jacobsen 2017; McCartan & Robson 2016; Recker 2013). Denna ansats används i regel tillsammans med den kvalitativa metoden och då denna studie använder sig av en kvantitativ metod, har den induktiva ansatsen inte tillämpats.

2.3 Litteraturstudie

Vid studiens början genomfördes en litteraturstudie för att få en överblick över den befintliga forskningen på området. Backman (2016) menar att litteraturgranskning främst används för att samla tidigare forskning och sedan presentera den som bakgrund i den valda frågan. Utifrån litteraturgranskningen kunde ett område identifieras där det saknades kunskap och därefter togs beslutet att undersöka området, vilket litteraturgranskningen kan användas till (Backman 2016). Den kan även användas för att identifiera områden som behöver utforskas mer, ge vägledning på metodformuleringar samt val av metod och analysmetod. Resultatet av litteraturgranskningen presenteras i huvudsak i avsnittet ("1.2 Tidigare forskning"), samt en viss del i ("1.1 Bakgrund"). Problemdiskussionen baseras sedan på dessa. Den tidigare forskningen används även i kapitlet ("3 Teoretiskt ramverk"). Det teoretiska ramverket ger först en kortare beskrivning av smarta hem, vilket sedan följs av en presentation av säkerhetsrisker, där sedan en fördjupning görs inom autentisering och beteendeanpassning.

För att identifiera och samla in relevant forskning och teorier kring området har två databaser använts, Primo och Scopus där tillgången till dessa givits av biblioteket på Högskolan i Borås. Informationen inhämtades främst från vetenskapliga artiklar som var "Peer reviewed", vilket innebär att de är granskade av ämnesexperter innan de får publiceras (Moberg 2015). Denna process säkerställde att källorna höll en hög nivå och var tillförlitliga. Ett fåtal hemsidor har använts. Dessa har blivit kritiskt granskade av författarna innan användning och jämförda med vad de vetenskapliga artiklarna hävdar om samma ämne. Anledningen till att hemsidor använts är för att de stundtals gav enklare förklaringar om samma ämne/fenomen, jämfört med artiklarna. För att öka kvaliteten och legitimiteten av informationen som presenteras behöver två eller fler källor beskriva samma fenomen på liknande sätt (Jacobsen 2017), vilket har tillämpats av författarna i stor utsträckning.

Vid insamlingen av information om hur studier bör genomföras har biblioteket på Högskolan i Borås använts för att hitta böcker om metodik och uppsatsskrivande. Även andra kandidatuppsatser har granskats för att identifiera lämpliga böcker inom ämnet.

2.4 Enkätundersökning

Till denna studie valdes en webbaserad enkätundersökning som insamlingsmetod för att samla empiri. Enkäten utformades med hjälp av verktyget ”Google formulär”. Val av metod berodde på det faktum att när författare vill nå och undersöka specifika grupper så är det lättare med enkätundersökningar (Cohen, Manion & Morrison 2007). Enkäter är av fördel när författarna vill inhämta information om populationers handlingar, uppfattningar och åsikter kring en fråga eller fenomen (Recker 2013). Vidare är de även ett bra tillvägagångssätt när studien har som målsättning att undersöka och jämföra relationer mellan olika variabler (Recker 2013). Studier som baseras på enkäter har även fördelen att de minskar tiden det tar att samla och bearbeta data, samt att deltagarna kan genomföra den när det passar dem (Cohen, Manion & Morrison 2007; Jacobsen 2017).

Utifrån litteraturstudien och det teoretiska ramverk som skapades har olika teman tagits fram. Det är med dessa som utgångspunkt som enkäten utformades, bestående av 18 frågor.

2.4.1 Utformning av enkät

Respondenterna möttes först av ett välkomstmeddelande som beskrev vad enkäten skulle handla om, vad den skulle användas till, samt vilka som låg bakom den. Den innehöll information om kraven för att få besvara den, och uppfyllde inte respondenterna detta krav tackades de ändå för visat intresse. Enkäten bestod främst av slutna frågor då de möjliggör jämförelser mellan olika frågor för att kunna identifiera eventuella mönster mellan dem (Cohen, Manion & Morrison 2007). Analyser kan därmed göras relativt snabbt, eftersom författarna redan vet karaktären på kategorierna och svaren. Genom att ge respondenten fasta svarsalternativ kan sedan statistiska analyser genomföras på empirin som inkommit (Cohen, Manion & Morrison 2007).

På ett fåtal ställen i enkäten valde författarna att ge respondenterna möjlighet att komplettera sina svar genom att ställa öppna följdfrågor som var valfria att besvara. Öppna frågor ger respondenter möjligheten att ge mer personifierade svar och kan leda till att den som besvarar enkäten delar med sig om information och synpunkter som inte hade fångats upp i en helt sluten enkät (Cohen, Manion & Morrison 2007; Jacobsen 2017). Detta resulterade i att ett stort antal delade med sig av olika produkter de använder och säkerhetsåtgärder de vidtagit, som författarna inte hade gett exempel på i svarsalternativen.

För att säkerställa att enkäten höll hög kvalitet, samt att inga tvetydigheter rådde kring någon fråga eller svarsalternativ utgick författarna utifrån anvisningar och uppmaningar från litteratur på hur enkäter bör utformas.

Samma begrepp kan tolkas olika av skilda respondenter (Jacobsen 2017). Enkäten bearbetades därmed flertalet gånger för att se till att språkbruket var anpassat till målgruppen, då formuleringen av frågor och svarsalternativ bör vara enkla och lättförståeliga (McCartan & Robson 2016; Jacobsen 2017). Författarna bör undvika att frågorna inte är ledande för att undvika att det antyds att ett alternativ skulle vara bättre än det andra (McCartan & Robson 2016; Jacobsen 2017). Detta kan leda till att författarna skapar åsikter, istället för att få fram de befintliga (McCartan & Robson 2016). Eftersom författarna ansåg att det var svårt att själva avgöra detta så efterfrågades återkoppling på frågorna när den skickades ut i Pilotstudien.

Vidare menar McCartan & Robson (2016) att frågorna inte ska upplevas som för långa, vilket innebar att ett flertal frågor omformulerades med färre ord, men med samma betydelse. Risk att det ställs dubbelfrågor (två saker frågas samtidigt) finns även vid långa frågor (McCartan & Robson 2016). Författarna granskade frågorna konsekvent för att försäkra sig om att det gick snabbt att läsa igenom dem, och att inte mer än en fråga ställdes vid varje fråga.

Frågor med dess tillhörande svarsalternativ bör presenteras på en sida, inte flera (Cohen, Manion & Morrison 2007). Som följd såg författarna till att enkäten bara bestod av en sida. På grund av att frågor inte bör ha för många tillhörande svarsalternativ (Jacobsen 2017) användes max sex svarsalternativ (med undantag vid frågorna kring ålder och användningsområden) vid samtliga frågor.

Författarna har även följt Cohen, Manion & Morrison (2007) direktiv kring de visuella aspekterna som bör tas i beaktning vid utformning av en webbaserad enkät. Bakgrundsfärger

och text designades konsekvent med samma färgskala och formalia för att se till att det blev lättare att navigera i enkäten. Dessutom undveks visuella skillnader i presentationen av svarsalternativ genom att följdriktigt använda samma svarsskala vid frågor av värderingskaraktär.

2.4.2 Pilotstudie

Innan studien anses redo för pilottestning bör den ha genomgått en pre-pilot (Cohen, Manion & Morrison 2007; Recker 2013). Syftet är att få ett första utkast på återkoppling om vad respondenter tycker om enkäten, att frågorna är relevanta, om den är visuellt presentabel samt klara upp eventuella oklarheter. De som deltagit i pre-piloten bör sedan även delta i den riktiga pilotstudien (Recker 2013). En selektiv grupp av individer valdes ut och tillfrågades om de ville delta. Utifrån responsen från dem ändrades olika delar i enkäten. Författarna presenterade sedan enkäten, med dess justeringar, för sin handledare som gav ytterligare feedback och fler korrigeringar gjordes.

Samma individer som deltog i pre-pilotstudien medverkade även i pilotstudien. Med hänsyn till den slutgiltiga återkopplingen från deltagarna i pilotstudien gjordes några mindre justeringar. Efter detta ansåg författarna att enkäten var redo att distribueras till eventuella respondenter.

2.5 Urval

Mot bakgrunden att 93% av svenskarna har en dator, 92% innehar en smartphone samt att 70% har minst en surfplatta i hemmet (Internetstiftelsen 2019) riktade sig denna studie till de som hade minst en uppkopplad enhet i sitt hem, utöver de tre ovannämnda. Detta på grund av att studien riktade sig till dem som anammat konceptet ”smart hem” i högre grad.

Enkäten gjordes tillgänglig i en svensk grupp på Facebook som behandlar automatisering av hemmet, som vid tidpunkten den gjordes tillgänglig hade drygt 37 tusen medlemmar. Därmed var den inte tillgänglig för personer som inte var medlem i denna grupp. Alla som ville bli medlemmar i gruppen vid tidpunkten enkäten var öppen för svar var tvungna att ansöka om medlemskap. Gruppen var därmed sluten för alla icke-medlemmar. De som ville gå med ombads att motivera varför de skulle bli beviljade åtkomst till den för att undvika att botar registrerade sig.

Ett inlägg i gruppen gjordes av författarna där de frågade medlemmarna om de ville besvara den. Ett påminnelse-inlägg gjordes under sista dagen enkäten var öppen. Totalt låg den öppen i sju dagar. Ytterligare två grupper kontaktades om lov för att lägga ut enkäten i de respektive grupperna. Den ena gruppen gav inte tillåtelse, medans den andra gav det, men gjorde så efter att enkäten hade stängts ner. Fler grupper som berörde automatisering av hemmet identifierades, men ansågs av författarna vara för nischade inom specifika smarthem-kategorier.

Alla de som författarna har intresse att undersöka kallas teoretisk population. Detta betyder att de som väljs att undersökas ska likna hela populationen (Jacobsen 2017). I denna studie var det användare av uppkopplade enheter inom en specifik Facebookgrupp som var populationen, således en begränsning av den totala populationen. Eftersom enkäten endast var åtkomlig i en specifik grupp på en social plattform kan representationen av användare till viss del upplevts ytterligare begränsad eftersom det uteslutande var en svensk grupp. Jacobsen (2017) beskriver emellertid hur författare tenderar att utgå från ett begränsat geografiskt kriterium. Då studien avgränsades till enbart svenska användare påträffades den önskade, men begränsade populationen likväl.

Cohen, Manion & Morrison (2007) menar att det är lätt hänt att fel respondenter väljs ut och konsekvensen blir att resultatet inte representerar målgruppens åsikter. Genom att inte göra den tillgänglig för alla minskade risken att detta skulle inträffa.

Till viss del tillämpades ett av de icke-sannolikhetsurval som Jacobsen (2017) beskriver, nämligen bekvämlighetsurval. Detta innebär att författarna väljer ut de respondenter som på ett enkelt sätt kan nås. Detta gällde dock endast ett fåtal som besvarade enkäten (14%). Problemet med ett sådant urval är att det minskar möjligheterna till att generalisera till andra grupper (Jacobsen 2017). Eftersom syftet med studien inte var att kunna generalisera resultatet till fler grupper än användare av uppkopplade enheter hemma var detta problem inte av någon större relevans för författarna.

2.6 Validitet

Studien kan anses som giltig om författarna mäter och undersöker det som de har till syfte att undersöka (Jacobsen 2017; Recker 2013). Det måste finnas en koppling mellan det empiriska materialet och de matematiska uttrycken i de kvantitativa relationerna. Författarna måste se till att de teoretiska koncepten har en tydlig koppling till den data som samlats in (Recker 2013). Uppnås inte detta så kan studien anses vara oanvändbar (Cohen, Manion & Morrison 2007). Studiens syfte var att undersöka användarperspektivet kring lagring och användning av privat information av uppkopplade enheter, vilket bidrog till att syftet med studien kunde uppfattas och beskrivas som ytterst abstrakt.

För att uppnå validitet utgick författarna utifrån de två validitets principer som Recker (2013) beskriver; face- och innehållsvaliditet. För att åstadkomma det förstnämnda behöver författarna se till att tillvägagångssättet studien genomförs på stämmer överens med den underliggande teorin (Recker 2013). Genom att endast låta användare av uppkopplade enheter i sina hem besvara enkäten uppnåddes detta.

Innehållsvaliditet är ett mått på hur väl frågorna stämmer överens med teorin, med andra ord att frågorna samlar in essensen av de teoretiska begreppen (Recker 2013). Det grundläggande för denna process är att se till att studien mäter det den ska mäta, att inget saknas, samt att icke relevant information tas bort (Jacobsen 2017). Validitet i innehållet uppnås därmed genom att vara noga vid datainsamlingen (Cohen, Manion & Morrison 2007). Genom att utforma enkäten parallellt med det teoretiska ramverket säkerställdes att frågorna i enkäten hade en tydlig koppling med den teori som skulle undersökas. Frågorna formades därmed utifrån de fyra olika teman det teoretiska ramverket bestod av; Smarta hem, Säkerhetsrisker, Autentisering och Beteendeanpassning (kapitel 3).

Frågeställningen studien hade som syfte att besvara kunde, utöver att uppfattas som abstrakt, även anses vara komplex och omfattande. Komplicerade fenomen bör inte mätas en enskild fråga, eftersom de i regel består av flertalet delar (Cohen, Manion & Morrison 2007; Jacobsen 2017). Enkäten utformades som följd av detta faktum till att bestå av flertalet delfrågor som behandlade olika aspekter utifrån användarnas syn på digital lagring och användning av privat information.

Cohen, Manion & Morrison (2007) menar vidare att det går att minska risken för att studien anses vara ogiltig genom att se till att urvalet som deltar i studien är representativt. Genom att

endast göra enkäten tillgänglig för medlemmar i en grupp som behandlar automatisering av hem minskade risken att obehöriga ej besvarade enkäten. De som valdes ut av författarna att besvara den som inte var medlemmar i denna grupp informerades att de var tvungna att uppnå kraven för att besvara enkäten, annars fick de inte lämna svar på den.

2.7 Reliabilitet

Reliabilitet innebär att undersökningen ska gå att återskapa med liknande förutsättningar och få samma resultat, att mätvariablerna mäter de teoretiska koncepten konsekvent och precist (Jacobsen 2017; Recker 2013). Problem med reliabiliteten kan uppstå från subjektiva observationer och datainsamlingar, samt från dåligt formulerade och/eller icke precisa frågor. Dock är den kvantitativa metoden mer objektiv än de flesta datainsamlingsmetoder, vilket ökar reliabiliteten (Recker 2013). För att säkerställa att frågorna i enkäten inte var dåligt formulerade och icke precisa, genomfördes en pilotstudie där frågorna testades innan enkäten skickades ut, för att öka reliabiliteten ytterligare. En bilaga med enkätfrågorna finns också att ta del av i uppsatsen (kapitel 7), vilket gör att framtida forskare kan använda samma frågor.

2.8 Etik

När en studie genomförs som på något sätt involverar människor måste personerna som genomför studien förhålla sig till etiska restriktioner. Detta är särskilt viktigt om studien behandlar ämnen såsom brott och sociala sårbarheter (McCartan & Robson 2016). När studien undersöker hur människor förhåller sig till något tenderar studien att medvetet eller omedvetet att associera det nya konceptet som positivt, och det gamla som negativt. Människor kan då påverkas och pressas till ställningstagande om att det ”nya” är den bättre vägen att gå efter (McCartan & Robson 2016). På grund av detta lades betydligt med resurser på att säkerställa att enkätsbeskrivningen samt frågorna och svarsalternativen som enkäten bestod av inte på något sätt antydde att det ena alternativet skulle vara mer positivt-laddat än de andra.

Ingen information som kan användas för att identifiera de individer som deltar i studien får utges (Cohen, Manion & Morrison 2007; McCartan & Robson 2016; Recker 2013). Hänsynen till integritet bryts lätt under studiers gång, eller efter studien har genomförts (Cohen, Manion & Morrison 2007). För att undvika detta scenario efterfrågades ingen information såsom namn, adress eller sysselsättning. Enkäten var frivillig att besvara, vilket den bör vara i alla studier (Cohen, Manion & Morrison 2007; McCartan & Robson 2016; Recker 2013). Om en

person hade påbörjat enkäten, men sedan beslutat sig för att inte fortskrida, kunde hen när som avbryta sitt deltagande genom att kryssa ner den.

De som genomför studien bör ta i beaktning om de håller inne på information om studiens egentliga syfte (McCartan & Robson 2016). De bör även informera om potentiella risker med studien (Recker 2013). För att säkerställa detta skrevs en informationstext om vilket ämne enkäten behandlade, vad resultatet från den skulle användas till, samt vilka som låg bakom enkäten innan deltagarna kunde klicka på den bifogade länken till enkäten i Facebookgruppen. I pilotstudien bads deltagarna att återberätta vad de ansåg enkätens syfte vara. Först när en gemensam bild gavs av samtliga presenterades den för handledare för ytterligare feedback.

2.9 Analysmetod

Det finns tre typer av data som fås från en enkät; nominell, ordinal och metrisk (Cohen, Manion & Morrison 2007; Jacobsen 2017). Utifrån nominella data går det att skilja på respondenter som har kryssat för olika svar, med andra ord likheter och skillnader. Med ordinal data går det även att rangordna kategorierna i förhållande till varandra, till exempel högt-lågt. Med metriska data går det sedan att göra en exakt rangordning av kategorierna, vad som skiljer de åt. Ett exempel på detta är att en femtioåring är dubbelt så gammal som en tjugofemåring (Jacobsen 2017). I denna studie är den största delen av data som presenteras nominell.

Innan analysen gjordes genomfördes en granskning av alla svar för att se att alla svar var ifyllda, vilket enligt McCartan & Robson (2016) är viktigt att kontrollera då synen på en fråga kan skilja sig från de som svarat och de som inte svarat. Resultatet var att alla respondenter hade svarat på alla obligatoriska frågor.

Det gjordes en univariat analys av data, vilket innebär att frågorna analyseras en och en (Jacobsen 2017; Recker 2013). Resultatet av analysen presenteras sedan i avsnitt ”4.1 Resultatanalys på univariat data”. För att ge läsaren en övergripande och tydlig bild över resultatet så har det visualiserats genom stapel- och cirkeldiagram, vilket Cohen, Manion & Morrison (2007) och Jacobsen (2017) rekommenderar att författarna gör. Jacobsen (2017)

menar att de öppna frågorna kan delas in i olika teman och sedan presenteras. Detta gjordes, och sedan angavs det hur många som tagit upp svarsalternativ inom respektive tema.

Utöver den univariata analysen har en bivariat analys av data genomförts. I den analyseras sambandet mellan två variabler (Jacobsen 2017; Recker 2013). För att genomföra den bivariata analysen har det statistiska verktyget 'Statistical Package for Social Sciences' (SPSS) använts. När enkäten stängdes exporterades all data till ett Excelark som sedan importerades in i SPSS. Det gjordes även en kontroll så all data var korrekt i SPSS, detta då Recker (2013) menar att det kan ske bortfall eller uppstå oriktigheter vid export och import av data. Analysen består av tre delar, en mer allmän del, en om autentisering och en gällande beteendeanpassning. Resultatet presenteras i tabeller vilket är ett enkelt och vanligt sätt att presentera en bivariat analys (McCartan & Robson 2016).

2.10 Metoddiskussion

Cohen, Manion och Morrison (2007) anser att en nackdel med webb-enkäter är att vissa typer av grupper riskerar att bli underrepresenterade. Detta var inte av större betydelse för studien då urvalet fokuserade på användare av smarta hem och inte en enskild specifik typ av grupp av användare. Vidare påstår de att det kan uppstå tekniska problem såsom långsamt internet. Detta ansågs inte av författarna var av större bekymmer då 98% av de svenska hushållen har tillgång till internet, samt att 95% av de som använder internet har en egen smartphone (Internetstiftelsen 2019).

Enligt både Jacobsen (2017) och Recker (2013) är en nackdel med kvantitativ metod att den har en låg svarsfrekvens, vilket Recker (2013) sedan menar kan ha en påverkan på generaliserbarheten. I Facebookgruppen där enkäten delades var det drygt 37 tusen medlemmar när enkäten var tillgänglig, vilket ger en låg svarsfrekvens. Detta eftersom det inkom 135 svar på enkäten, varav några svar kom från respondenter som inte var med i gruppen. Det fanns dock ingen statistik på hur många av de 37 tusen som sett enkäten, vilket gör det problematiskt att räkna ut en svarsfrekvens på exakt hur många som sett enkäten jämfört med hur många som svarat på den. För att ha haft möjlighet att ge en exakt svarsfrekvens hade personer kunnat väljas ut slumpmässigt ur gruppen och blivit tillfrågade en och en. Detta ansågs dock för tidskrävande för studien. Det hade dessutom inneburit att samtliga som deltog hade gjort det utifrån ett bekvämlighetsurval, vilket inte var syftet.

3 Teoretiskt ramverk

3.1 Smarta Hem

Ett smart hem kan definieras som ”/.../ en bostad med ett internetanslutet datorsystem för att automatisera och styra tekniska system (hemautomatisering)” – Nationalencyklopedin (u.å).

Smarta hem tjänster innebär att produkter eller system i ett hem är uppkopplade och kan kommunicera med varandra. Genom detta möjliggörs att vissa aktiviteter i hushållet kan bli automatiserade. Det här innebär mer bekvämlighet för användarna, då det blir mindre att göra och komma ihåg, eftersom enheterna sköter det åt oss (Miller 2015). Genom smarta hem ökar användares bekvämlighet genom automatisering, säkerhet, energieffektivisering, och för vissa specifika användare – hälsa och assistans (Cook & Rashidi 2009). Smart hem-enheter inkluderar allt från vitvaror, belysning, uttag och övervakning (Miller 2015).

Målet för smarta hem-miljöer blir att anpassa sig efter personerna som befinner sig i denna miljö för att kunna underlätta, samt förbättra livskvalitén (Pau et al. 2019). Det är dock en bit kvar tills det finns smarta hemsystem som kan ta intelligenta beslut och anpassa sig autonomt efter användarna. Idag går det att dela in smarta hemsystem i tre olika nivåer. Den första är aktioner via fjärrstyrning. Här krävs det fortfarande input från användaren för att något ska ske. Den andra nivån använder sig utav enheter som känner av omgivningen och samlar in information om den och sedan utför aktioner baserat på fördefinierade regler. Den sista och tredje nivån innebär personlig service och en mer användarvänlig upplevelse. Här anpassar sig systemet till omgivningen, men också till användarens beteenden automatiskt. Det innebär att systemen har möjligheter att lära sig och sedan kunna förutse användarens beteenden. Idag är majoriteten av smarta hemsystem på den andra nivån (Liang, Liu, Ye, Zeng & Zou 2018).

Genom denna anpassning kan enheter i smarta hem förbättra användarkomforten genom att använda kontextmedvetenhet (kontexten användarna befinner sig i och hur de agerar) för att urskilja/utmärka lokalisering, identitet och aktiviteter och skapa en förståelse för de olika förhållanden mellan olika enheter och de som använder dem (Alam, Ali & Reaz 2012).

3.2 Säkerhetsrisker

Ju smartare ett hem blir, desto mer komplexa och sammankopplade blir de, vilket kan skapa beroenden som kan minska tillförlitligheten. Till exempel slutar enheterna fungera vid ett strömavbrott (Furszyfer & Sovacool 2020). Säkerhetsrisker kring privatliv, såsom att få sin personliga information stulen, har en stor negativ påverkan på användarnas tillit till sina enheter och därmed deras attityd kring smarta hem (Mashal & Shuhaiber 2019). Vidare spelar säkerhetsrisker, vid exempelvis autentisering och datasäkerhet en stor roll för att lyckas med integrationen av enheter i hemmen (Kalra & Sood 2015).

När enheter och apparater som tidigare inte varit uppkopplade blir det medföljer flertalet risker då nätverket som enheterna är uppkopplade mot går att nå utanför huset, även om huset i sig är säkert (Lin & Bergmann 2016). Idag beräknas cirka 80% av alla uppkopplade enheter i hemmet vara sårbara för olika typer av attacker (Rambus u.å).

Exempelvis är kommunikationen som sker mellan olika uppkopplade enheter sårbara för avlyssning och andra metoder som har som mål att komma åt personers privata data. Det kan leda till förlust av integritet för användarna, med mistande av autentiseringsdata som följd. Enheterna är i behov av en förbättrad och mer robust autentiseringsprocess för att säkerställa att användarnas data är skyddade (Borgohain et al. 2015; Maras 2015).

Vidare menar Furzyfer & Sovacool (2020) att de tre vanligaste riskerna är en kombination av integritet, säkerhet och hackning, teknisk tillförlitlighet/garantier samt interoperabilitet. Hargreaves, Hauxwell-Baldwin och Wilson (2015) menar att oroligheter kring dessa områdena i kombination med användarvänlighet har en stark koppling till acceptansen hos användarna. För att kunna maximera smarta hems effektivitet och prestanda behöver dessa samla in stora mängder data gällande andra enheter, samt om användarens och dess vanor och beteenden. Detta skapar allvarliga risker då sådan information kan stjälas, hackas eller missbrukas (Furszyfer & Sovacool 2020). Användarna saknar även kunskap om vilken information som enheterna genererar. En anledning till detta kan vara att det konstant kommer ny teknologi och nya produkter, vilket gör det svårt att skapa sig en överblick över vad som faktiskt lagras, och vem som kan använda den informationen (Atzori, Iera & Morabito 2010).

Avsaknaden av interoperabilitet och standarder för olika uppkopplade enheter är ett problem då olika företag anammar olika strategier och förhållningssätt till dessa enheter. Företag såsom Apple och Google har skapat ekosystem som består av deras egna produkter, men med avsaknaden av standarder och en begränsad förmåga att kommunicera med enheter som inte tillhör samma ekosystem, kan det skapa problem för dess användare (Andonova et al. 2015). Bergmann och Lin (2016) hävdar att det är väldigt få smarta hem-enheter som får regelbundna säkerhetsuppdateringar. Kalra & Sood (2015) belyser en annan risk, nämligen att de flesta enheter har väldigt limiterad datakraft och lagring, vilket gör att det inte går att implementera komplicerade säkerhetsalgoritmer. Även de mest krypterade säkerhetsprotokoll kan bli hackade (Kalra & Sood 2015).

En attack mot en samtrafikordningsenhet (hub) kan till leda till att en hackare får tillgång till autentiseringsmaterial och kan då ändra den. En hackare kan därmed få tillgång till alla enheter i nätverket och dess information (Awad & Bako 2018).

3.2.1 Autentisering

Autentisering är att kunna bekräfta en användares identitet, användaren är den som den utger sig för att vara. Autentisering från ett digitalt perspektiv innebär att garantera att användaren har behörighet till användning, alternativt koppla upp sig till ett system eller kopplas ihop med ett användarkonto. Vanligtvis används ett användarnamn och lösenord för att autentisera sig, men det är dessvärre en mindre säker metod då det är vanligt att personer använder samma användarnamn och lösenord på flera ställen (Borgohain et al. 2015). Det räcker att en obehörig får tillgång till ett konto för sedan kunna komma åt flera andra konton (Awad & Bako 2018).

I och med att smarta hem har förmågan att ändra hur människor interagerar med sin omgivning är det essentiellt att varje distinkt enhet innehar en hög säkerhetsnivå, med tanke på att dessa lagrar och använder privat information (You et al. 2019). Genom att hacka en enhet kan en person få tillgång till alla andra enheter genom att skapa sig tillgång till autentiseringsdata. Utomstående har möjlighet att manipulera och/eller fabricera felaktiga data, utan att användarna har någon aning om det (Awad & Bako 2018). På grund av detta kan smarta hem liknas vid glashus: ett skrämmande yttre som ger bilden av att vara ogenomträngligt, men som inte kan försvara sig mot inre hot och vars väggar lätt kan krackelera (Liu et al. 2018).

Ett sätt att öka säkerheten kring autentisering är som användare använda sig av tvåfaktorsautentisering eller multifaktorsautentisering. Tvåfaktorsautentisering är när det krävs en kod som bara användaren har tillgång till, utöver användarnamn och lösenord. Multifaktorsautentisering ger ytterligare en dimension med säkerhet. Det är dock sällsynt och används mestadels när system har exceptionellt höga krav gällande säkerheten. Den vanligaste autentiseringsmetoden här är fingertrycksavläsning, men det finns även ansikts- och ögonavläsning (Borghain et al. 2015). Det finns även en viss optimism bland användare som leder till att de underestimerar risken att bli utsatt för något hot, exempelvis tror de inte att just de kommer bli utsatta för en attack (Barbosa et al. 2019).

3.2.2 Beteendeanpassning

För att det smarta hemmet ska kunna anpassa sig efter omgivningen och användaren så används maskininlärning tillsammans med olika sensorer (Cook & Rashidi 2009). Enheterna är i stort behov av att kunna resonera sig fram till handlingar som baseras på data från andra enheter och sensorer, samt vad användarna gör för att kunna förbättra livskvaliteten och öka bekvämligheten (Chen et al. 2016). Miller (2015) menar vidare att eftersom enheterna i hemmet har lagrad data om vem du är, vad du gör, när du gör det och hur du gör det, kan det få förödande konsekvenser för individerna om den informationen hamnar i fel händer. Atzori, Iera & Morabito (2010) är inne på samma spår och påstår att användare saknar kunskap om vilken information som enheterna genererar. Maras (2015) bestryker detta ytterligare och betonar att användarens rätt till integritet är hotad, eftersom de inte har någon kontroll över hur mycket och vilken information som distribueras mellan enheterna.

Enheterna har kapacitet att öka välbefinnandet hos användarna (Pau et al. 2019) i form av bland annat ökad bekvämlighet och användarvänlighet. Användarna har dock en begränsad kontroll över hur enheterna samlar och lagrar privat information och hur företagen skickar informationen vidare (Maras 2015). Informationen som lagras kan vara värdefull ur ett marknadsföringssyfte, då företag kan identifiera potentiella kunder genom att de lär sig sina användares beteenden och preferenser (Marketing-Schools.org u.å) Barbosa et al. (2019) hävdar även att användare inte skulle vara villiga att dela med sig av deras data, även om de fick rabatter i utbyte. De flesta användarna förväntar sig nämligen att rätten till integritet inte ska kosta extra utan vara inkluderat från början.

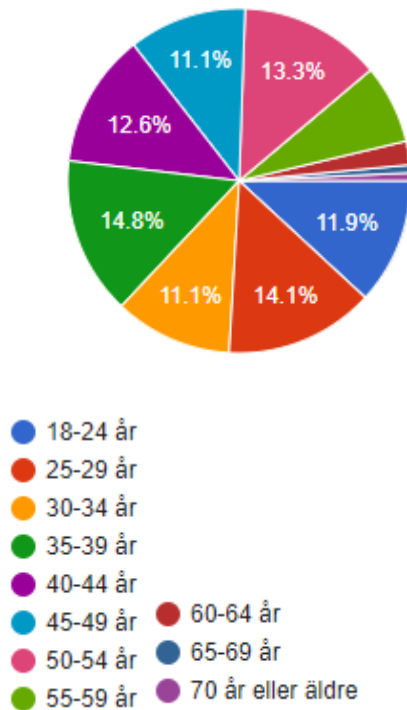
Användare står inför svåra val kring om hur mycket de vill öka bekvämlighet och användarvänlighet hos sina enheter i förhållande till vilken information de vill dela med sig av. Vill en användare skydda sig mot inkräktare i sitt hem med hjälp av kameraövervakning kommer även användaren att behöva bli övervakad av samma system (Miller 2015).

4 Resultat

4.1 Resultat av univariat data

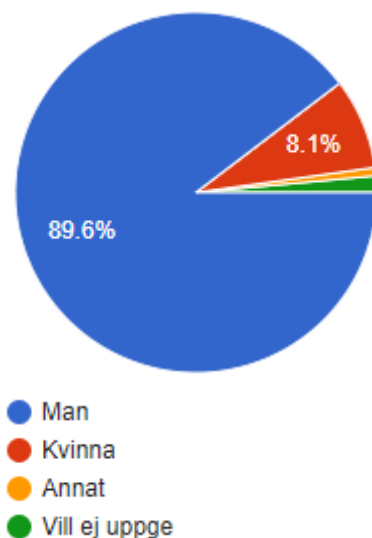
Fråga 1. Hur gammal är du?

Figur 4.1 ålder



Från figur 4.1 går det att se att den största åldersgruppen är 35–39 år med nästan 15%, tätt följd av åldersgrupperna från 18–24 år upp till 50–54 år som alla ligger inom fyra procentenheter. De minsta grupperna är 65–69 år och 70 år eller äldre där det finns en respondent i respektive åldersgrupp.

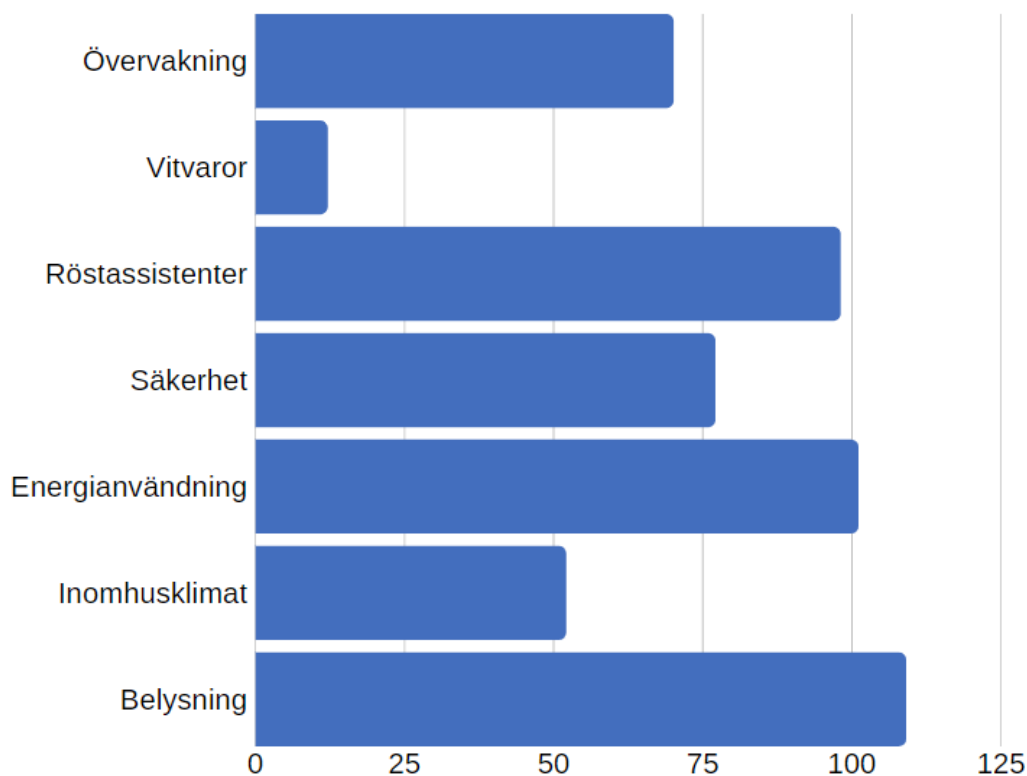
Fråga 2. Vad har du för könsidentitet?



Utifrån figur 4.2 går det att utläsa att nästan nio av tio respondenter är män och sedan är fyra femtedelar av de resterande respondenterna kvinnor.

Figur 4.2 Könsfördelning

Fråga 3. Inom vilka smarta hem-kategorier har du enheter?



Figur 4.3 Inom vilka kategorier har du enheter?

I tabell 4.3 går det att se att den största smarta hem-kategorin är belysning, med nästan 110 respondenter som angett denna kategori. Belysningen är tätt följd av kategorierna energianvändning och röstassistenter. Den minsta kategorin är vitvaror där knappt en av tio av respondenterna innehar enheter.

Efter fråga 3 ställdes följdfrågan: Använder du något annat än alternativen ovan?

Beskriv gärna kortfattat.

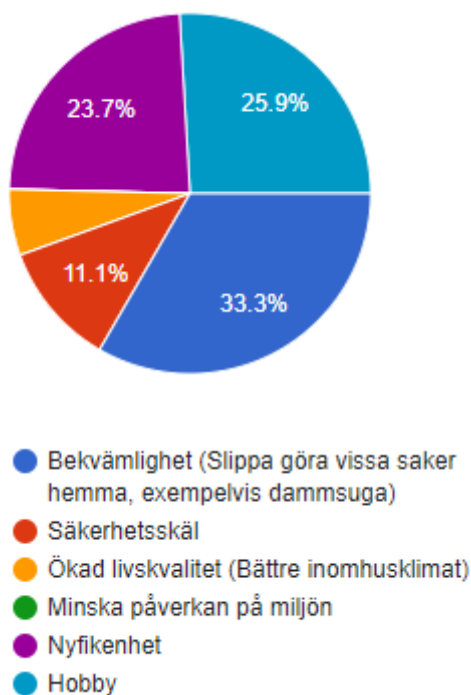
Svar:

Av alla svar som inkom var det dessa två som nämndes tre gånger eller fler.

Robotdammsugare (13st)

Gräsklippare (3st)

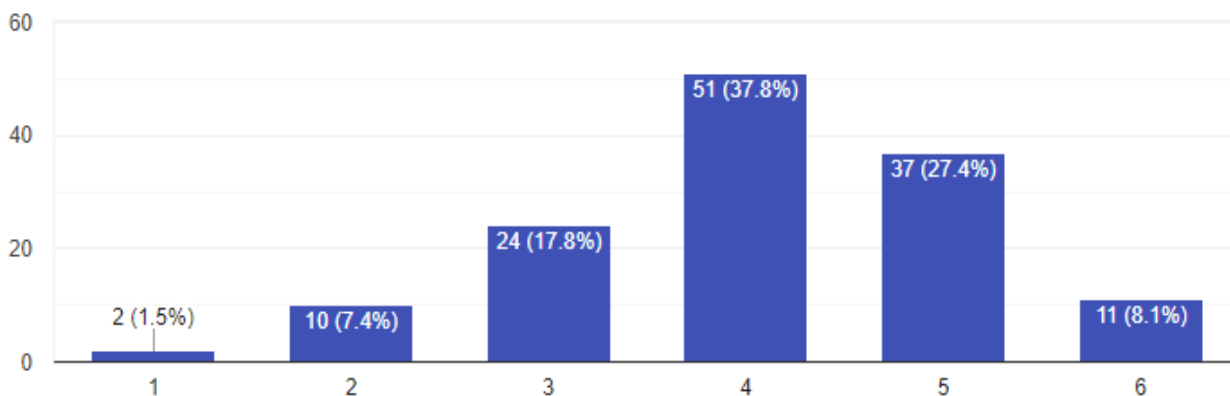
Fråga 4. Vilken är huvudanledningen till att du införskaffade din smarta enhet/enheter?



Från figur 4.4 går det att utläsa att den största anledningen till att respondenterna införskaffade sina enheter är bekvämlighet, som en tredjedel valt. Ungefär en fjärdedel har valt nyfikenhet respektive hobby. Ingen av respondenterna har valt minskad påverkan på miljön. Bortsett från den är säkerhet den minsta kategorin.

Figur 4.4 Anledning till införskaffande av enhet/enheter

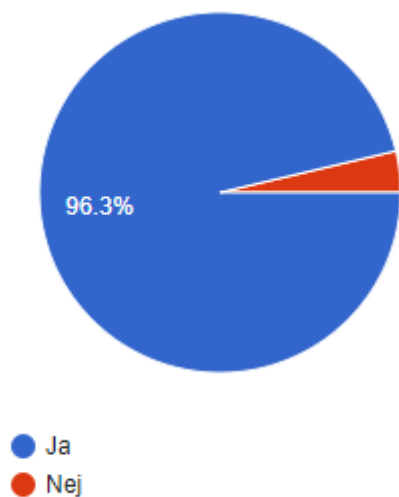
Fråga 5. På en skala 1–6, hur stor tillit har du till säkerheten hos din enhet/enheter? 1 = Inte alls, 6 = Mycket stor.



Figur 4.5 Hur stor tillit har du till säkerheten hos din enhet/enheter

Utifrån figur 4.1 går det att se att nästan tre fjärdedelar har tillit till säkerheten hos sina enheter, men nästan hälften av dem har bara lite mer tillit än inte.

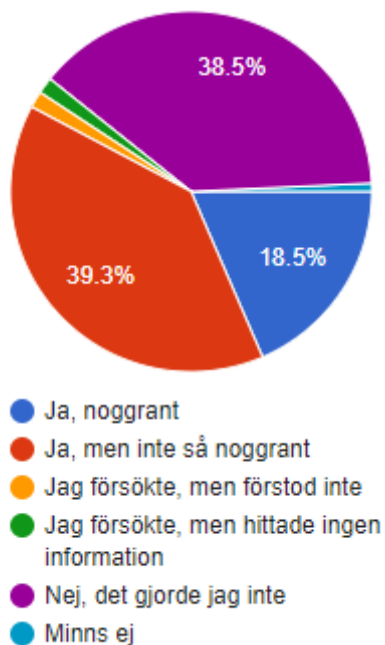
Fråga 6. Är du medveten om att smarta-enheter ofta samlar in och lagrar personlig information om dig? (Förutom inloggningsuppgifter eller andra nödvändiga uppgifter för att enheterna skall fungera)



Från figur 4.6 går det att se att nästan alla av respondenterna är medvetna att smarta enheter samlar in och lagrar information om dem.

Figur 4.6 Är du medveten att smarta-enheter ofta samlar in och lagrar information?

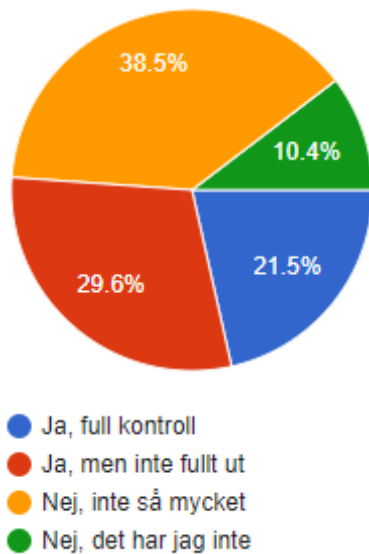
Fråga 7. Har du kollat upp vilken information som din enhet/enheter lagrar?



I figur 4.7 går det att utläsa att nästan sex av tio respondenter har kollat upp vilken information som lagras av sina enheter, och av dem är det ungefär hälften som gjort det noggrant. Av de resterande respondenterna var det bara några enstaka som försökte kolla upp vilken information som lagrades och resten har inte gjort det.

Figur 4.7 Kollat upp vilken information enheten lagrar?

Fråga 8. Känner du att du har kontroll (det vill säga möjlighet att kunna påverka) över vilken information som lagras och används av din enhet/enheter?



Utifrån figur 4.8 går det att se att nästan hälften upplever att de har någon sorts kontroll, antingen full kontroll eller kontroll men inte fullt ut över vilken information som lagras. Den andra hälften upplever att de har ingen kontroll eller inte så mycket kontroll.

Figur 4.8 Har du kontroll över vilken information som lagras och används?

Efter fråga 8 ställdes följdfrågan: ”Om inte, varför då?”

Angivna skäl:

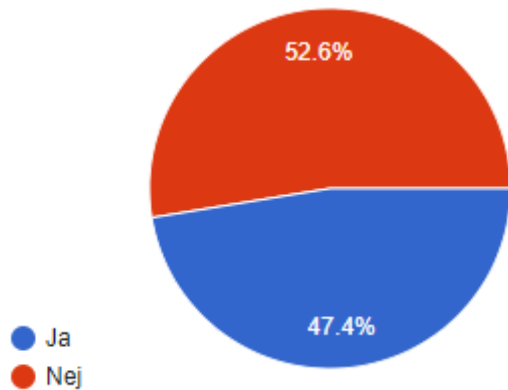
Bryr mig inte/inte tagit reda på om jag kan (nämnt av 12st)

Funktionen/tjänsten kräver viss information (7st)

Framgår inte av tillverkaren/företagen gör som de vill ändå (5st)

Svårt att kontrollera (4st)

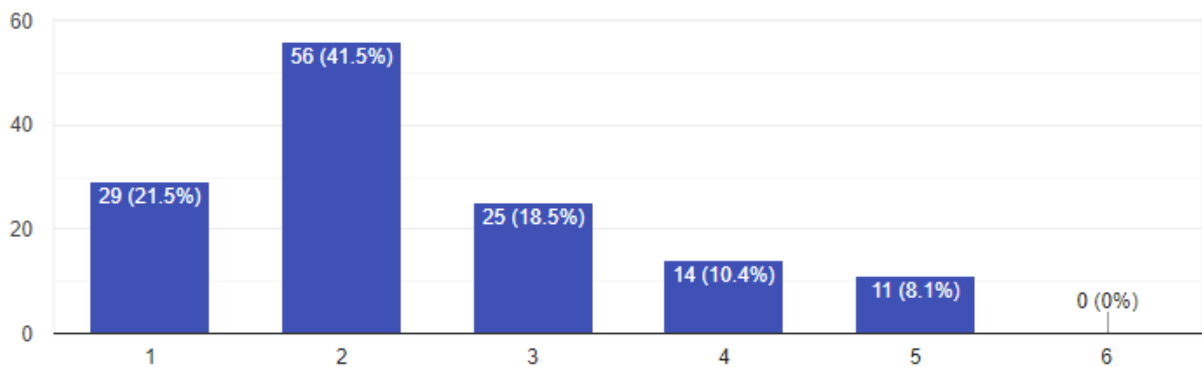
Fråga 9. Har du någon gång undvikit att införskaffa en enhet på grund av informationen den vill lagra och använda?



Från figur 4.9 går det att utläsa att nästan hälften av respondenterna har undvikit att införskaffa sig en enhet på grund av information den vill lagra och använda.

Figur 4.9 Undvikit att införskaffa en enhet?

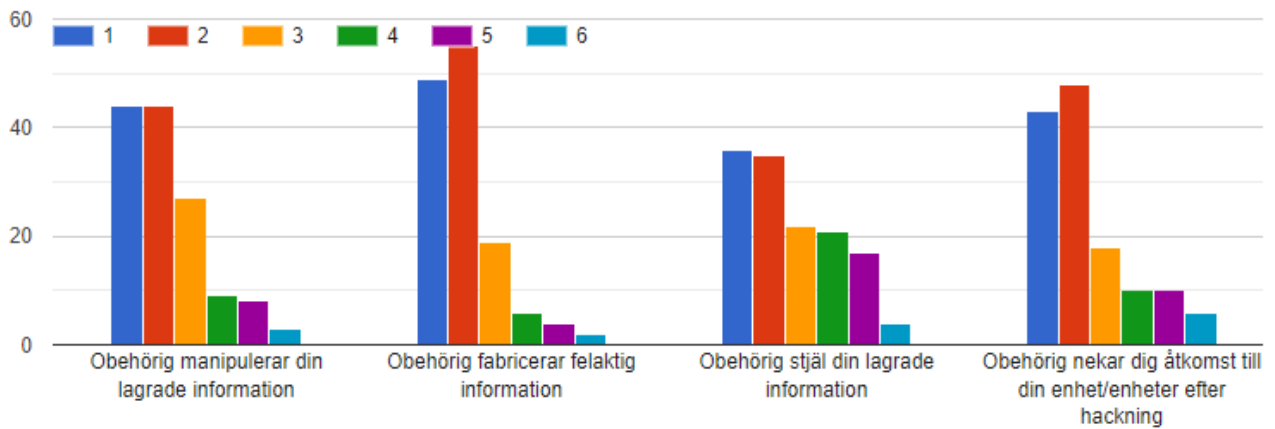
Fråga 10. På en skala 1–6, hur orolig är du att obehöriga kan, via till exempel hackning, skapa sig tillgång till din enhet/enheter? 1 = Inte orolig, 6 = Mycket orolig.



Figur 4.10 Hur orolig är du att obehöriga kan skapa sig tillgång?

I figur 4.10 går det att se att drygt åtta av tio inte är eller inte är så oroliga över att någon obehörig kan skapa sig tillgång till deras enheter.

Fråga 11. Här följer ett par alternativ. Vi vill att du tar ställning till varje alternativ utifrån hur troligt det är att dessa skulle kunna hända dig och din enhet/enheter? 1 = Inte troligt, 6 = Högst troligt.



Figur 4.11 Troligt att detta händer dig?

Utifrån figur 4.11 går det att se att respondenterna i stor utsträckning inte anser det särskilt troligt att någon obehörig fabricerar felaktig data, manipulerar deras data eller nekar dem åtkomst till sina enheter. De anser det dock lite troligare att en obehörig skulle stjäla deras information, men fortfarande mindre troligt att det skulle ske.

Fråga 12. Har du vidtagit egna åtgärder för att försäkra dig om att det bara är du som har tillgång till dina enheter?



Från figur 4.12 går det att utläsa att nästan hälften av respondenterna har vidtagit några åtgärder för att säkerställa att det är just de som har tillgång till sina enheter. En knapp femtedel har vidtagit någon enstaka åtgärd och nästan en tredjedel har inte vidtagit någon åtgärd.

Figur 4.12 Har du vidtagit egna åtgärder?

Efter fråga 12 ställdes följdfrågan: Om du svarat ja på frågan ovanför, ge gärna exempel på hur.

Angivna åtgärder:

Åtgärder som rör internetåtkomsten för enheterna (41st)

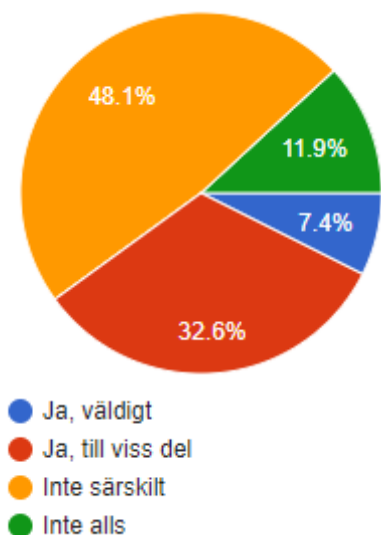
Extra starka lösenord (20st)

Två- eller flerfaktorsautentisering (10st)

Inga molnbaserade produkter (6st)

Säkerhetsinställningar (3st)

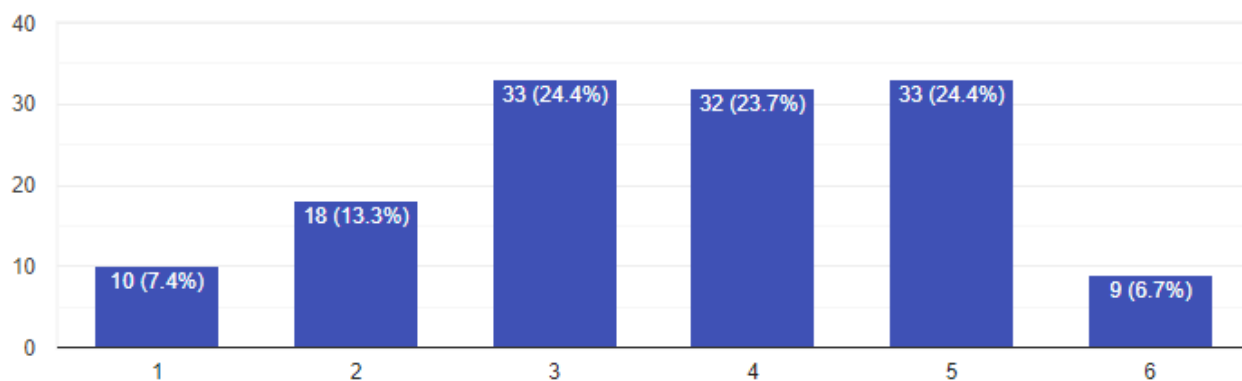
Fråga 13. Är du orolig att produkttillverkare av smarta hem-enheter skapar sig åtkomst till din information från andra enheter i ditt hem, utan din tillåtelse?



I figur 4.13 går det att se att knappt hälften inte är särskilt oroliga över att produkttillverkare skapar sig åtkomst till deras information utan tillåtelse. 40% är till viss del eller väldigt oroliga och drygt en av tio är inte alls oroliga.

Figur 4.13 Orolig att produkttillverkare skapar sig åtkomst till din information?

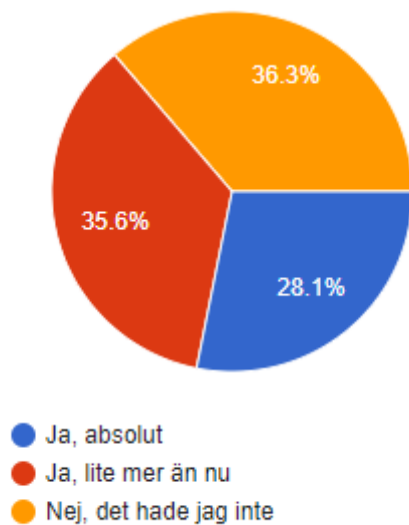
Fråga 14. På en skala 1–6, vad tycker du om att enheter skulle kunna använda lagrad information om dina vanor och beteenden för att försöka öka användarvänligheten? 1 = Mycket obehagligt, 6 = Mycket tilltalande.



Figur 4.14 Åsikt om att enheter använder lagrad information?

Utifrån 4.14 går det att utläsa att en knapp majoritet av respondenterna anser det mer tilltalande än inte att enheterna skulle använda lagrad information om deras vanor för att få ökad bekvämlighet. Drygt hälften av de respondenter som anser det obehagligt tycker att det är lite mer obehagligt än tilltalande.

Fråga 15. Skulle du vara villig att ge tillgång till mer personlig information till din enhet/enheter om det hade lett till ökad bekvämlighet (slippa göra vissa saker hemma, exempelvis dammsuga)?



Från figur 4.15 går det att se att nästan två tredjedelar skulle vara villiga att ge enheterna mer, eller lite mer tillgång till personlig information för ökad bekvämlighet.

Figur 4.15 Tillgång till mer personlig information?

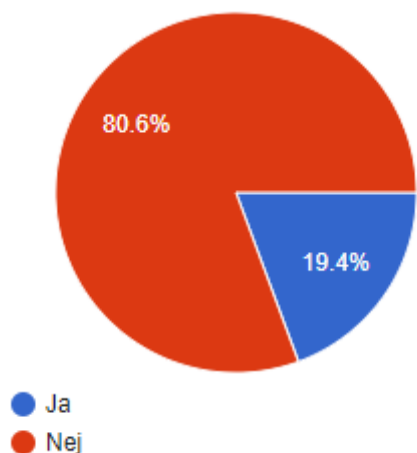
Fråga 16. Skulle du vara villig att dela med dig av din information från enheterna, till exempelvis enhetens tillverkare eller dess samarbetspartners i marknadsföringssyfte? Detta för att ge dig anpassade erbjudanden utifrån dina preferenser och vanor.



I figur 4.16 går det att utläsa att bara en av tio skulle vara villiga att dela med sig av information i marknadsföringssyfte och drygt hälften skulle inte göra det.

Figur 4.16 Information mot erbjudanden?

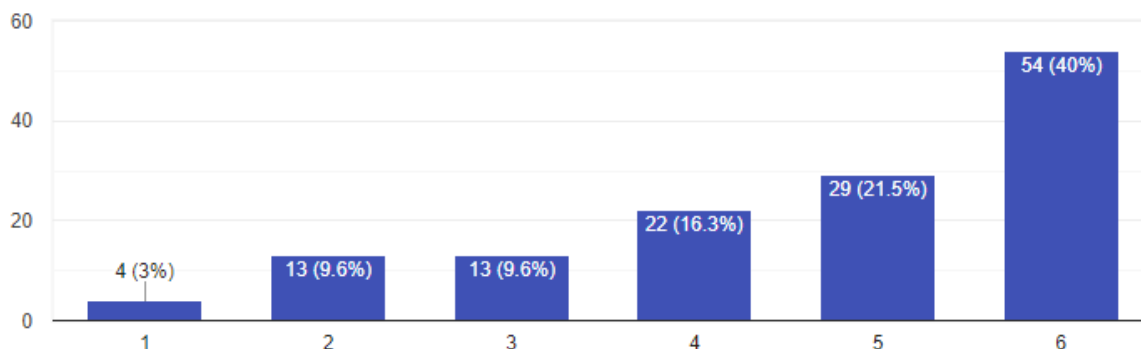
Fråga 17. Om du svarat "Tveksamt" eller "Nej" på förgående fråga, skulle du svara "Ja" om du fick rabatter i utbyte mot informationen?



Utifrån figur 4.17 går det att se att två av tio av de som svarade "Nej eller "Tveksamt" på fråga skulle 16 vara villiga att ge ut information i marknadsföringssyfte i utbyte mot rabatter.

Figur 4.17 Information mot rabatter?

Fråga 18. Du kommer nu ställas inför ett scenario. Vi vill att du på en skala 1–6 ger din syn på detta: Du kommer hem från jobbet och din bil skickar en signal till garageporten så den öppnas. När garageporten öppnas så tänds belysningen i ditt hem automatiskt. När belysningen tänts och garageporten öppnats så startas kaffemaskinen, då den lärt sig att du brukar dricka kaffe efter jobbet.



Figur 4.18 Syn på hög automatisering

Från figur 4.8 går det att se en klar majoritet som tycker att scenariot som presenteras låter fantastiskt, nästan åtta av tio. Fyra av tio har gett scenariot det högsta som går.

4.2 Resultat av bivariat data

Jämförelser mellan olika variabler presenteras nedan. Jämförelser mellan frågor inom respektive teman har gjorts, samt mellan variabler inom temat ”Säkerhetsrisker” jämt mot ”Autentisering” och ”Beteendeanpassning”. Detta kan hänföras till frågeställningen:

- *Hur ser användare av uppkopplade-enheter i smarta hem på säkerhet utifrån autentisering och beteendeanpassning?*

Med detta i beaktning har inga jämförelser mellan variabler inom ”Autentisering” och ”Beteendeanpassning” gjorts mellan varandra. Detta på grund av att dessa sågs som två separata områden, som inte har en lika tydlig koppling mellan varandra. Författarna anser inte att denna typ av jämförelse är omöjlig att utföra, men på grund av tidsbrist valt att inte genomföra. Detta då denna typ av jämförelse ansågs mer tidskrävande och komplex.

Tabell. 4.1 Jämförelse mellan ålder och tillit till säkerheten hos enheterna

5. På en skala 1-6, hur stor tillit har du till säkerheten hos din enhet/enheter? 1 = Inte alls, 6 = Mycket stor.

		1	2	3	4	5	6	Total
1. Hur gammal är du?	18-24 år		12,5%	12,5%	25,0%	25,0%	25,0%	100,0%
	25-29 år		10,5%	31,6%	26,3%	26,3%	5,3%	100,0%
	30-34 år		6,7%	20,0%	33,3%	26,7%	13,3%	100,0%
	35-39 år	5,0%	10,0%	25,0%	30,0%	20,0%	10,0%	100,0%
	40-44 år		5,9%		47,1%	41,2%	5,9%	100,0%
	45-49 år		6,7%	26,7%	60,0%	6,7%		100,0%
	50-54 år	5,6%		16,7%	38,9%	38,9%		100,0%
	55-59 år		10,0%		30,0%	50,0%	10,0%	100,0%
	60-64 år			33,3%	66,7%			100,0%
	65-69 år				100,0%			100,0%
	70 år eller äldre				100,0%			100,0%
Total		1,5%	7,4%	17,8%	37,8%	27,4%	8,1%	100,0%

Utifrån tabellen 4.1 går det att utläsa att det inte finns några signifikanta skillnader mellan ålder och tilliten till säkerheten hos enheterna. Den åldersgrupp med minst tillit är 25–29 år och den åldersgrupp med högst tillit är 40–44 år. Åldersgrupperna 65–69 år samt 70 år eller äldre har visserligen 100% tillit men det är bara en respondent i respektive åldersgrupp och anses därför inte vara den åldersgrupp med högst tillit.

Tabell 4.2 Jämförelse mellan könsidentitet och tillit till säkerheten hos enheterna

5. På en skala 1-6, hur stor tillit har du till säkerheten hos din enhet/enheter? 1 = Inte alls, 6 = Mycket stor.

		1	2	3	4	5	6	Total
2. Vad har du för könsidentitet?	Annat		100,0%					100,0%
	Kvinna			27,3%	27,3%	36,4%	9,1%	100,0%
	Man	1,7%	7,4%	17,4%	38,8%	27,3%	7,4%	100,0%
	Vill ej uppge				50,0%		50,0%	100,0%
Total		1,5%	7,4%	17,8%	37,8%	27,4%	8,1%	100,0%

I tabellen 4.2 går det att se kvinnor har något högre tillit än män men procentuellt sett så skiljer sig inte tilliten så mycket mellan män och kvinnor.

Tabell 4.3 Jämförelse mellan huvudanledning till införskaffande av smarta enheter och tillit till säkerheten hos enheterna

		5. På en skala 1-6, hur stor tillit har du till säkerheten hos din enhet/enheter? 1 = Inte alls, 6 = Mycket stor.						Total
		1	2	3	4	5	6	
4. Vilken är huvudanledningen till att du införskaffade din smarta enhet/enheter?	Bekvämlighet (Slippa göra vissa saker hemma, exempelvis dammsuga)		4,4%	28,9%	28,9%	22,2%	15,6%	100,0%
	Hobby	2,9%	11,4%	14,3%	37,1%	31,4%	2,9%	100,0%
	Nyfikenhet	3,1%	12,5%	18,8%	53,1%	9,4%	3,1%	100,0%
	Säkerhetsskäl				46,7%	46,7%	6,7%	100,0%
	Ökad livskvalitet (Bättre inomhusklimat)				12,5%	75,0%	12,5%	100,0%
Total		1,5%	7,4%	17,8%	37,8%	27,4%	8,1%	100,0%

I tabellen 4.3 går det att se hur tilliten till enheterna ser ut utifrån vilken som var huvudanledningen till att respondenten införskaffade enheterna. Det går att utläsa att den största procenten av svaren hamnat på svarsalternativet ”4” med nästan 38%. Vidare går det att se att alla som svarat ”Säkerhetsskäl” eller ”Ökad livskvalitet” har hög tillit till sina enheter. Ingen har svarat att de har låg tillit av dessa. Resten av svarsalternativen har också tillit, men inte i samma utsträckning. De som har svarat ”Säkerhetsskäl” har lägst tillit, 65%. Tätt därefter följer ”Nyfikenhet” som har fem procentenheter högre tillit. Drygt hälften av de som svarat ”Nyfikenhet” har svarat att de har lite mer tillit än inte och de som har högre tillit är drygt en av tio. Det verkar inte heller som det finns större skillnader inom samma svarsalternativ.

Tabell 4.4 Jämförelse mellan om respondenten kollat upp vilken information enheten/enheterna lagrar och om de undviker att införskaffa en enhet på grund av information den vill lagra

		9. Har du någon gång undvikit att införskaffa en enhet på grund av informationen den vill lagra och använda?		
		Ja	Nej	Total
7. Har du kollat upp vilken information som din enhet/enheter lagrar?	Ja, men inte så noggrant	56,6%	43,4%	100,0%
	Ja, noggrant	72,0%	28,0%	100,0%
	Jag försökte, men förstod inte	100,0%		100,0%
	Jag försökte, men hittade ingen information	50,0%	50,0%	100,0%
	Minns ej		100,0%	100,0%
	Nej, det gjorde jag inte	25,0%	75,0%	100,0%
Total		47,4%	52,6%	100,0%

Utifrån tabellen 4.4 går det att utläsa att det verkar finnas en samvariation med om respondenten har kollat upp vilken information som hans enheter lagrar och om hen har undvikit att införskaffa enheter på grund av information den vill lagra och använda. Sju av tio som noggrant hade kollat upp hade också valt att inte införskaffa en enhet, medan drygt hälften av de som

kollat upp, men inte så noggrant hade undvikit. Bland de som inte kollat upp vilken information som lagras var det en fjärdedel som valt att inte införskaffa en enhet.

Tabell 4.5 Jämförelse mellan hur orolig respondenten är att obehöriga får tillgång till sin enhet och hur troligt respondenten tror det är att någon manipulerar sin lagrade information

11. Här följer ett par alternativ. Vi vill att du tar ställning till varje alternativ utifrån hur troligt det är att dessa skulle kunna hända dig och din enhet/enheter. 1 = Inte troligt, 6 = Högst troligt [Obehörig manipulerar din lagrade information]

		1	2	3	4	5	6	Total
10. På en skala 1-6, hur orolig är du att obehöriga kan, via till exempel hackning, skapa sig tillgång till din enhet/enheter? 1 = Inte orolig, 6 = Mycket orolig	1	75,9%	24,1%					100,0%
	2	26,8%	46,4%	21,4%	3,6%	1,8%		100,0%
	3	4,0%	40,0%	36,0%	12,0%	8,0%		100,0%
	4	35,7%		21,4%	21,4%	7,1%	14,3%	100,0%
	5	9,1%	9,1%	27,3%	9,1%	36,4%	9,1%	100,0%
Total		32,6%	32,6%	20,0%	6,7%	5,9%	2,2%	100,0%

Från tabellen 4.5 går det att se att de som är oroliga över att bli hackade anser det mer troligt att någon skulle manipulera deras lagrade information. Nästan hälften av de som är oroliga anser det mer troligt än inte, medan drygt en av tio av de som är mindre oroliga anser det mindre troligt. Det som sticker ut är att de som inte alls är oroliga över att bli hackade är inte heller oroliga över att deras information skulle bli manipulerad.

Tabell 4.6 Jämförelse mellan hur orolig respondenten är att obehöriga får tillgång till sin enhet och hur troligt respondenten tror det är att någon fabricerar felaktig information

11. Här följer ett par alternativ. Vi vill att du tar ställning till varje alternativ utifrån hur troligt det är att dessa skulle kunna hända dig och din enhet/enheter. 1 = Inte troligt, 6 = Högst troligt [Obehörig fabricerar felaktig information]

		1	2	3	4	5	6	Total
10. På en skala 1-6, hur orolig är du att obehöriga kan, via till exempel hackning, skapa sig tillgång till din enhet/enheter? 1 = Inte orolig, 6 = Mycket orolig	1	75,9%	24,1%					100,0%
	2	28,6%	58,9%	10,7%		1,8%		100,0%
	3	16,0%	52,0%	16,0%	12,0%	4,0%		100,0%
	4	35,7%	7,1%	35,7%	7,1%		14,3%	100,0%
	5	18,2%	9,1%	36,4%	18,2%	18,2%		100,0%
Total		36,3%	40,7%	14,1%	4,4%	3,0%	1,5%	100,0%

I tabellen 4.6 går det att utläsa att en majoritet av de som är oroliga över att bli hackade inte anser det särskilt troligt att någon skulle fabricera felaktig information. Över 90% av de som inte är oroliga anser det inte heller särskilt troligt att någon skulle fabricera felaktig data.

Tabell 4.7 Jämförelse mellan hur orolig respondenten är att obehöriga får tillgång till sin enhet och hur troligt respondenten tror det är att någon stjälar hans lagrade information

11. Här följer ett par alternativ. Vi vill att du tar ställning till varje alternativ utifrån hur troligt det är att dessa skulle kunna hända dig och din enhet/enheter. 1 = Inte troligt, 6 = Högst troligt [Obehörig stjälar din lagrade information]

		1	2	3	4	5	6	Total
10. På en skala 1-6, hur orolig är du att obehöriga kan, via till exempel hackning, skapa sig tillgång till din enhet/enheter? 1 = Inte orolig, 6 = Mycket orolig	1	65,5%	24,1%	3,4%	3,4%	3,4%		100,0%
	2	19,6%	33,9%	12,5%	23,2%	10,7%		100,0%
	3	12,0%	20,0%	28,0%	24,0%	16,0%		100,0%
	4	21,4%	21,4%	28,6%	7,1%	14,3%	7,1%	100,0%
	5		9,1%	27,3%		36,4%	27,3%	100,0%
Total		26,7%	25,9%	16,3%	15,6%	12,6%	3,0%	100,0%

Utifrån tabellen 4.7 går det att se att en klar majoritet av de som är ganska oroliga över att bli hackade anser det troligt att deras information stjäls. Bland de som inte är oroliga alls eller inte är särskilt oroliga anser 80% att det inte är särskilt troligt att deras information stjäls. Drygt varannan av de som är lite mindre oroliga än mer oroliga anser det inte heller troligt att någon skulle stjäla deras information medan de som är lite mer oroliga än inte tror det är mindre troligt att information stjäls.

Tabell 4.8 Jämförelse mellan hur orolig respondenten är att obehöriga får tillgång till sin enhet och hur troligt respondenten tror det är att någon nekar hen tillgång till sin enhet

11. Här följer ett par alternativ. Vi vill att du tar ställning till varje alternativ utifrån hur troligt det är att dessa skulle kunna hända dig och din enhet/enheter. 1 = Inte troligt, 6 = Högst troligt [Obehörig nekar dig åtkomst till din enhet/enheter efter hackning]

		1	2	3	4	5	6	Total
10. På en skala 1-6, hur orolig är du att obehöriga kan, via till exempel hackning, skapa sig tillgång till din enhet/enheter? 1 = Inte orolig, 6 = Mycket orolig	1	75,9%	20,7%				3,4%	100,0%
	2	28,6%	44,6%	10,7%	5,4%	8,9%	1,8%	100,0%
	3	16,0%	28,0%	28,0%	16,0%	4,0%	8,0%	100,0%
	4		35,7%	35,7%	14,3%	7,1%	7,1%	100,0%
	5	9,1%	45,5%		9,1%	27,3%	9,1%	100,0%
Total		31,9%	35,6%	13,3%	7,4%	7,4%	4,4%	100,0%

I tabellen 4.8 går det att utläsa att en klar majoritet av de som inte är oroliga för att bli hackade även anser det inte särskilt troligt att en obehörig nekar dem åtkomst till sina enheter. Drygt sju av tio som är ganska oroliga över att bli hackade har dock svarat att de anser det mindre troligt att de skulle bli nekad åtkomst till sina enheter. Även bland de som är mest oroliga är det en knappt majoritet som menar att det är mindre troligt att de nekas åtkomst till sina enheter.

Tabell 4.9 Jämförelse mellan hur orolig respondenten är att obehöriga får tillgång till sin enhet och om respondenten vidtagit några egna åtgärder för att försäkra sig att bara hen har tillgång till sina enheter

		12. Har du vidtagit egna åtgärder för att försäkra dig om att det bara är du som har tillgång till dina enheter?			Total
		Ja, någon enstaka	Ja, några stycken	Nej	
10. På en skala 1-6, hur orolig är du att obehöriga kan, via till exempel hackning, skapa sig tillgång till din enhet/enheter? 1 = Inte orolig, 6 = Mycket orolig	1	10,3%	55,2%	34,5%	100,0%
	2	23,2%	50,0%	26,8%	100,0%
	3	12,0%	40,0%	48,0%	100,0%
	4	35,7%	35,7%	28,6%	100,0%
	5	9,1%	72,7%	18,2%	100,0%
Total		18,5%	49,6%	31,9%	100,0%

Från tabellen 4.9 går det att utläsa ett möjligt mönster mellan hur orolig respondenten är över att någon obehörig får tillgång till dess enheter och ifall denne har vidtagit åtgärder för att försäkra sig att bara just denne har tillgång till sina enheter. Nästan 70% av de som är ganska oroliga har svarat att de har vidtagit flera åtgärder och knapp tiondel har vidtagit en åtgärd. Av de som inte är oroliga alls så har en tydlig majoritet vidtagit en eller flera åtgärder, dock i en mindre utsträckning än de som är oroliga. Det som sticker ut är de som svarat att de är mindre oroliga än oroliga, där har nästan hälften svarat än att de inte vidtagit åtgärder, vilket är mest av samtliga grupper.

Tabell 4.10 Jämförelse mellan hur orolig respondenten är att obehöriga får tillgång till sin enhet och hur orolig respondenten är att en produkttillverkare skapar sig åtkomst till hens information från andra enheter i hemmet

		13. Är du orolig att produkttillverkare av smarta hem-enheter skapar sig åtkomst till din information från andra enheter i ditt hem, utan din tillåtelse?				Total
		Inte alls	Inte särskilt	Ja, till viss del	Ja, väldigt	
10. På en skala 1-6, hur orolig är du att obehöriga kan, via till exempel hackning, skapa sig tillgång till din enhet/enheter? 1 = Inte orolig, 6 = Mycket orolig	1	41,4%	48,3%	6,9%	3,4%	100,0%
	2	7,1%	51,8%	39,3%	1,8%	100,0%
	3		52,0%	32,0%	16,0%	100,0%
	4		50,0%	50,0%		100,0%
	5		18,2%	45,5%	36,4%	100,0%
Total		11,9%	48,1%	32,6%	7,4%	100,0%

Utifrån tabellen 4.10 går det att se att de som är oroliga över att en obehöriga får tillgång till deras enheter också är oroliga över att produkttillverkare skapar sig tillgång till deras information, utan deras tillåtelse. Bland de som svarat att de inte alls är oroliga över att en obehörig får tillgång till deras enheter har drygt nio av tio svarat att de inte är särskilt oroliga över produkttillverkarna. Dock är det nästan bara sex av tio som inte är särskilt över att

produkttillverkarna skapar sig åtkomst till deras information av de som är lite oroliga över att bli hackade. Av de respondenter som bara är lite mer eller lite mindre oroliga över att bli hackade har ungefär hälften svarat att de inte är särskilt oroliga eller att de är till viss del oroliga/väldigt oroliga.

Tabell 4.11 Jämförelse mellan om respondenten vidtagit några egna åtgärder för att försäkra sig att bara hen har tillgång till sina enheter och hur stor tillit de har till säkerheten hos sin enhet/enheter

		5. På en skala 1-6, hur stor tillit har du till säkerheten hos din enhet/enheter? 1 = Inte alls, 6 = Mycket stor.						
		1	2	3	4	5	6	Total
12. Har du vidtagit egna åtgärder för att försäkra dig om att det bara är du som har tillgång till dina enheter?	Ja, någon enstaka		8,0%	28,0%	28,0%	28,0%	8,0%	100,0%
	Ja, några stycken	3,0%	7,5%	11,9%	43,3%	28,4%	6,0%	100,0%
	Nej		7,0%	20,9%	34,9%	25,6%	11,6%	100,0%
Total		1,5%	7,4%	17,8%	37,8%	27,4%	8,1%	100,0%

I tabellen 4.11 går det att utläsa att som vidtagit några åtgärder har lägst tillit till säkerheten hos enheterna och de som inte vidtagit några åtgärder har mer tillit än de som vidtagit någon enstaka.

Tabell 4.12 Jämförelse mellan om respondenten är villig att ge tillgång till mer personlig information och hur stor tillit de har till säkerheten hos sin enhet/enheter

		5. På en skala 1-6, hur stor tillit har du till säkerheten hos din enhet/enheter? 1 = Inte alls, 6 = Mycket stor.						
		1	2	3	4	5	6	Total
15. Skulle du vara villig att ge tillgång till mer personlig information till din enhet/enheter om det hade lett till ökad bekvämlighet (slippa göra vissa saker hemma, exempelvis dammsuga)?	Ja, absolut		2,6%	10,5%	47,4%	28,9%	10,5%	100,0%
	Ja, lite mer än nu		8,3%	12,5%	33,3%	37,5%	8,3%	100,0%
	Nej, det hade jag inte	4,1%	10,2%	28,6%	34,7%	16,3%	6,1%	100,0%
Total		1,5%	7,4%	17,8%	37,8%	27,4%	8,1%	100,0%

Utifrån tabellen 4.12 går det att de som är villiga att ge ut mer personlig information för ökad bekvämlighet har en tillit till säkerheten, drygt åtta av tio har mer tillit än inte. Av de som inte skulle ge ut mer information är det drygt 57% som har tillit till enheterna.

Tabell 4.13 Jämförelse mellan om respondenten är villig att ge tillgång till mer personlig information och om respondenten är villig att dela med sig av information i marknadsföringssyfte

		16. Skulle du vara villig att dela med dig av din information från enheterna, till exempelvis enhetens tillverkare eller dess samarbetspartners i marknadsföringssyfte? Detta för att ge dig anpassade erbjudanden utifrån dina preferenser och vanor.			
		Ja, det skulle jag	Nej, det skulle jag inte	Tveksamt	Total
15. Skulle du vara villig att ge tillgång till mer personlig information till din enhet/enheter om det hade lett till ökad bekvämlighet (slippa göra vissa saker hemma, exempelvis dammsuga)?	Ja, absolut	28,9%	42,1%	28,9%	100,0%
	Ja, lite mer än nu	4,2%	45,8%	50,0%	100,0%
	Nej, det hade jag inte	2,0%	75,5%	22,4%	100,0%
Total		10,4%	55,6%	34,1%	100,0%

Från tabellen 4.13 går det att utläsa att knappt tre av tio som absolut skulle ge ut mer information för ökad bekvämlighet är villiga att dela med sig av sin information i marknadsföringssyfte (exempelvis för att kunna få anpassade erbjudanden). Lika många svarade även tveksamt ur den gruppen. Bland de som skulle gett ut lite mer information än nu är hälften tveksamma till att ge ut information i marknadsföringssyfte och nästan svarade att de inte skulle göra det. Tre fjärdedelar av alla som inte skulle ge ut information för ökad bekvämlighet skulle inte ge ut information i marknadsföringssyfte och nästan alla av de resterande var tveksamma till det.

Tabell 4.14 Jämförelse mellan om respondenten är villig att dela med sig av information i marknadsföringssyfte och hur stor tillit de har till säkerheten hos sin enhet/enheter

		5. På en skala 1-6, hur stor tillit har du till säkerheten hos din enhet/enheter? 1 = Inte alls, 6 = Mycket stor.						
		1	2	3	4	5	6	Total
16. Skulle du vara villig att dela med dig av din information från enheterna, till exempelvis enhetens tillverkare eller dess samarbetspartners i marknadsföringssyfte? Detta för att ge dig anpassade erbjudanden utifrån dina preferenser och vanor.	Ja, det skulle jag			7,1%	50,0%	35,7%	7,1%	100,0%
	Nej, det skulle jag inte	2,7%	6,7%	18,7%	40,0%	22,7%	9,3%	100,0%
	Tveksamt		10,9%	19,6%	30,4%	32,6%	6,5%	100,0%
Total		1,5%	7,4%	17,8%	37,8%	27,4%	8,1%	100,0%

I tabellen 4.14 går det att se att de som är villiga att ge ut information i marknadsföringssyfte har en tillit till säkerheten hos enheterna, där drygt nio av tio har tillit. Av de som är tveksamma eller inte skulle göra det så är det sju av tio som har tillit till enheterna.

Tabell 4.15 Jämförelse mellan om respondenten är villig att ge tillgång till mer personlig information och respondentens syn på ett scenario

		18. Du kommer nu ställas inför ett scenario. Vi vill att du på en skala 1-6 ger din syn på detta: Du kommer hem från jobbet och din bil skickar en signal till garageporten så den öppnas. När garageporten öppnas så tänds belysningen i ditt hem automatiskt. När belysningen tänts och garageporten öppnats så startas kaffemaskinen, då den lärt sig att du brukar dricka kaffe efter jobbet.						
		1	2	3	4	5	6	Total
15. Skulle du vara villig att ge tillgång till mer personlig information till din enhet/enheter om det hade lett till ökad bekvämlighet (slippa göra vissa saker hemma, exempelvis dammsuga)?	Ja, absolut				5,3%	21,1%	73,7%	100,0%
	Ja, lite mer än nu	6,3%	4,2%	6,3%	27,1%	20,8%	35,4%	100,0%
	Nej, det hade jag inte	2,0%	22,4%	20,4%	14,3%	22,4%	18,4%	100,0%
Total		3,0%	9,6%	9,6%	16,3%	21,5%	40,0%	100,0%

Utifrån tabellen 4.15 går det att se att alla som absolut skulle ge ut information för ökad bekvämlighet tycker att scenariot som presenterades i fråga 18 låter mer fantastiskt än obehagligt. Även de som svarat att de skulle ge ut lite mer information ännu är positivt inställda till scenariot. Det är bara drygt 16% av de som tycker det låter mer obehagligt. Bland de som inte skulle ge ut mer information är det en knapp majoritet som tycker det låter mer fantastiskt än obehagligt.

5 Analys och diskussion

Denna del av studien har delats upp utifrån de fyra olika teman som presenterades i det teoretiska ramverket (kapitel 3). Uppdelningen har gjorts för att skapa en tydlighet kring vilka aspekter som analyseras och diskuteras. Analyserna med tillhörande diskussion utgår från det presenterade resultatet (kapitel 4) tidigare forskning (avsnitt 1.2) och det teoretiska ramverket (kapitel 3).

5.1 Smarta hem

Det är en relativt jämn fördelning mellan de olika användningsområdeskategorier användare har uppkopplade enheter inom. Miller (2015) menar att belysning är en av vanligaste kategorierna. Detta bestryks av resultatet som visar att det är den vanligaste kategorin. Energianvändning är inte långt efter i resultatet, vilket bestryks när Cook & Rashidi (2009) & Miller (2015) påstår att det är ett av de främsta områdena. Knappt var tionde person använde sig av uppkopplade vitvaror, vilket stämmer överens med teorin, då det endast är Miller (2015) som diskuterar vitvarors roll i smarta hem. Cook & Rashidi (2009) menar att säkerhet är bland de största fokusområdena, tillsammans med Miller (2015) som även hävdar att övervakning är det. Det går att utläsa från resultatet att övervakning och säkerhet är två betydande kategorier, som dessutom är starkt kopplade till varandra. Även detta stämmer väl överens med teorin, där bland annat Alam, Ali & Reaz (2012) och Kim & Robles (2010) diskuterar hur implementerade säkerhetssystem kan underlätta för hushåll vid eventuella nätsituationer.

Främsta anledningen till att användare använder sig av uppkopplade enheter, enligt både studien och teorin är bekvämlighet. Intressant är att bara drygt elva procent uppger att säkerhet var huvudanledningen till införskaffandet, men det är över hälften som använder enheter inom denna kategori. Detta faktum är både framstående och notabelt eftersom Alam, Ali & Reaz (2012); Cook & Rashidi (2009); Kim & Robles (2010) & Miller (2015) alla påstår att säkerhet är ett av de främsta områdena inom smarta hem.

Studien har också visat att nästan 60% har kollat upp vilken information som lagras av deras enheter, och av dessa har 64% valt att inte införskaffa en enhet på grund av informationen den vill lagra och använda. Det har visat att flertalet användare försöker ha kontroll och vara medvetna om vilken information som lagras. Faktumet överensstämmer inte helt med teorin,

som främst påstått att användare saknar kunskap om ämnet. En stor andel hävdar ändå att de inte har kontroll över den lagrade informationen, men det gäller inte för majoriteten.

Ingen respondent menar att minska påverkan på miljön har varit den drivande faktorn till att skaffa enheter, vilket ingen tidigare litteratur har diskuterat kring dess betydelse för användarna. Visserligen använder sig tre fjärdedelar av respondenterna av enheter inom energianvändning, men ingen av dessa menade att miljön skulle vara huvudanledningen till införskaffandet av dessa enheter.

5.2 Säkerhetsrisker

Teorin menar att tilliten till säkerheten hos enheterna är knapp på grund av att det inte tas på allvar. Det stämmer inte överens med studiens resultat som visar att 7 av 10 har mer tillit än misstro till säkerheten hos enheterna. Användarnas tilltro till säkerheten stämmer inte helt överens med teorin, där Chen, Huang & Zhu (2016) tvärtom menar att enheter tenderar att inte operera som användarna har föreställt sig på grund av bristande säkerhet. Dessutom är misstron till säkerheten hos enheterna orsaken till att tilliten till dem minskar (Mashal & Shuhaiber 2019), vilket inte går att utläsa från resultatet. Maras (2015) menar att när ny IoT-teknologi kontinuerligt kommer ut på marknaden är det svårt att skaffa sig en överblick över vad som faktiskt lagras. Detta går att tyda från resultatet, där knappt var femte person har noggrant undersökt vilken information enheterna lagrar, samtidigt som det endast är några fler procent som menar att de även har full kontroll över vilken information som lagras och används av enheterna.

Atzori, Iera & Morabito (2010) hävdar att användare saknar kunskap om vilken information som enheterna genererar, lagrar samt vem som kan använda denna information. Detta påstående går det som tidigare nämnts att hitta visst stöd för, men samtidigt visar resultatet en annan intressant aspekt. Inom gruppen respondenter som antingen har uppgivit att de noggrant, eller till viss del har kollat upp vilken information som lagras (knappt 60%) har över hälften av dessa tagit beslutet att någon gång inte införskaffa en enhet på grund av informationen den vill lagra och använda. Faktumet överensstämmer därmed inte helt med vad litteraturen hävdar. Vidare går det att utläsa att generellt är användare mer medvetna och mindre oroliga för säkerhetsrisker än vad tidigare litteratur menat på. Resultatet ger även sken av ett mönster mellan de som har en hög tillit till säkerheten hos enheterna, och villigheten att ge ut information. En individ med stor tillit är mer villig att ge ut information, jämfört med en

individ med mindre tillit. Att användare som har högre tillit även tenderar att vara mer villiga att ge ut mer information är inte särskilt anmärkningsvärt. Om resultatet istället visat tvärtom, att de som har lägre tillit även är de som är mer villiga att ge ut information, hade detta faktum troligtvis betraktats som oerhört uppseendeväckande.

Det finns ingen samvariation mellan att tilliten till säkerheten skulle vara annorlunda mellan olika könsidentiteter eller åldrar inom litteraturen. Detta återspeglas i resultatet, där det inte återfinns någon större skillnad mellan dessa.

De som införskaffar sina enheter av säkerhetsskäl eller ökad livskvalité som huvudanledning tenderar att ha en högre tilltro till säkerheten hos sina enheter. Samtliga respondenter som uppgivit något av dessa två anledningar har alla en relativt hög till mycket hög tilltro till säkerheten. Däremot går det att se att de som främst har skaffat enheter på grund av att de har det som hobby eller nyfikenhet generellt har mindre tilltro till säkerheten, jämfört med övriga.

Avsaknaden av standarder för uppkopplade enheter mellan olika företag skapar problem för användarna, då de tenderar att tillämpa olika förhållningssätt till dessa Andonova et al. (2015). Bergman & Lin (2016) menar att i flera fall så är det upp till hushållen att sköta säkerheten själva. Till viss del går detta att se, då nästan hälften av användarna uppger att de inte har någon större kontroll över vilken information som lagras och används. Dessutom har ett flertal respondenter direkt uppgivit att de inte känner att de har kontroll eftersom informationen antingen inte framgår av produkttillverkarna, eller att ”de ändå gör som de vill”. När användare känner att det är upp till de själva att sköta säkerheten, exempelvis vilken information som får lagras och användas, blir konsekvensen förmodligen att tilltron till tillverkarna minskar.

5.3 Autentisering

Från enkätundersökningen går det att utläsa att endast två av tio respondenter är oroliga över att någon obehörig kan skapa sig tillgång till deras enheter, vilket visar på en optimism bland användare gällande risken att bli utsatt för attacker. Resultatet stödjer Barbosa et al. (2019) som menar att det just finns en sådan tilltro bland användarna. Vidare har 76% av de som är oroliga över att någon obehörig kan skapa sig tillgång till deras enheter, vidtagit en eller flera åtgärder för att minimera denna risk. Resultatet visar även att ungefär 63% av de som är inte är så oroliga också har vidtagit en eller fler åtgärder. Att en stor del av de som inte är oroliga över att någon obehörig kan skapa sig tillgång har vidtagit åtgärder, vilket är

anmärkningsvärt. De som är oroliga har dock vidtagit åtgärder i en större utsträckning. Det resultatet kan visserligen vara logiskt, då de som är oroliga förmodligen vidtar åtgärder för att känna sig säkra.

Borghain et al. (2015) menar att det är vanligt att människor använder samma användarnamn och lösenord på flera ställen och att användarnamn och lösenord är en mindre säker metod för autentisering. I enkätundersökningen nämns ”extra starka lösenord” 20 gånger vilket visar en mindre del användare som är medvetna om riskerna med att använda ”svaga” och eventuellt samma lösenord fler gånger. Majoriteten nämner likväl inte detta, vilket även detta stödjer Borghain et al. (2015) påstående. Borghain et al. (2015) menar även att tvåfaktorsautentisering är ett sätt för användarna att öka säkerheten kring autentisering. Detta påvisas i resultatet då flertalet respondenter nämner att de använder sig av det.

Det går att utläsa ett nästan identiskt resultat gällande hur troligt respondenterna tror det är att någon antingen manipulerar, fabricerar felaktig information eller nekar respondenten åtkomst till sina enheter. Dock menar användarna att det troligaste är att någon skulle stjäla deras information, vilket Furszyfer och Sovacool (2020) menar är en av de allvarligaste riskerna. Vidare har respondenterna svarat liknande på frågan om hur oroliga de är att någon kan skaffa sig tillgång till deras enheter och hur troligt de tror det är att någon manipulerar eller fabricerar felaktig information, samt nekar dem åtkomst till sina enheter.

En möjlig anledning till detta är att frågorna är relativt lika, då alternativen som presenteras i fråga 11 bygger på att en obehörig har tillgång till en enhet/enheter. Även här finns en optimism bland respondenterna, då de inte anser det troligt att de skulle bli utsatta för något av dessa. En stor majoritet är därmed inte oroliga över att någon obehörig får tillgång till deras enheter, samt att det som anses som mest troligt är att någon skulle stjäla informationen,

4 av 10 är till viss del eller väldigt oroliga att produkttillverkare skapar sig tillgång till information från andra enheter, utan tillåtelse. De som är mest bekymrade för detta är dessutom de som är mest oroliga att obehöriga kan skapa sig tillgång till deras enheter: Ju mindre oroliga respondenterna är att någon får tillgång till deras enheter, desto mindre bekymrade är de att produkttillverkare skapar sig tillgång till deras information.

Respondenterna är även mer ängsliga att information stjäls än manipuleras, eller att det fabriceras felaktiga data. Nästan två tredjedelar av de som svarade att de är rädda över att någon annan får tillgång till deras enheter är dessutom oroliga över att produkttillverkarna skaffar sig tillgång till deras information. Fernandes et al. (2017) hävdar bland annat att en

stor del av applikationerna på plattformen ”SmartThings” tilldelas åtkomst och tillgång till funktioner och information de inte fått tillåtelse av användaren att använda. I linje med studien, eller som konsekvens av den, visar resultatet att användare är mer bekymrade att produkttillverkare skapar sig åtkomst till deras information, än att någon annan skulle göra det.

En möjlig anledning till att fler är rädda över att produkttillverkare skapar sig åtkomst till deras information, jämfört om någon annan obehörig, kan bero på att produkttillverkarna redan finns i hemmet. De har enheter som är uppkopplade mot andra enheter, vilket gör att de redan har tillgång till internet och viss information. Detta i kombination med optimismen som Barbosa et al. (2015) nämner kan förklara varför respondenterna är mer oroliga över att produkttillverkarna skapar sig åtkomst till deras information än någon annan utomstående.

5.4 Beteendeanpassning

Miller (2015) menar att bekvämlighet är en stor del av smarta hem och Chen et al. (2016) belyser det faktumet att för att kunna öka bekvämligheten behöver smarta hem använda data från andra enheter. Användarna behöver därmed vara villiga att ge ut mer information för att kunna nå maximal bekvämlighet, vilket nästan två tredjedelar av respondenterna är villiga att göra. Drygt hälften av respondenterna tycker det är tilltalande att enheter kan använda lagrad information om vanor och beteenden för ökad användarvänlighet, som sedermera skulle kunna kopplas till bekvämlighet. Det återfinns ett mönster mellan om respondenterna är villiga att ge ut mer personlig information och deras tillit till säkerheten hos enheterna. De som är villiga att ge ut mer information tenderar också att ha en högre tillit till enheterna, vilket skulle kunna bero på att de som har högre tillit dessutom anser det säkrare att ge ut information till enheterna, jämfört med de som har lägre tillit, och är därför mer villiga att lämna ut den. Det återfinns en tydlig koppling till Miller (2015) påstående om att det är en balansgång med hur mycket information som enheterna behöver, och hur mycket användarna är villiga att ge dem. Resultatet visar att flertalet är villiga att ge ut mer information till enheterna för att få ökad bekvämlighet. Dessutom anser en majoritet det vara okej för enheter att använda lagrad information om användarens vanor och beteenden för att även öka användarvänligheten.

Det går att uttyda att nästan 8 av 10 tycker scenariot som presenterades i fråga 18 låter mer behagligt än obehagligt. De respondenter som är mest positivt inställda till scenariot är även de som är mer villiga att ge enheterna tillgång till mer personlig information. Av de

respondenter som inte vill ge enheterna tillgång är drygt hälften positivt inställda. I scenariot så har hemmet och enheterna anpassat sig efter användaren och lärt sig dess vanor och beteenden för att öka bekvämligheten, vilket liknar fråga 15 om respondenten är villig att ge ut mer information i utbyte mot ökad bekvämlighet. Det kan vara så att scenariot låter lite mjukare och när det sätts i ett sammanhang. Det kan därmed vara enklare och tydligare vad det kan innebära, jämfört med en vanlig fråga och därför är de mer positiva till själva scenariot.

Endast 1 av 10 hade varit villig att dela med sig av sin information från sina enheter till exempelvis enhetens tillverkare eller samarbetspartners i marknadsföringssyfte för anpassade erbjudanden. Dock hade ytterligare två av tio av de som svarat att de inte ville dela med sig i marknadsföringssyfte varit villiga att ge ut mer information för samma ändamål om de även hade fått rabatter i utbyte. Detta stödjer till viss del Barbosa et al. (2019) som hävdar att personer inte är villiga att dela med sig av sin data, även om de fick rabatter i utbyte. Här kan valet av enheter eventuellt kunna ha betydelse. Vissa typer av enheter hanterar mer känslig information än andra, vilket leder till att användaren inte vill dela med sig av den informationen. Hade användaren istället haft enheter som inte har tillgång till lika känslig information så skulle användarna möjligtvis vara mer villig att dela med sig av den.

Av de som är villiga att ge ut information utan rabatter är det nästan 30% av dessa som också skulle vara villiga ge sina enheter tillgång till mer personlig information för att få ökad bekvämlighet. Endast 3% av de respondenter som har svarat att de är tveksamma till, alternativt sagt att de inte skulle ge ut information i marknadsföringssyfte, har även svarat att de skulle vara villiga att ge ut personlig information för ökad bekvämlighet. Även här går att se att de som är villiga att ge ut information i marknadsföringssyfte har en högre tillit till säkerheten hos enheterna än de som inte skulle göra det eller är tveksamma.

Miller (2015) menar att enheterna har lagrad data om vem du är, vad du gör, när du gör och hur du gör det och att det kan bli förödande konsekvenser för en individerna i ett hem om informationen hamnar i fel händer. Detta kan vara en möjlig anledning till att vissa av respondenterna inte vill ge tillgång till personlig information, medan de som är villiga att ge ut information kanske inte är så medvetna om konsekvenserna ifall någon annan kommer över informationen.

6 Slutsats och utvärdering

6.1 Slutsats

Slutsatsen har grundats på teorin som presenterats tidigare i studien, samt analysen och diskussionen som bygger på empirin som samlats in i enkätundersökningen. Utifrån de fyra teman som studien utgått ifrån har en slutsats kunnat dras för att ge svar på frågeställningen:

Hur ser användare av uppkopplade-enheter i smarta hem på säkerhet utifrån autentisering och beteendeanpassning?

Användare är medvetna om säkerhetsrisker kopplat till autentisering. Det finns inte någon större oro över att obehöriga på något sätt skulle skapa sig åtkomst till deras enheter, med manipulering av deras privata information som följd. Det finns tendenser av ett mönster, nämligen att den mindre del användare som är oroliga för dessa risker dessutom är de som är oroliga att andra aktörer (produkttillverkare) skapar sig åtkomst till deras enheter och dess lagrade informationen. Användarna som ger uttryck för oro kring säkerheten tenderar att göra detta i samtliga säkerhetsfrågor som berör autentisering. Det är trots detta en majoritet av användarna som inte är särskilt oroliga över säkerhetsriskerna kopplat till detta ämne.

Studien har visat att användare är mer bekymrade kring lagring av personlig information i syfte att öka bekvämlighet och användarvänlighet. En större del är positivt inställda till delning av privat information för att uppfylla dessa ändamål. Dock är de inte lika många som är gynnsamt inställda jämfört med lagring av autentiseringsdata. De som är mer villiga att dela med sig av sin information är även de som visar ansatser till att inneha en högre tilltro till sina enheter.

6.2 Värdering av studien

Mot bakgrunden att 9 av 10 respondenter var män menar författarna att det inte går att generalisera resultatet för alla användare, utan främst för manliga användare. Det var inget i resultatet som antydde att det fanns en skillnad, men för att kunna generalisera behövs en större representation av fler könsidentiteter än män. Ett annat urval där fördelningen mellan kön hade kunnat kontrolleras hade möjligtvis kunnat ge ett annat resultat samt gett större möjlighet till generalisering av alla användare. En stor majoritet av respondenterna nåddes genom en Facebookgrupp för smarta hem, vilket kan ha haft en påverkan på resultatet, då den gruppen möjligtvis domineras av människor som är intresserade och insatta i området, än den genomsnittliga smarta hem-användaren.

Valet av enkätundersökning samt det faktum att alla obligatoriska frågor hade fördefinierade svar har sannolikt gjort så att enkäten gick snabbt för respondenten att fylla i. Detta kan ha resulterat i att svaren inte var så genomtänkta som om de skulle kunnat vara om de istället skrev alla svar själva. På de frågor där författarna ansågs det relevant har öppna följdfrågor använts för att fånga upp svar och tankar som annars skulle missats. Trots detta har författarna säkerligen gått miste om svar och tankar på grund av att det inte fanns följdfrågor till alla frågor. Detta hade dock varit oerhört tidskrävande och minskat en av fördelarna med en kvantitativ metod, nämligen att den insamlade data är standardiserad och därmed kan analyseras på ett statistiskt sätt, vilket har gjorts.

Betydligt med resurser lades ner på att utforma enkäten. Både en pre-pilotstudie och en pilotstudie, så att frågorna var tydliga och inte riktade åt något håll samt var relevanta för den som deltog. Säkerligen hade vissa frågor och framförallt svarsalternativ på vissa frågor kunnat förtydligas och konkretiserats. Ett exempel är fråga 16, där respondenten frågades om hen var villig att dela med sig av information i marknadsföringssyfte för att kunna ge anpassade erbjudanden. Sedan frågades respondenterna som svarat "Nej" eller "Tveksamt" på denna om de skulle svarat "Ja" ifall de fick rabatter i utbyte för information. En respondent menade att "rabatter" var vagt och att det för hen skulle spela roll hur mycket rabatt hen i så fall skulle få i utbyte.

6.3 Förslag på framtida forskning

Det vore passande att genomföra en likadan undersökning om några år för att se om resultatet blir detsamma eller om användarnas syn har förändrats i takt med att utbudet av produkter och tjänster ökar, samt att konceptet smarta hem förmodligen blivit vanligare. En stor majoritet av denna studies respondenter har varit män och därmed hade det varit intressant att genomföra en likadan studie men med andra könsidentiteter för att undersöka och identifiera eventuella likheter och skillnader mellan hur olika kön ser på uppkopplade-enheters säkerhet utifrån autentisering och beteendeanpassning. En kvalitativ undersökning hade också kunnat genomföras för att få en djupare förståelse av användarnas syn och för att kunna fånga fler tankar och åsikter kring säkerhet, autentisering och beteendeanpassning.

7 Referenser

Alam, M. R., Ali, M. A. M. & Reaz, M. B. I. (2012). A Review of Smart Homes-Past, Present, and Future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 42(6), ss. 1190–1203.

DOI: <https://doi.org/10.1109/TSMCC.2012.2189204>

Andonova, Y., Hajjat, F., Milne, G. & Weinberg, B. (2015). Internet of Things: Convenience vs. Privacy and secrecy. *Business Horizons*, 58(6), ss. 615–624.

DOI: <https://doi.org/10.1016/j.bushor.2015.06.005>

Atzori, L., Iera, A. & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), ss. 2787–2805.

DOI: <https://doi.org/10.1016/j.comnet.2010.05.010>

Awad, A. & Bako, A. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors*, 18(3).

DOI: <https://doi.org/10.3390/s18030817>

Backman, J. (2016). *Rapporter och uppsatser*. 3. uppl., Lund: Studentlitteratur.

Balta-Ozkan, N., Bicket, M., Davidson, R. & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy*, (63), ss. 363–374.

DOI: <https://doi.org/10.1016/j.enpol.2013.08.043>

Barbosa, N., Park, J., Wang, Y. & Yao, Y. (2019). “What if?” Predicting Individual Users’ Smart Home Privacy Preferences and Their Changes. *Proceedings on Privacy Enhancing Technologies*, 2019(4), ss. 211–231.

DOI: <https://doi.org/10.2478/popets-2019-0066>

Bergmann, N. & Lin, H. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information*, 7(3), ss. 44.

DOI: <https://doi.org/10.3390/info7030044>

Borgohain, A., Borgohain, T., Kumar, U. & Sanyal, S. (2015). Authentication Systems in Internet of Things. *International Journal of Advanced Networking and Applications*, 6(4), ss. 2422–2426.

Brill, J. (2015). The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control. *Fordham Law Review*, 83(1), ss. 205–218.

Chen, S., Huang, X., Yi, J. & Zhu, X. (2016). A Semantic Approach with Decision Support for Safety Service in Smart Home Management. *Sensors (Basel, Switzerland)*, 16(8), ss. 1224.
DOI: <https://doi.org/10.3390/s16081224>

Cohen, L., Manion, L. & Morrison, K. (2007). *Research methods in education*. 6. uppl., London: Routledge.

Cook, D.J. & Rashidi, P. (2009). Keeping the Resident in the Loop: Adapting the Smart Home to the User. *IEEE Transactions on Systems, Man, and Cybernetics. Part A: Systems and Humans*, 39(5), ss. 949–959.
DOI: <https://doi.org/10.1109/TSMCA.2009.2025137>

Davidson, B. & Patel, R. (2019). *Forskningsmetodikens Grunder: att Planera, Genomföra och Rapportera en Undersökning*. 5, uppl. Lund: Studentlitteratur.

Fernandes, E., Jung, J., Prakash, A. & Rahmati, A. (2017). Security Implications of Permission Models in Smart-Home Application Frameworks. *IEEE Security & Privacy*, 15(2), ss. 24–30.
DOI: <https://doi.org/10.1109/MSP.2017.43>

Furszyfer, D, R. & Sovacool, B, K. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and Sustainable Energy Reviews*, (120).
DOI: <https://doi.org/10.1016/j.rser.2019.109663>

Haglund, F. (2015). *Svenskar först att flytta hemifrån*.
<https://www.europaportalen.se/2015/04/svenskar-forst-att-flytta-hemifran>. [2020-05-11].

Hargreaves, T., Hauxwell-Baldwin, R. & Wilson, C. (2015). Smart homes and their users: a systematic analysis and key challenges. *Personal and Ubiquitous Computing*, 19(2), ss. 463–476.

DOI: <https://doi.org/10.1007/s00779-014-0813-0>

Internetstiftelsen (2019). *Svenskarna och internet 2019*. Tillgänglig:

<https://svenskarnaochinternet.se/app/uploads/2019/10/svenskarna-och-internet-2019-a4.pdf>

Jacobsen, D. I. (2017) *Hur genomför man undersökningar? Introduktion till samhällsvetenskapliga metoder*. 2. uppl., Lund: Studentlitteratur AB.

Jacobson, A. (2019). Smart Home Devices and Privacy Risk. *Risk Management*, 66(9), ss. 4–7.

Kalra, S. & Sood, S, K. (2015). Secure authentication scheme for IoT and cloud servers. *Pervasive and Mobile Computing*, (24), ss. 2010–223.

DOI: <https://doi.org/10.1016/j.pmcj.2015.08.001>

Kim, M, H. & Wong, K-S. (2014). Preserving Differential Privacy for Similarity Measurement in Smart Environments. *The Scientific World Journal*, 1(9).

DOI: <https://doi.org/10.1155/2014/581426>

Kim, T-H. & Robles, R-J. (2010). Applications, Systems and Methods in Smart Home Technology: A Review. *International Journal of Advanced Science and Technology*, (15).

Liang, T., Liu, J., Ye, L., Zeng, B. & Zou, C. (2018). An Unsupervised User Behavior Prediction Algorithm Based on Machine Learning and Neural Network For Smart Home. *IEEE Access*, (6), ss. 49237–49247.

DOI: <https://doi.org/10.1109/ACCESS.2018.2868984>

Liu, J., Gong, W., Shea, R. & Sun, A. (2018). A Castle of Glass: Leaky IoT Appliances in Modern Smart Homes. *IEEE Wireless Communications*, 25(6), ss. 32–37.

DOI: <https://doi.org/10.1109/MWC.2017.1800120>

Maras, M-H. (2015). Internet of Things: security and privacy implications. *International Data Privacy Law*, 5(2), ss. 99–104.

DOI: <https://doi.org/10.1093/idpl/ipv004>

Marketing-Schools.org (u.å). *One-to-One Marketing*. <https://www.marketing-schools.org/types-of-marketing/one-to-one-marketing.html> [2020-04-21].

Mashal, I. & Shuhaiber, A. (2019). Understanding users' acceptance of smart homes. *Technology in Society*, (58).

DOI: <https://doi.org/10.1016/j.techsoc.2019.01.003>

McCartan, K. & Robson, C. (2016). *Real world research: a resource for users of social research methods in applied settings*. 4. uppl., Hoboken: Wiley.

Mendez, D., Papapanagiotou, L. & Yang, B. (2017) Internet of Things: Survey on Security and Privacy. *arXiv.org*, 27(3), ss. 162–182.

DOI: <https://doi.org/10.1080/19393555.2018.1458258>

Miller, M. (2015). *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World*. Indianapolis: Que

Moberg, K. (2015). *Är artikeln peer reviewed?*. <https://kib.ki.se/whatsup/blog/ar-artikeln-peer-reviewed> [2020-05-04].

Nationalencyklopedin (u.å). Smart hem. Tillgänglig: Nationalencyklopedin. [2020-04-25].

Nilsson, T. (2018). *Vi förklarar IOT, sakernas internet*. <https://www.mobil.se/nyheter/vi-forklarar-iot-sakernas-internet> [2020-05-09]

Pau, G., Salerno, V-M., Sharma, V. & You, I. (2019). Special Issue 'Internet of Things for Smart Homes'. *Sensors*, 19(19).

Rambus (u.å). *Smart Home: Threats and Countermeasures*.

<https://www.rambus.com/iot/smart-home/> [2020-04-26].

Recker, J. (2013). *Scientific Research in Information Systems A Beginner's Guide*. Springer – Verlag Berlin and Heidelberg GmbH Co. K.

Vinel, A., Wang, L., Xia, F. & Yang, L. (2012) Internet of Things. *International Journal of Communication Systems*, 25(9), ss. 1101–1102.

Bilaga. Enkätundersökning

2020-06-04

Smarta hem - Autentisering och beteendeanpassning

Smarta hem - Autentisering och beteendeanpassning

Den här enkäten handlar om de uppkopplade prylar vi har i våra hem, och hur vi som användare förhåller oss till säkerheten och integriteten kring all den information som lagras, genereras och används av dessa prylar.

Har du en eller fler uppkopplade enheter (såsom vitvaror, röstassistenter, brandlarm, lås, termostater och lampor) UTÖVER en dator, mobil och surfplatta, så hade vi uppskattat om du tog dig tiden att besvara denna enkät, bestående av 18 korta frågor.
Har du inte det så vill vi ändå tacka för visat intresse!

Enkäten är anonym och resultatet kommer ligga till grund för en analys som kommer presenteras i vår kandidatuppsats.

Med vänliga hälsningar,
André Hamberg och Fredrik Lundgren - två studenter på Högskolan i Borås.

* Required

1. 1. Hur gammal är du? *

Mark only one oval.

- 18-24 år
- 25-29 år
- 30-34 år
- 35-39 år
- 40-44 år
- 45-49 år
- 50-54 år
- 55-59 år
- 60-64 år
- 65-69 år
- 70 år eller äldre

2. 2. Vad har du för könsidentitet? *

Mark only one oval.

- Man
- Kvinna
- Annat
- Vill ej uppge

3. 3. Inom vilka smart hem-kategorier har du enheter? Kryssa för alla du använder. *

Check all that apply.

- Övervakning (Exempelvis övervakningssystem)
- Vitvaror (Exempelvis kylskåp, brödrost och ugn)
- Röstassistenter (Exempelvis Google Home, Alexa och Siri)
- Säkerhet (Exempelvis brandlarm, lås och dörrklockor)
- Energianvändning (Exempelvis uttag och strömbrytare)
- Enheter som förbättrar inomhusklimat (Exempelvis termostater eller sensorer som känner av luftkvaliteten)
- Belysning (Exempelvis lampor och LED-strips)

4. Använder du något annat än alternativen ovan? Beskriv gärna kortfattat.

5. 4. Vilken är huvudanledningen till att du införskaffade din smarta enhet/enheter? *

Mark only one oval.

- Bekvämlighet (Slippa göra vissa saker hemma, exempelvis dammsuga)
- Säkerhetsskäl
- Ökad livskvalitet (Bättre inomhusklimat)
- Minska påverkan på miljön
- Nyfikenhet
- Hobby

6. 5. På en skala 1-6, hur stor tillit har du till säkerheten hos din enhet/enheter? 1 = Inte alls, 6 = Mycket stor. *

Mark only one oval.

	1	2	3	4	5	6	
Inte alls	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Mycket stor

7. 6. Är du medveten om att smarta-enheter ofta samlar in och lagrar personlig information om dig? (Förutom inloggningsuppgifter eller andra nödvändiga uppgifter för att enheterna skall fungera) *

Mark only one oval.

- Ja
 Nej

8. 7. Har du kollat upp vilken information som din enhet/enheter lagrar? *

Mark only one oval.

- Ja, noggrant
 Ja, men inte så noggrant
 Jag försökte, men förstod inte
 Jag försökte, men hittade ingen information
 Nej, det gjorde jag inte
 Minns ej

9. 8. Känner du att du har kontroll (det vill säga möjlighet att kunna påverka) över vilken information som lagras och används av din enhet/enheter? *

Mark only one oval.

- Ja, full kontroll
- Ja, men inte fullt ut
- Nej, inte så mycket
- Nej, det har jag inte

10. Om inte, varför då?

11. 9. Har du någon gång undvikit att införskaffa en enhet på grund av informationen den vill lagra och använda? *

Mark only one oval.

- Ja
- Nej

12. 10. På en skala 1-6, hur orolig är du att obehöriga kan, via till exempel hackning, skapa sig tillgång till din enhet/enheter? 1 = Inte orolig, 6 = Mycket orolig *

Mark only one oval.

	1	2	3	4	5	6	
Inte orolig	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Mycket orolig

13. 11. Här följer ett par alternativ. Vi vill att du tar ställning till varje alternativ utifrån hur troligt det är att dessa skulle kunna hända dig och din enhet/enheter. 1 = Inte troligt, 6 = Högst troligt *

Mark only one oval per row.

	1	2	3	4	5	6
Obehörig manipulerar din lagrade information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Obehörig fabricerar felaktig information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Obehörig stjälar din lagrade information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Obehörig nekar dig åtkomst till din enhet/enheter efter hackning	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

14. 12. Har du vidtagit egna åtgärder för att försäkra dig om att det bara är du som har tillgång till dina enheter? *

Mark only one oval.

- Ja, några stycken
 Ja, någon enstaka
 Nej

15. Om du svarat ja på frågan ovanför, ge gärna exempel på hur.

16. 13. Är du orolig att produkttillverkare av smarta hem-enheter skapar sig åtkomst till din information från andra enheter i ditt hem, utan din tillåtelse? *

Mark only one oval.

- Ja, väldigt
- Ja, till viss del
- Inte särskilt
- Inte alls

17. 14. På en skala 1-6, vad tycker du om att enheter skulle kunna använda lagrad information om dina vanor och beteenden för att försöka öka användarvänligheten? 1 = Mycket obehagligt, 6 = Mycket tilltalande. *

Mark only one oval.

	1	2	3	4	5	6	
Mycket obehagligt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Mycket tilltalande

18. 15. Skulle du vara villig att ge tillgång till mer personlig information till din enhet/enheter om det hade lett till ökad bekvämlighet (slippa göra vissa saker hemma, exempelvis dammsuga)? *

Mark only one oval.

- Ja, absolut
- Ja, lite mer än nu
- Nej, det hade jag inte

19. 16. Skulle du vara villig att dela med dig av din information från enheterna, till exempelvis enhetens tillverkare eller dess samarbetspartners i marknadsföringssyfte? Detta för att ge dig anpassade erbjudanden utifrån dina preferenser och vanor. *

Mark only one oval.

- Ja, det skulle jag
- Tveksamt
- Nej, det skulle jag inte

20. 17. Om du svarat "Tveksamt" eller "Nej" på förgående fråga, skulle du svara "Ja" om du fick rabatter i utbyte mot informationen?

Mark only one oval.

- Ja
- Nej

21. 18. Du kommer nu ställas inför ett scenario. Vi vill att du på en skala 1-6 ger din syn på detta: Du kommer hem från jobbet och din bil skickar en signal till garageporten så den öppnas. När garageporten öppnas så tänds belysningen i ditt hem automatiskt. När belysningen tänts och garageporten öppnats så startas kaffemaskinen, då den lärt sig att du brukar dricka kaffe efter jobbet. *

Mark only one oval.

	1	2	3	4	5	6	
Känns obehagligt!	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Låter fantastiskt!

Tack så mycket för din medverkan!

Med vänliga hälsningar, André och Fredrik

This content is neither created nor endorsed by Google.



HÖGSKOLAN I BORÅS

Besöksadress: Allégatan 1 · Postadress: 501 90 Borås · Tfn: 033-435 40 00 · E-post: registrator@hb.se · Webb: www.hb.se