Examensarbete

HÖGSKOLAN I SKÖVDE

Integritet vid passiv biometrisk autentisering: en demografisk analys av användarupplevelse

Privacy in passive biometric authentication: A demographic analysis of user experiences

Examensarbete inom huvudområdet informationsteknologi med inriktning mot informationssystem.

Grundnivå 30 Högskolepoäng

Vårtermin 2024

Andréas Gebrail

Handledare: Manfred Jeusfeld
Examinator: Joeri van Laere

Sammanfattning

Denna studie fokuserar på användarupplevelser samt integritet och dess beredskap att kompromissa med denna när det kommer till passiv biometri som autentiseringsmetod hos olika demografiska grupper, vilket i detta fall har fokuserat på kön och högsta avslutad utbildning för individer över 18 år. Denna autentiseringsmetod är allt mer vanlig idag och den växer samt implementeras i fler enheter kontinuerligt idag. Informationen som lagras i dessa enheter kan vara värdefull för båda användare men även andra aktörer som har negativa handlingar i åtanke.

För att kunna få den relevanta data som behövs har både den kvalitativa och kvantitativa metodansatsen brukats med strukturerade intervjuer med likertskalor samt öppna frågor för att få ett mer djup i vissa svar. Slumpmässiga deltagare har intervjuats och en litteraturstudie gjorts.

Det som är återkommande teman i studien är att flera har förtroende för autentiseringsmetoden men att det ändå finns en oro hos vissa demografiska attribut. Olika upplevelser som att det går snabbt och effektivt utan problem är en bidragande faktor till en positiv sådan men då informationen som lagras i enheten kan vara känslig finns en oro att denna ska komma i obehörigas händer.

Denna studie är heller inte representativ för en hel befolkning eller olika demografiska grupper utan detta är mer lik en förstudie för att testa de olika metoderna om dessa är genomförbara över ett större urval av respondenter.

Nyckelord: Passiv biometri, autentiseringsmetod, integritet, användarupplevelse, användaracceptans.

Innehållsförteckning

1 Inledning

Passiv biometri är när en särskild aktiv handling inte behövs för att autentisera sig när exempelvis autentiseringsmetoden 'ansiktsigenkänning' används; autentiseringen sker när systemet automatiskt känner igen användarens ansikte. Det betraktas som passiv biometrisk autentisering eftersom den sker som en del av den naturliga interaktionen mellan användaren och enheten utan behov av specifika användarinitierade handlingar för autentisering.

Passiv biometri som autentiseringsmetod är idag en teknologi som visar de framsteg som skett inom autentisering och verifikation inom både. Vad som kännetecknar passiv biometrisk autentisering är att användaren aktivt inte behöver utföra någon handling för att identifieras utan att system gör detta passivt utan att användaren behöver göra något (Xu, Zhou and Lyu, 2014). Genom att exempelvis identifiera ansiktet utan att användaren behöver klicka eller utföra en handling med sitt ansikte (Zhang and Gao, 2009; Dargan and Kumar, 2020). Detta har blivit standarden både för säkerhet men även användarvänligheten och upplevelsen. Genom att använda människans fysiologiska och/eller beteendemässiga egenskaper som exempelvis röstidentifiering och ansiktsigenkänning. Denna metod eliminerar behovet av traditionella lösenord och pinkoder som minskar risk för säkerhetsincidenter samt bortglömda lösenord (Chopra, 2019; Meng et al., 2015).

Aktiv biometrisk autentisering är en annan form av autentisering som kräver användarens aktiva deltagande eller en aktiv handling från användaren för att få åtkomst till systemet. Detta kan vara att exempelvis placera fingret på en platta som läser av fingeravtrycket. Detta likt passiv biometri eliminerar problemen som traditionella autentiserings metoder har (Dargan and Kumar, 2020; Li et al., 2013; Meng et al., 2015).

Förståelse för hur diverse demografiska faktorer påverkar användarens attityd och acceptant för passiv biometrisk autentisering är viktigt för utöver utforma och utveckla teknologin där hänsyn till användarpreferenser, men även för att hantera integritetsbekymmer på ett mer effektivt sätt. Inom ramen för passiv biometri blir demografin en nyckelaspekt för denna studie genom att förstå användaracceptans och för att i framtiden kunna forma policys som respekterar individens integritet.

De två forskningsfrågor som ska besvaras är:

1. *I vilken utsträckning påverkar olika demografiska attribut, såsom kön och utbildningsbakgrund, individernas attityd gentemot användningen av passiv biometrisk autentisering?*
2. *Hur varierar demografiska grupper i sin beredvillighet att kompromissa med integritetsaspekter för att uppnå en förbättrad användarupplevelse och användarvänlighet i samband med passiv biometrisk autentisering?*

Genom att undersöka demografiska faktorer möjliggör det att förstå att om det finns specifika grupper som känner större oro för integritetsfrågor kopplade till just passiv

biometrisk autentisering. Detta perspektiv kan bidra till att exempelvis kunna skapa riktade informationskampanjer och eventuella utbildningsinitiativ för att bemöta och adressera denna oro samt bygga förtroende för tekniken inom dessa demografiska grupper.

Det förväntade resultatet är att olika grupper kommer att ha olika upplevelser och attityder kring passiv biometri som autentiseringsmetod men att vissa unika händelser kan påverka individens synsätt på teknologin, oavsett om denna är positiv eller negativt lagt.

Denna förståelse för demografi och integritet är avgörande för att skapa en balans mellan teknologisk innovation och individuell integritet, vilket i slutändan kan leda till ökad acceptans och framgångsrik implementering av passiv biometrisk autentisering i diverse sammanhang.

2 Bakgrundskapitel

I detta kapitel ska bakgrund till användningen av biometrisk autentisering ske genom att presentera vetenskaplig forskning kring detta ämne. Vidare ska detta ge läsaren en grundlig förståelse över ämnet.

2.1 Användande utav Biometrisk autentisering

Idag är biometrisk autentisering både väl studerat och utvecklat (Riley et al., 2009; Abed et al., 2012; Ratjeana Malatji, van Eck and Zuva, 2020). Detta har varit till stor hjälp för att undvika hantering av massvis av lösenord och även användbarheten för diverse system. För mobila enheter såsom telefoner och surfplattor är detta en utav de vanligaste autentiseringsmetoder idag och underlättar autentiseringen (Rui and Yan, 2019).

Med införandet utav ansiktsigenkänning där fingeravtryck börjar frångås när det kommer till biometrisk autentisering idag så finns många olika system för detta beroende på operativsystem som används men funktionaliteten är mer eller mindre densamma. Idag används Commercial Off-The-Shelf (COTS) ansiktsigenkänning som inte alltid är väldesignade att hantera spoofade ansikten vilket leder till osäkerhet av autentiseringen (Di Wen, Hu Han and Jain, 2015). Rui and Yan (2019) påvisar att det finns olika attack punkter som är sårbara mot attacker. Exempelvis hänvisar de till attackpunkt 1 där man utbyter originalbiometriska datan som finger, foto eller röst mot en egengjord sådan. Detta leder till förfalskade biometriska drag används och godkänns av systemunder falska omständigheter. Detta skulle kunna uppfattas som integritetskränkande av användare som brukar denna typ autentiseringsmetod samt ett brott vid identitetsstöld. Sedan kan även systemet godkänna felaktig biometri genom att den avläser datan inkorrekt, dessa är kända som *false positive* vilket innebär att systemet verifierar och godkänner fel biometri och ger åtkomst till person som ej bör ha åtkomst (Wang et al., 2017). Motsatsen till false positive är false negative och innebörden med denna är att verifikation systemet inte känner igen korrekt person och nekar åtkomst till en person som faktiskt ska identifieras korrekt.

Idag säljs även olika biometriska autentisering system från diverse företag runt om i världen (Nandhini Anbalagan et al., 2020). Vad dessa företag gör med informationen är svårt att ta reda på då de är baserade i länder där lagarna är otydliga eller att företaget måste dela med sig av sin information till staten. Får då ett främmande stat ta del av en annans stats biometriska data (Inkster, 2016). Räknas detta som integritetskränkande av användaren eller finns det en gråzon för staten att begära denna information för säkerhetenskull eller bör ingen aktör ha denna makt.

2.2 Integritet

Alla förtjänar att ha sin integritet respekterad och intakt vid bruk av olika mjukvaror och hårdvaror. Detta är idag en diskussion som blir allt mer omtalad eftersom ju mer system

som finns ju fler attacker kommer då försöka penetrera dessa system och få åtkomst till datan (Rui och Yan, 2019).
För att integriteten ska kunna kränkas måste först en relation etableras genom ett godkännande av användare och därefter kan information samlas in utav mjuk/hårdvara som sedan kan läckas eller användas av företag på oetiskt sätt (Mamonov and Benbunan-Fich, 2015). Detta menar Mamonov och Benbunan-Fich (2015) är vanligt idag och på detta vis påverkas användarna utav företagets säkerhet och policys. Policys och hur företagen ska arbeta för att motverka och minska intrång, läckor och oetiskt användande av individens data kan förstärka förtroende bland användaren till företaget som hanterar denna information.
Biometri fungerar som autentiseringsmetod om den sociala acceptansen finns och ifall denna skulle upphöra genom att förtroendet minskas eller försvinner helt så kommer det ej att fungera för att meningen är att det ska kunna skydda tillgången till en enhet eller ett system. Det samlar kontinuerligt in biometriska data och kan därav lära sig av användarens psykologiska och fysiska beteendemönster (Zhaleh Semnani-Azad et al., 2019). Det blir övertid väldigt mycket data om användaren. Detta kan användas negativt av aktörer som söker att göra skada mot användare.
Zhaleh Semnani-Azad et al (2019) beskriver även att det finns olika dimensioner till förtroende till biometrisk autentisering. Individer i studien är mindre kritiska till autentisering för åtkomst till enheten som exempelvis sin smarttelefon men är mer skeptiska att utföra och godkänna bankärenden som transaktioner via biometrisk autentisering. Detta påvisar att ett förtroende finns men är begränsad. Att användaren är villig att dela med sig sin biometri för att låsa upp sin enhet men ej när det kommer till vissa andra mjukvaror. Anser användaren att integriteten och säkerheten sämre vid bankärenden eller riskerar man hellre innehållet på sin telefon än bank.

2.3 Passiv biometri som övervakningsmetod

Hur framtiden ser ut är oviss, men hur passiv biometri kan användas i framtiden för att inskränka på individens integritet och privatliv går att jämföras med exempelvis Kina. Där har ett avancerat teknologiskt övervakningssystem implementerats där invånare bedöms i hur de agerar i det offentliga. Detta sker genom massvis med kameror som via passiv biometri analyserar individer och hur det följer lagar (Smith and Miller, 2021; Vinogradov, 2023; Liang et al., 2018). Via deras *Social Credit System* rankar systemet individer och ger fördelar till människan som gör rätt för sig men straffar den som icke gör det. Som användare kan du inte välja att ej delta utan alla som bor och befinner sig i området är delaktiga och dess data lagras för staten och de ansvarige över systemet att hantera. Dessa algoritmer som brukas kan dra skam över individer vars brott varit att gå över gatan när lyset är rött.

Utöver dessa frågor, bör även frågan om etiska problem nämnas. Anledning till denna implementation är för att stabilisera och trygga allmänheten men är ett väldigt enkelt

uttryck medan uppfattningen är att sittande makt har full kontroll över sina medborgare (Clancy, 2021).
Idag har även många länder kameror uppsatta för övervakning. Även om dessa inte identifierar medborgare via passiv biometri betyder det inte att de en dag kan utbytas och ersättas med kameror som kan detta. Kommer detta kunna berättigas genom trygghet undrar Watt (2017). Hur kommer det sedan kunna bli ifall telefoner och andra enheter som spelar in ljud och bild med passiv biometris autentiserings teknologi fungera om privata aktörer och staten får oändlig med tillgång till den data som samlas in.

2.4 Säkerhet av biometrisk data

Den finns olika aspekter som bör beaktas när det kommer till biometrisk autentisering idag. Den biometriska egenskapen som användaren har är unik till varje människa, även om den är lik så är varje person unik in sin fysiologiska eller beteendemässiga egenskap. Att varje individ är unik är kritisk och möjliggör för en säker och pålitlig identifiering, i de fall systemet är väl utvecklat. Detta minimerar risken för felaktigt autentisering som kan leda till obehörig åtkomst samt förhindrar identitetsstölder (Anil et al., 2008). Problemet som kan förekomma är att tillskillnad från traditionella lösenord och pinkoder kan denna data vara svårt att återkalla eller ändras ifall den biometriska datan hamnar i fel händer och komprometteras är det svårt att återställa säkerheten. Ett sätt att detta sker på är falsifiering, detta innebär att med den avancerade teknik som finns idag och hur teknologiska avancemang sker konstant så är det möjligt att skapa förfalskningar genom ansiktsmasker för ansiktsigenkänning och konstgjorde fingeravtryck (Akhtar, Michelon and Gian Luca Foresti, 2014). Samtidigt börjar även AI inkluderas i denna diskussion där spoofing sker mer frekvent och hur denna teknik kommer att påverka både passiv biometri som autentiseringsmetod (Hu et al., 2023).

Spoofing inom biometrisk autentisering refererar till försöket att lura eller lura systemet genom att använda fejkad biometriska data för att få obehörig åtkomst. Det är en typ av bedrägeri där en angripare försöker imitera eller återskapa de biometriska egenskaperna hos en legitim användare för att övervinna autentiseringssystemet (Di Wen, Hu Han and Jain, 2015).

Förlusten av biometriska data kan medföra allvarliga risker och potentiella konsekvenser för en individ. Genom detta kan identitetsstölder ske genom med hjälp av biometriska datan verifiera eller autentisera sig som en annan person, spoofing och andra typer av bedrägeri ske. Ett annat stort problem är att denna data är oåterkallelig, det betyder att en individ inte kan byta ut sin biometri, vilken är en nackdel kontra hur lösenord är lätta att byta ut. Detta kan medföra stora integritetsproblem ifall dessa hamnar i fel händer. Detta kan alltså missbrukas för kriminellt bruk och kan påverka både på individnivå men även organisationer (Patel, Ratha and Chellappa, 2015; Savvides, Kumar and Khosla, 2004; Shukla and Kaur, 2023).

2.5 Deep Fake

Deep Fake är en teknik där avancerade maskininlärningsalgoritmer används för att skapa realistiska och manipulerade multimediafiler, såsom videor, där personers ansikten eller röster byts ut (Yang, Li and Lyu, 2019). Denna teknik kan ha en betydande påverkan på passiva biometri som autentiseringsmetod, speciellt där röst ansiktsigenkänning används men även röststyrning. Vad denna teknik bidrar till är skapande av realistiska ansiktskopior som utgör en risk för bedrägeri inom system som förlitar sig på denna typ av autentisering som Deep Fakes kan utnyttja. Potentiellt kan aktörer och angripare använda dessa för att lura autentiseringssystem.

Detta bör ge incitament för företag som utvecklar biometrisk autentiseringssystem att även utveckla mer avancerade detektionsmetoder som kan bemöta det växande problemet kring Deep Fakes. För att ifall det system inte är tillräcklig robust kan angripare få obehörig åtkomst med hjälp av denna teknik (Lyu, 2020). Detta i form utav mer avancerade detektionsmetoder som skiljer mellan äkta och förfalskad biometrisk data. Förhöjd pricksäkerhet kan krävas för att även minska falska positiva samt falska negativa (Lyu, 2020).

Utöver den samhälleliga och etiska aspekten utav brukande av Deep Fakes där vanliga individer kan påverkas utöver autentiseringsprocessen så utgör denna teknologi ett hot mot cybersäkerhet i det stora för användare kan utge sig för att vara någon annan och göra väldig skada mot en individ eller en grupp beroende på position denna person har och hur det kan påverka mer än individen som Deep Faken utger sig för (Westerlund, 2019). Detta är höst integritetskränkande för individer som ej givit tillstånd att någon skapar Deep Fakes på den person.

Det som denna teknologi brukar sig av är redan existerande bilder, ljud och andra multimediafiler. I dagens samhälle är sociala medier ett utbrett fenomen som brukas av väldigt många runt om i världen. Individer lägger frivilligt upp dessa multimediafiler som Deep Fake teknologin frodar i och ger väldigt mycket data som den kan använda för att skapa så precis förfalskning som möjligt. Personer som är ännu mer offentliga och har mycket livestreamad data i form utav filmer/livestreaming eller personer med makt som ministrar och dylikt. Där ansiktsrörelser och beteende uppvisas i många olika former. Detta påverkar de ännu mer då större mängd data finns tillgänglig i flera format. Vad för konsekvens skulle ske ifall angripare ger sig på en statsminister som har en maktposition som kan påverka samhället.

Replay-attacker är en teknik som används där en angripare exempelvis kan använda en tidigare inspelning för att konstruera om den biometriska datan för att få obehörig åtkomst. Detta är sårbart för system som inte har tekniken som kan detektera upprepade inspelningar (Mo and Sinopoli, 2009).

Attacker med hjälp av denna metod sker kontinuerligt och teknologin för att motarbeta detta fenomen är under ständigutveckling den med. Ifall någon riktigt har lyckats kringgå autentisering system med hjälp av deepfakes är inte säkert men forskningen kring hur att kunna upptäcka den förfalskade datan är enorm och påvisar att forskare ser detta som ett framtida problem om det inte hanteras omgående (Cozzolino et al., 2021).

2.6 Demografiska syner och acceptans på teknologi

Teknikacceptans och dess könsskillnader är av stor betydelse för att förstå hur olika grupper av människor reagerar på och använder sig av teknologi i olika sammanhang. Genom att analysera dessa skillnader kan man få en djupare insikt i vilka faktorer som påverkar attityder och beteenden gentemot teknik. Forskningen visar på tydliga könsskillnader när det gäller uppfattningar om teknikens användbarhet och sociala påverkan, där kvinnor ofta värderar användbarheten högre medan män är mer mottagliga för sociala influenser (Kim, 2016). För att få en mer omfattande förståelse av teknikacceptans är det viktigt att inkludera flera demografiska aspekter såsom ålder, social bakgrund och professionell bakgrund. Ålder spelar en betydande roll i hur teknik uppfattas och används. Yngre generationer, som ofta växer upp med modern teknologi, har en tendens att vara mer tekniskt kunniga och öppna för nya teknologiska innovationer. Äldre individer kan däremot uppleva större hinder i teknikanvändningen på grund av lägre teknisk tillit eller brist på erfarenhet.

Social bakgrund och socioekonomisk status påverkar också teknikacceptans. Personer från högre socioekonomiska bakgrunder har ofta bättre tillgång till teknologi och utbildning, vilket kan leda till en mer positiv inställning till tekniska innovationer. Däremot kan individer från lägre socioekonomiska bakgrunder uppleva hinder i form av kostnader och tillgänglighet, vilket kan påverka deras vilja att använda ny teknik(Venkatesh, Thong och Xu, 2012). Professionell bakgrund spelar en kritisk roll i teknikacceptans. Yrken som kräver högteknisk kompetens, såsom IT eller ingenjörsyrken, tenderar att ha en arbetskraft som är mer positivt inställd till ny teknologi. Å andra sidan kan yrken som inte primärt involverar teknisk användning uppleva mer motstånd mot tekniska förändringar på grund av brist på direkt relevans eller nödvändighet i deras dagliga arbete.

Att ta hänsyn till dessa köns- och demografispecifika preferenser är avgörande för att skapa teknik som tilltalar och används av en bredare användarbas. Genom att anpassa designen och marknadsföringen av tekniska produkter och tjänster efter dessa skillnader kan man öka deras acceptans och användning över hela spektrumet av användare. En annorlunda strategi kan innebära att fokusera på olika aspekter av tekniken beroende på kön och utbildningsbakgrund såsom dess praktiska nytta för kvinnor och dess sociala fördelar för män. Genom att integrera denna kunskap i utvecklings- och marknadsföringsprocessen kan teknikföretag skapa produkter och tjänster som tilltalar en bredare och mer diversifierad publik, vilket i sin tur kan öka kundnöjdhet och lojalitet på lång sikt (Kim, 2016).

Könsskillnader påverkar acceptansen och synen på teknologi. Den visar att könsskillnader kan vara avgörande faktorer när det gäller vilka aspekter av teknik som prioriteras och hur de påverkar beteendet. Till exempel tenderar kvinnor att lägga större vikt vid faktorer som prisvärde och användbarhet, medan män kan vara mer benägna att motiveras av andra fördelar som underhållning eller status (Venkatesh, Thong och Xu, 2012).

Dessa könsskillnader kan delvis härledas till traditionella könsroller och sociala förväntningar. Även om dessa mönster förändras över tid, kan de fortfarande påverka hur olika kön ser på och använder teknologi. Till exempel kan sociala normer kring teknikanvändning vara starkare för män, vilket kan leda till en ökad benägenhet att experimentera med nya teknologier eller att visa upp tekniska färdigheter. För kvinnor kan teknikanvändning vara mer kopplad till praktisk nytta och socialt sammanhang, vilket kan påverka deras preferenser och beteenden när det gäller teknik (Venkatesh, Thong och Xu, 2012).

För att maximera teknikacceptans och användning är det viktigt att ta hänsyn till dessa könsskillnader och skapa teknikprodukter och marknadsföringsstrategier som är känsliga för olika köns preferenser och behov. Detta kan inkludera att erbjuda olika prispaket eller att utforma användargränssnitt och funktioner som tilltalar olika könsgrupper. Genom att förstå och anpassa sig till dessa könsskillnader kan teknikföretag skapa mer inklusiva och användarcentrerade produkter och tjänster (Venkatesh, Thong och Xu, 2012).

I studien (Gefen och Straub, 1997) undersöktes hur könsskillnader och andra faktorer påverkar acceptans och synen på teknologi, särskilt med fokus på könsroller och eventuella utbildningsbakgrunder. Resultaten indikerar att kvinnor tenderar att värdera e-post som ett medium med högre social närvaro och användbarhet jämfört med män. Detta kan delvis härledas till traditionella könssocialiseringar, där kvinnor oftare värderas för sin förmåga att bygga relationer och samarbeta. Å andra sidan visade resultaten att män kanske inte har lika höga förväntningar på den sociala närvaron i epostkommunikationen. Att kvinnor litar mer på teknologin som används och dess system är något som kan tas i beaktning för att kunna nå ut till sitt sociala nät.

När det gäller teknikacceptans och användning kan könsskillnader spegla både sociala normer och individuella erfarenheter. Kvinnor kan till exempel möta olika förväntningar och hinder baserat på sina utbildningsbakgrunder, där de kanske har mindre exponering för teknologi i vissa yrkesområden eller akademiska discipliner. Detta kan bidra till en mer avvaktande attityd gentemot teknik och därigenom påverka deras upplevelse av i detta fall e-post och användarvänlighet. För att främja en jämnare teknikacceptans och användning är det viktigt att inte bara adressera könsskillnader utan också ta hänsyn till socioekonomiska och utbildningsrelaterade faktorer som kan forma individers uppfattningar och beteenden kring teknologi (Gefen och Straub, 1997).

Kulturella värderingar formar individuellt beteende i teknologianslutning. Den finner att könsmässig maskulinitet/femininitet spelar en avgörande roll i hur subjektiva normer relaterar till beteendet när det gäller teknologianvändning. I kulturer där feminina värderingar är starka visar sig detta samband vara mer framträdande, medan det omvända gäller för kulturer präglade av maskulinitet. Detta pekar på en annorlunda syn på teknologi beroende på kulturella könsmönster och visar på vikten av att ta hänsyn till sådana faktorer vid utformning av teknologiska lösningar (Srite och Karahanna, 2006).

Vidare betonar studien (Srite och Karahanna, 2006) att individernas värderingar av individualism/kollektivism och maktdistans påverkar deras inställning till teknologi och dess användning. Medan individualistiska värderingar tenderar att betona individens autonomi och självständighet, kan kollektivistiska värderingar främja samarbete och gemenskap. Dessa insikter lyfter fram vikten av att anpassa teknologiska lösningar och implementationsstrategier utifrån de kulturella kontexter där de ska användas, och pekar på behovet av att integrera kulturella hänsynstaganden i teknologidriven innovation och för förändringar i framtiden.

3 Problemområde

Idag är biometrisk autentisering både som passiv men även aktiv biometri en vanlig metod till att få åtkomst och tillgång till sina enheter och information som lagras bakom autentiseringsprocessen. Detta har gjort att autentiseringsprocessen blivit effektivare och mer användarvänligt (Chaudhari et al., 2023; Xu, Zhou and Lyu, 2014; Meng et al., 2015). Detta i samband med att teckenlösenord börjar bli allt mer komplext om individen vill hålla sin information säker. Individen ska ej ha samma lösenord på flera ställen vilket kan bli jobbigt att komma ihåg om du har 20st användarkonton på olika sidor som kräver verifiering (Chopra, 2019). Samtidigt påpekar Chopra (2019) att ifall användaren har ett gemensamt lösenord till samtliga konton och det hackas eller sprids så är individen sårbar på samtliga ställen.

Utvecklingen av passiv biometri som autentiseringsmetod har vuxit snabbt och motar bort de problem som teckenlösenord haft samt att den är smidigare än aktiv biometrisk autentisering och användarvänligt (Chaudhari et al., 2023; Meng et al., 2015). Men till vilken kostnad? Det som potentiellt finns risk för är att exempelvis den kameran som analyserar och verifierar ansiktet eller den mikrofon som används för att kontrollera röst, vad händer ifall den används på felaktigt sätt av antingen företaget eller en utomstående entitet som vill agera mot en individ med negativa konsekvenser. Litar människan blint på säkerheten och att företag som bedriver och stödjer denna teknologi att de lovar att hålla integritet säker och att denna inte brister. Spelar demografin någon roll i de beslut som tas när användaren väljer att bruka denna funktion och vad påverkar individen att ta dessa beslut. Detta problemområde utgör grunden för en fördjupad utforskning för att förstå kopplingen mellan demografiska faktorer och individers syn på samt oro kring passiv biometrisk autentisering.

3.1 Problem/fråga

Första frågeställningen som ska besvaras är:

- *I vilken utsträckning påverkar olika demografiska attribut, såsom kön och utbildningsbakgrund, individernas attityd gentemot användningen av passiv biometrisk autentisering?*

Målet med detta är att jämföra de skillnader mellan individer även om det inte kan representera en hel demografisk grupp vill arbetet få en överblick om bakgrund påverkar individens attityd mot just passiv biometri som autentiseringsmetod.

Den andra frågeställningen som ska undersökas är:

- *Hur varierar demografiska grupper i sin beredvillighet att kompromissa med integritetsaspekter för att uppnå en förbättrad användarupplevelse och användarvänlighet i samband med passiv biometrisk autentisering?*

Detta är viktigt för att undersöka ifall olika demografiska grupper har varierande nivåer av tillfredsställelse med integritetsaspekterna av passiv biometrisk autentisering och hur

villiga de är att tämja på sin integritet i förhållande till användarvänlighet och upplevelse. Genom att identifiera samband mellan användarnas demografiska faktor samt deras tillfredsställelse kan utvecklare och företag i framtiden skräddarsy åtgärder och förbättringar för att adressera deras specifika behov samt bekymmer inom diverse demografiska grupper. Förhoppningsvis kan detta även leda till mer inklusiva lösningar framöver. Med begränsad antal respondenter kommer detta inte spegla en hel demografisk grupp utan med dessa frågeställningar kommer att testa ifall metoden och frågor kommer att kunna ge den form av underlag som eftersöks.

3.2 Avgränsningar

Den avgränsning kring den demografiska faktorn är kring kön och utbildningsbakgrund. Den geografiska aspekten kommer inte att undersökas eller andra demografiska aspekter. Detta för den tidsram som finns för arbetets gång samt antal deltagare kommer vara svårt att hitta för att kunna minska den partiskheten som finnes med färre antal deltagare än vad som behövs för att kunna få fram tydlig och konsekvent data.
Kön och utbildningsbakgrund är de enda demografiska aspekter som ska studeras och resultatet kommer spegla detta då inga andra aspekter kommer beaktas.

3.3 Förväntat resultat

Studien förväntas testa och utforska metoden för att identifiera eventuella samband och mönster mellan olika demografiska attribut och attityder/integritetsbekymmer gentemot passiv biometrisk autentisering. Detta ska i framtiden kunna ge klarhet i hur olika befolkningsgrupper reagerar på och uppfattar denna teknologi. Det ska även ge en insikt på hur variationer inom demografiska gruppers oro och attityder kring ämnet samt undvika att generalisera respondenterna. 28 respondenter kommer inte kunna representera en hel befolkning utan endast ge underlag för tillvägagångssättet att bruka denna metod på en större skala grupper.

4 Metod

Detta kapitel innefattar vilken metodansats som valts samt, hur material har samlats in och vart informationen kommer ifrån.

4.1 Val av metod

I detta arbete kommer både den kvalitativa och kvantitativa metodansatsen att tillämpas (Bryman, 2018). Genom att kombinera dessa två metoder kan vi få en mer omfattande förståelse av det ämne vi studerar. Kombinationen av metoderna gör det möjligt att inte bara identifiera mönster och samband på en övergripande nivå utan även att fånga upp de mer subtila och komplexa aspekterna av respondenternas upplevelser och åsikter. Detta metodval ger oss möjlighet att triangulera våra data, vilket ökar tillförlitligheten och validiteten i våra resultat.

Den kvantitativa metodansatsen tillämpas för att samla in numerisk data, med fokus på att undersöka och analysera mönster, samband och variationer inom ämnet för arbetet (Bryman, 2018). En av de största fördelarna med den kvantitativa metoden är att den möjliggör generalisering av resultaten till en större population tack vare datainsamlingen från ett stort antal respondenter. Numerisk data minskar också risken för forskarens subjektiva tolkningar, vilket kan öka studiens trovärdighet. Dessutom kan kvantitativa studier oftare replikeras, vilket är en viktig aspekt av vetenskaplig forskning.

Den kvalitativa metodansatsen fokuserar på att förstå och beskriva komplexa fenomen och sammanhang genom att samla in och analysera icke-numerisk data, såsom ord, bilder eller ljudinspelningar (Bryman, 2018). Denna metod erbjuder fördelen av att ge djupgående insikter genom att undersöka deltagarnas perspektiv på ett öppet och flexibelt sätt, vilket ger en djupare förståelse för komplexa och nyanserade aspekter av ett fenomen. Denna metodansats tillåter även att utforska hur kontextuella faktorer påverkar fenomenet, något som ofta förbises i kvantitativ forskning. Flexibiliteten i den kvalitativa metoden gör det möjligt att justera frågor och fokus under datainsamlingsprocessen baserat på deltagarnas svar och de nya insikter som uppstår.

Att kombinera kvalitativa och kvantitativa metoder, en strategi känd som metodtriangulering, erbjuder flera fördelar. Medan den kvantitativa metoden kan ge bredd och generaliserbarhet, kan den kvalitativa metoden ge djup och detaljerad förståelse. Tillsammans ger de en mer komplett bild av forskningsproblemet. Genom att verifiera resultat från en metod med en annan kan forskaren öka tillförlitligheten och validiteten i studiens resultat. Kombinationen av metoder kan också bidra till att identifiera och minska forskarens bias, eftersom olika metoder tenderar att ha olika styrkor och svagheter. Genom att använda både kvantitativa och kvalitativa metoder strävar denna studie efter att dra nytta av fördelarna med båda tillvägagångssätten, vilket ger en mer nyanserad och robust förståelse av forskningsämnet (Oppenheim 1992).

4.2 Arbetsprocess

Det strukturerade intervjuerna kommer följa riktlinjer enligt Oppenheim (1992). Detta genom att ha ett tydligt syfte och mål. I detta fall ska olika demografiska grupper uttrycka sina orohetsgrad och dylikt kring integritetsaspekterna vid passiv biometrisk autentisering. Därefter ska frågor designas som både ska vara tydliga och relevanta för ämnet där olika jargonger undviks för att samtliga deltagare ska ha samma förutsättningar att besvara frågorna jämlikt. För att få ut den uppfattade användarvänligheten och användbarheten ska majoriteten av frågor som designas besvaras enligt en likert skala där respondenten får betygsätta sin upplevde uppfattning i grad utav överensstämmelse eller oenighet om påståendet som förs fram. Detta sker i en Likertskala mellan värdena 1–7 där den kvantitativa datan som produceras kan användas för analys senare under processen. Följd frågor tillkommer även för att kunna få en förståelse om något avviker från den allmänna datan som produceras och kunna få en överblick ifall flera respondenter upplever samma typ av negativitet eller positivitet mot passiv biometri som autentiseringsmetod där denna kvalitativa data kan analyseras senare under processen.

Samtliga intervjuer kommer att spelas in och detta kommer att meddelas till deltagaren i god tid men även innan själva inspelningen startar.
Två testrespondenter ska intervjuas för att mäta tid, data och träna på standardisering av intervjuprocessen för att säkerställa att samtliga deltagare har samma upplevelse samt undvika eventuella problem och missförstånd. Ett kort intro ska skapas för att beskriva passiv biometri som autentiseringsmetod och skillnaden mellan aktiv och passiv. För att hitta respondenter kommer ett inlägg läggas upp på sociala medier som exempelvis Linkedin och Facebook för att hitta respondenter. Studien kommer kräva minst 30 deltagare för att kunna uppnå en mättnad i den data som samlas in men siktar på än så. Under hela processen ska Vetenskapsrådets (2018) riktlinjer beaktas för att både respektera individens integritet men även arbetets integritet. Viktigt att samtycke ges både innan men ifall respondent vill häva sitt deltagande ska detta vara fullt möjligt. Information om själva studien ska framföras tydligt för att samtliga deltagare vet vad studien handlar som och konfidentialitetskrav respekteras på sådant vis att inga personuppgifter behandlas med säkerhetsåtgärder och efter transkribering ska inspelning raderas.

Avslutningsvis ska svaren från respondenterna analyseras genom att mäta den kvantitativa data som producerats från de besvarade likert skalorna.
Det sker genom att summera eller omvandla enskilda respondenter eller grupper av respondenter till en sammanvägd poäng. Detta kan göras genom att lägga ihop poängen för varje svar eller att hitta genomsnittlig poäng beroende på deltagare. Utföra en frekvensanalys för varje svarsalternativ för att se fördelningen av svar. Detta ger en överblick över respondenternas huvudsakliga tendenser och preferenser. Beräkna standardavvikelsen för att mäta variationen i respondenternas svar. En hög standardavvikelse indikerar att svaren varierar mycket från genomsnittet.

Använda diagram, såsom stapeldiagram och cirkeldiagram, för att visuellt representera resultaten. Detta gör det lättare att observera mönster och skillnader.
Jämföra resultaten mellan olika demografiska grupper. Det kan inkludera jämförelser mellan kön, utbildningsbakgrund eller andra demografiska variabler. För att testa om skillnader mellan grupper är signifikanta. Tolka resultaten med hänsyn till den specifika forskningsfrågan.

När det gäller kvantitativ data handlar det om att sammanställa och analysera numeriska resultat, vanligtvis med hjälp av statistiska metoder för att identifiera mönster, samband och variationer. Detta kan inkludera frekvensanalys och korrelationsanalyser och
efter att ha analyserat varje data typ separat jämförs resultaten för att se om de kompletterar varandra eller om det finns motsägelser eller skillnader. Detta kan göras genom att titta på hur de olika datatyperna belyser samma fenomen eller fråga på olika sätt. Om resultaten överensstämmer kan det öka tillförlitligheten i studien och bekräfta forskningsresultatens validitet. Om det finns skillnader eller motsägelser kan forskarna gräva djupare för att förstå varför och identifiera eventuella brister i studien.
I slutändan kan denna jämförelse bidra till att ge en mer omfattande förståelse av det undersökta fenomenet och öka studiens validitet och tillförlitlighet.

Utbildningskategorierna kommer att delas upp i 3 olika grupper för att underlätta kommer grupper slås ihop på detta vis, grundskola och gymnasiet till en kategori, Yrkes och folkhögskola till en kategori och en kandidat samt master till en annan kategori. Kategori 1 kommer kallas K1 (Grundskola/Gymnasial), Kategori kommer kallas K2 (Yrkesutbildning/Yrkeshögskola/Folkhögskola) och Kategori 3 kommer kallas K3 (Kandidatexamen/Masterexamen). Män och Kvinnor i en grupp och sedan ska K1, K2, K3 jämföras bland könen.

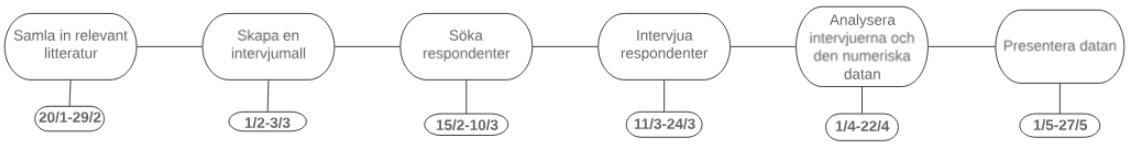
Varav 14 kvinnor och 14 män som har olika utbildningar men vilket togs ej i beaktning vid första intervjukontakt vilket leder till att en grupp av könen finns och tillhör i en större mängd av en viss typ av kategori. Detta är för att intervjudeltagarna varit slumpmässigt utvalda när det kommit till utbildning men inte kön. Sedan jämföra ifall svaren skiljer sig åt markant och vad det beror på eller ifall det ens gör detta. Genom att ta fram standardavvikelsen kan även avvikelser presenteras ifall grupperna svarar på helt olika sidor av spektrumet eller att åsikterna är lika. Detta för att påvisa hur trovärdigt genomsnittet är eller om det skiljer sig markant mellan individer där genomsnittet inte alltid är pålitligt. Sedan är det värt att notera att detta inte är representativt för en hel demografisk grupp utan ifall dessa fynd som hittas kanske inte är signifikanta då antal respondenter är begränsad.

Därefter ska även de följdfrågor som är mer öppna för att få förståelse av bakgrunden till vissa svar analyseras kvalitativt och kategoriseras för att hitta samband och olika teman mellan olika typer av upplevelser bland respondenterna. Därefter att ha analyserat de två datatyperna separat, identifieras samband och jämförelser mellan dem. En metod som används är triangulering, där resultaten från båda datatyperna jämförs för att se om de

bekräftar varandra. Om kvalitativa intervjuer indikerar hög användartillfredsställelse med en ny teknik och kvantitativa undersökningar visar höga poäng på användartillfredsställelse, ökar detta tillförlitligheten i resultaten.

Vidare jämförs teman från den kvalitativa analysen med resultaten från den kvantitativa analysen. Om exempelvis ett tema från intervjuerna är att användare oroar sig för integritet, kan detta jämföras med kvantitativa data om hur många respondenter som betygsatte integritetsaspekten som viktig i en enkät.

Intervjuerna kommer ske under veckorna 11 och 12 (11–24 mars 2024) och bokas in i slutet på februari fram tills första veckan i mars (8e mars). Varje intervju ska ta mellan 20–30 minuter och kan ske både på distans via Telefon eller någon form av kommunikationsapplikation likt Zoom eller på neutral fysisk plats i någon av Högskolan i Skövdes lokaler. Intervjun kommer bestå av totalt 35 frågor varav 5 kontrollfrågor (**se bilaga 1**) för att fastställa att svaren under intervjun är konsekventa med tidigare svar. När samtliga frågor har besvarats ska dessa kvalitets checkas gemensamt med respondenten för att säkerställa att deltagare är nöjd med sina svar.



Figur 1 - Arbetsprocess

När all kvalitativt och kvantitativ data är sammanställd ska det sedan jämföras med den litteratur som sammanställts i bakgrundskapitlet. Detta sker genom att jämföra ifall respondenternas upplevelser kring integritet överensstämmer med de problem och bekymmer men även den användarvänliga aspekterna som lyfts.

Svaren från intervjuerna ska sedan jämföras med litteraturen och studier kring relaterade ämnen som ex olika användarupplevelser kring säkerhet kopplat till IT och användning utav internet banker (E-banking). Hur dessa korrelerar med just passiv biometrisk autentisering.

4.3 Forskningsetiska principer

Ansvar, respekt, ärlighet och tillförlitlighet är forskningsetiska principer som ska beaktas i detta arbete från början till slut. Det gäller att vara ärlig, genom att granska arbetet på ett objektivt sätt. Respektera samtliga deltagare, kollegor och miljön samt säkerställa kvalitén på forskningen (Vetenskapsrådet, 2018).

4.3.1 Konfidentialitetskrav

Detta krav finns för att respektera individens integritet, genom att behandla personuppgifter med extra försiktighet och ha säkerhetsåtgärder samt i konfidens behandla uppgifterna. Samtliga respondenter kommer att tilldelas ett smeknamn som inte kan kopplas till individens personuppgifter samt att inspelningarna kommer bara att sparas fram till transkribering är färdig för att inte behålla inspelningen längre än vad som behövs för att utföra arbetet (Vetenskapsrådet, 2018).

4.3.2 Samtyckeskrav

För att denna studie ska följe det samtyckeskrav som Vetenskapsrådet (2018) rekommenderar, ska deltagaren ge samtycke till användning av information som samlas in under intervjun. Det ska vara tydligt både vi kontakt men även under intervjun ska deltagare behöva ge sitt samtycke. Då studien riktar sig till personer som är över 18 år är samtliga deltagare myndiga.

4.3.3 Informationskrav

Deltagaren ska även informeras av forskaren över det som gäller, vad studien handlar om och vad för villkor som finns. Om deltagaren skulle vilja avbryta sitt deltagande under processens gång så ska detta vara möjligt och det ska även informeras till deltagaren för att respektera individens val och integritet (Vetenskapsrådet, 2018). Vid inbjudan till intervju har samtliga deltagare fått information om detta och även en extra gång innan starten av intervjun för att deltagaren ska veta sin a rättigheter och ifall denna skulle vilja avbryta.

5 Materialpresentation

I detta kapitel ska det insamlade materialet från intervjuerna presenteras.

5.1 Intervjudeltagare

För denna studie intervjuades 28 personer. 14 män 14 kvinnor som tilldelats olika ID:n likt R1, R2 osv. Se bilaga 2 för att får en komplett lista av samtliga deltagare som anonymiserats där endast relevant demografisk tillhörigt noterats vilket är kön och utbildningsbakgrund. Delat upp efter olika kategorier på detta vis:

Kategori 1 kommer kallas K1 (Grundskola/Gymnasial), Kategori kommer kallas K2 (Yrkesutbildning/Yrkeshögskola/Folkhögskola) och Kategori 3 kommer kallas K3 (Kandidatexamen/Masterexamen). Män och Kvinnor i en grupp och sedan ska K1, K2, K3 jämföras bland könen.

Kön	K1	K2	K3
Man	8	3	3
Kvinna	5	3	6

Tabell 1 – Fördelning av deltagare

Sedan ska även samtliga männen och kvinnor delas upp i KM respektive KF. Kategori Male (KM) är kategori för männen och Kategori Female (KF) för kvinnorna och har 14 deltagare vardera.

För att se Intervjufrågor så detta finnes under Bilaga 1. Där inkluderas även ett intro som lästs upp för deltagarna innan intervjun.

6 Analys

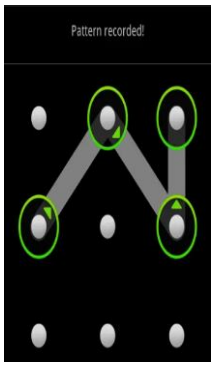
Här ska intervjusvaren analyseras och jämföras med bakgrundslitteraturen. Poäng från likertskalor ska presenteras i genomsnittlig poäng istället för totalpoäng med anledning av varierande antal deltagare i dem olika kategorierna. Tematisk analys av frisvars frågor för att hitta samband och olikheter bland deltagarnas svar.

6.1 Användande av autentiseringsmetoder

Av samtliga deltagare var det endast en som inte hade använt någon form av passiv biometrisk autentisering. Fortsättningsvis visade det sig att samtliga 27 deltagare som använt passiv biometrisk autentisering har gjort detta genom en telefonenhet, primärt Iphone och Android enheter. Utöver detta fanns det även 5 deltagare som använt en passiv biometrisk autentiseringsmetod genom datorer/laptops. En från varje grupp förutom Man tillhörande grupp i **K1** har använt passiv biometrisk autentisering för att autentiserings sig på en dator.

För att sedan jämföra vilken typ av autentisering som föredrogs av deltagarna visades 4 olika bilder upp som hänvisar till olika autentiseringsmetoder som idag används och de olika deltagarna fick välja mellan de 4 olika alternativen.

1



2

3

4

Bild 1 visar en typ av pinkod som är vanligt att använda när autentiseringen sker när inte biometriska aspekterna funkar eller inte är möjlig att utföra av någon anledning och just denna är ifrån företaget Apples system som idag används för primärt Iphones och Ipads. Bild 2 är ett mönster autentiseringsmetod. Denna är ifrån de en variant av Android telefon som brukas idag. Bild 3 representerar ansiktsigenkänning och bild 4 visar en form av fingeravtryckavläsning.

Endast en person föredrog autentiseringsmetod 1 och 2 och det var en Kvinna tillhörande **K1**. Resterande deltagare valde metod 3 där två av deltagarna även har haft med metod 4 med sig men ingen av dessa valde endast 4 utan hade det samtidigt som metod 3. Dessa två är tillhör **K1** och är av könen man och kvinna respektive.

För att få lite djup varför ansiktsigenkänning är den föredragna metoden fick deltagarna förklara på ett djupare plan varför denna metod föredrogs i form av en intervjufråga som lyder,

- Vilken autentiseringstyp föredrar du vanligtvis och varför? Finns det några specifika?

Man tillhörande **K1** säger:

Ansiktsigenkänning. Det är smidigare och går väldigt fort att komma in på telefonen där jag slipper komma ihåg lösenord och sådant.

Att det går fort och är smidigt är ett återkommande tema som flera deltagare nämner där de kommer från båda könen och tillhörande samtliga utbildningsbakgrunder. Detta är linje med det som Rui och Yan (2019) nämner att med denna metod har det underlättat för användare att autentisera sig.

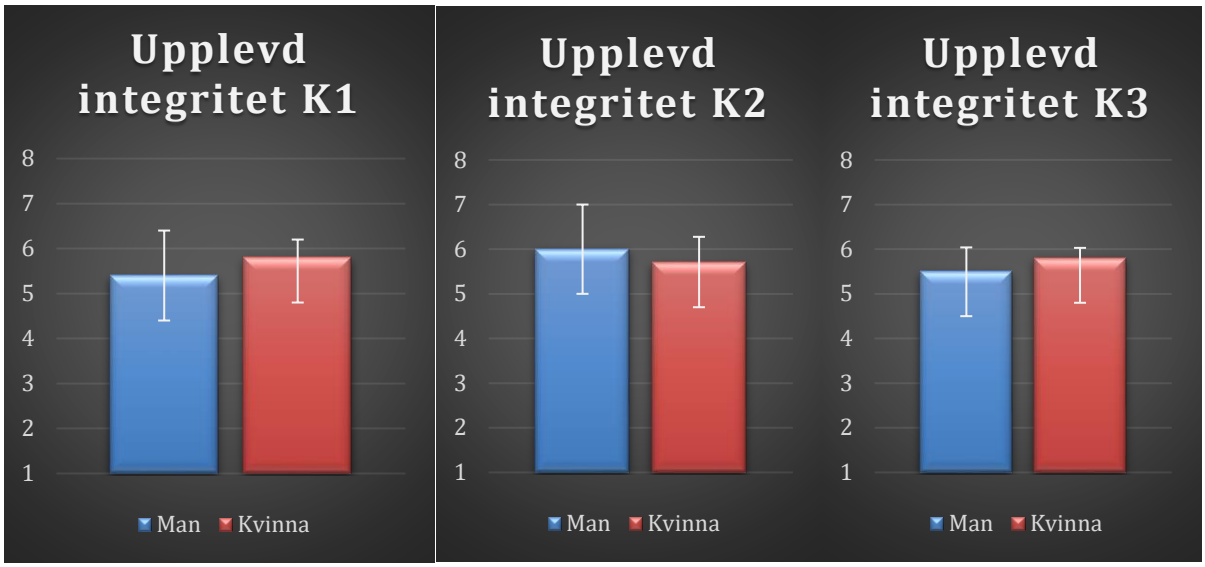
6.2 Hur viktigt anses integriteten

6.2.1 Upplevda integriteten

Att beakta upplevda integriteten och den faktiska integriteten bland användaren när det kommer till biometri i olika former är två faktorer som är helt olika. Du kan känna dig trygg med att datan som lagras verkar säker men samtidigt inte vara det då det an finnas brister. Respondenterna är tydliga med att användarupplevelsen är det viktiga när det kommer till passiv biometri som autentiseringsmetod. Det ska gå fort, enkelt och slippa komma ihåg lösenord som andra personer kan se över axeln när det knappas in. Det är flera teman som är återkommande bland olika respondenter.

För att fokusera på hur respondenterna anser den upplevda integriteten, besvarades några frågor för att fastställa hur anseendet är och om respondenternas upplevelse om integriteten respekteras utav företag. Till frågan:

- *Hur skulle du bedöma din upplevelse av hur företag behandlar din biometriska data med fokus på integritet?*



Figur 2 – Stapel 1

Att en respondenten ska förstå hur företag hanterar sin data är inte meningen att utforska men hur den upplevs är syftet, det kan vara att respondenten blir informerad om hur informationen lagras, vart den tar vägen eller annan orsak som påverkar upplevda integriteten.

Bland de olika utbildningskategorierna var det inget som stack ut, utan upplevelsen bland respondenterna till hur deras data hanteras var hög och avvikelsen inget märkvärdigt.

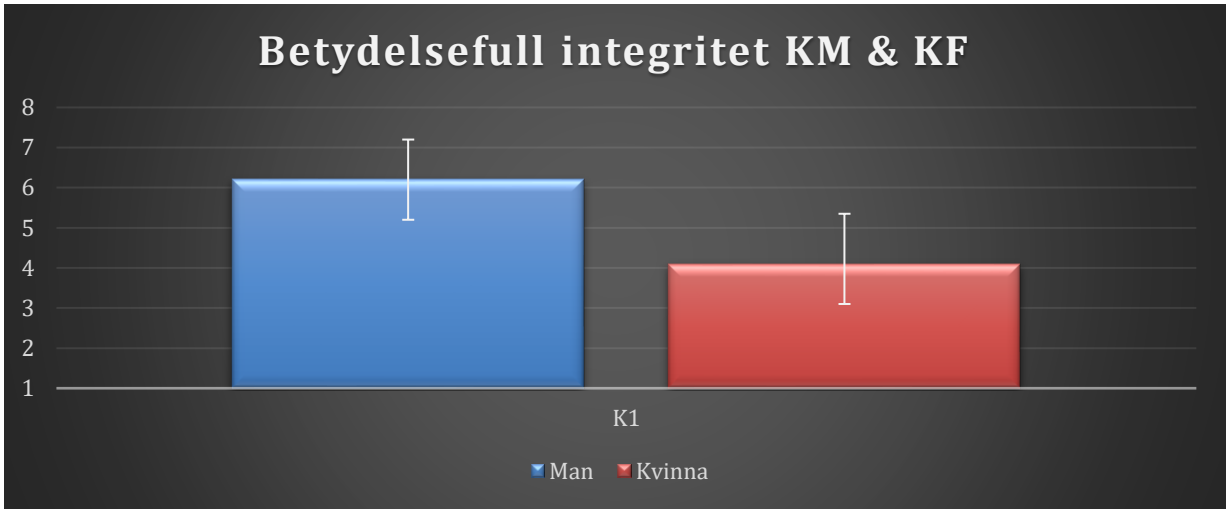
Jämförs det bland kön och kategorier skiljer det sig inte markant utan siffrorna justeras lite med att kvinnor i **K1** har lite bättre upplevelse än män men där antal deltagare måste beaktas. En följdfråga ställdes för att få en inblick i vad respondenterna tänkte och där nämndes det att information om hur datan lagras finns att söka efter på exempelvis Apples hemsida och att de är transparanta om hur datan lagras. **R4, R15** och **R26** beskriver att den informationen inte skickas till något externt system utan att den behålls lagrad i enheten enligt respondenterna. **R15** säger även *"Ett så stort företag som exempelvis Apple måste ju kunna gå att lita på när det kommer till säkerhet. Finns ju en anledning till att många använder deras produkter och telefoner.".* Tillsammans med tidigare respondenter finns det olika dimensioner till förtroendet för företagen och dessa autentiseringssystem något som Zhaleh Semnani-Azad et al (2019) påpekar.

Transparens är en grundläggande princip för att säkerställa integritet vid användning av biometriska autentiseringsteknologier. Genom att tillhandahålla användare med tydlig och begriplig information om hur deras biometriska data samlas in, lagras och används, kan förtroendet för teknologin stärkas. Användarna måste vara medvetna om vilka data som samlas in, syftet med insamlingen och eventuella tredjepartsdelningar av data. Denna öppenhet ger användarna möjlighet att fatta informerade beslut om sin integritet och väger riskerna och fördelarna med att använda biometriska autentiseringsteknologier (Mamonov and Benbunan-Fich, 2015).

6.2.2 Hur viktig är integriteten

Att användare upplever att integriteten beaktas av företag och andra aktörer är positivt men något som skiljer sig är ifall respondenterna tycker att integriteten faktiskt är betydelsefull när det kommer till biometriska autentiseringsmetoder. Hur ser användarna av biometriska system på hur viktig det är att deras integritet respekteras eller är det något som förbises och inte är en prioritet till detta.

- *Hur betydelsefull anser du integriteten vara vid användning av biometriska autentisering teknologier?*



Figur 3 – Stapel 2

Det som stack ut här är att mellan könen var det 2,1 poäng som skiljde sig åt när denna fråga besvarades. Männen ansåg att integriteten var mer betydelsefull vid användning av biometriska autentiserings metoder där ett återkommande tema som snabbt, effektiv och simpelt framkommer och 4,1 på skalan påvisar att den inte är lika prioriterad bland kvinnorna. Jämförs detta med männen så har de en genomsnittlig poäng på 6,2. **R18** beskriver det såhär; *"Integriteten är oerhört betydelsefull för mig vid användning av denna typ av autentisering eftersom det handlar om att säkerställa mitt skydd mot missbruk eller obehörig åtkomst av min personliga data.".* Till exempel, om en person använder ansiktsigenkänning för att låsa upp sin telefon, är det viktigt att deras ansiktsdata inte missbrukas eller komprometteras. Om så skulle ske kan det leda till allvarliga integritetsintrång och potentiellt missbruk av personuppgifter. Därför är det nödvändigt att integrera starka integritetsåtgärder och säkerhetsprotokoll för att säkerställa att biometriska autentiseringsmetoder inte hotar användarnas integritet (Mamonov and Benbunan-Fich, 2015).

Standardavvikelsen bland svaren är lite högre när det jämförs bland könen då svar på båda sidor av spektrumet har givits och flera respondenter är inte helt överens om hur viktigt integriteten faktiskt är.

Utöver detta är säkerheten för biometriska data är avgörande för att skydda användarnas integritet. Biometriska data är känsliga och unika för varje individ, vilket gör dem till attraktiva mål för potentiella angripare. Därför måste lämpliga säkerhetsåtgärder vidtas för att förhindra obehörig åtkomst, manipulation eller stöld av biometriska data (Anil et al., 2008).

Användarkontroll över biometriska data är avgörande för att respektera användarnas integritet och autonomi. Användarna bör ha möjlighet att hantera och kontrollera sin egen biometriska data, inklusive att kunna radera eller begränsa dess användning. **R17** och **R18** påpekar detta när de blir bemötta med denna fråga;

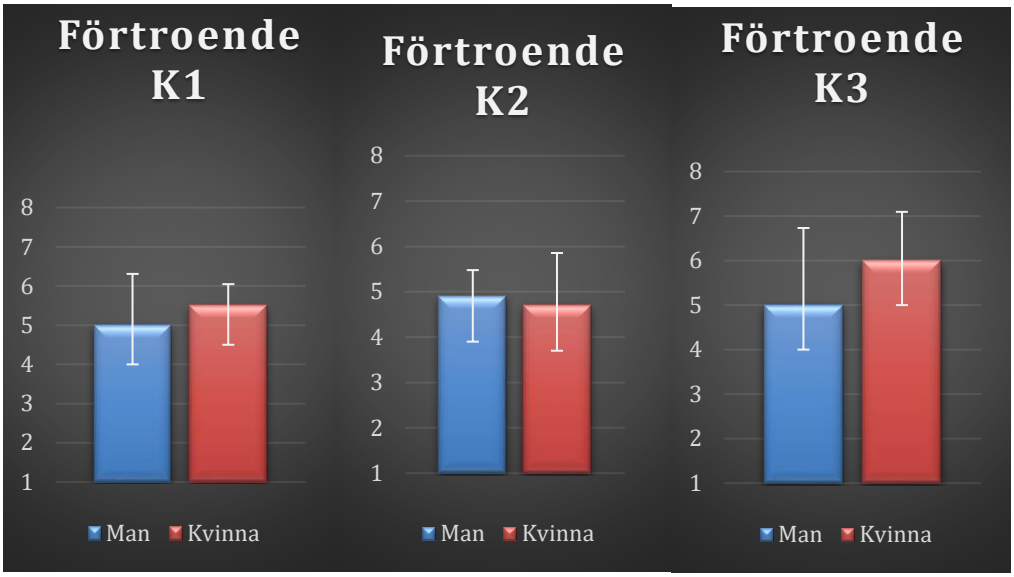
- För att fördjupa oss i ditt svar, kan du beskriva några specifika aspekter av integritet som du anser vara särskilt viktiga eller mindre viktiga i detta sammanhang?

Respondenterna menar att kunna radera sina biometriska data ifall användaren vill detta ger förtroende och att denna data inte lagras kvar i telefonen utan raderas för alltid och har sin integritet respekterad. Mamonov and Benbunan-Fich (2015) förklarar genom att ge användarna denna kontroll kan organisationer demonstrera respekt för användarnas integritet och bygga förtroende för sina autentiseringsprocesser. Användarkontroll kan också öka användarnas komfort och tillit till teknologin, vilket kan främja dess bredare antagande och användning.

6.3 Förtroende för passiv biometri som autentiseringsmetod

Användare ser passiv biometri som en bekväm autentiseringsmetod eftersom den eliminerar behovet av att komma ihåg komplicerade lösenord eller genomföra manuella autentiseringssteg. För dessa användare ökar passiv biometri användarupplevelsen och ger en känsla av smidighet och effektivitet. **R13** säger att ”Det är så smidigt. Att slippa komma ihåg lösenord varje gång jag vill låsa upp min lur är skönt” och detta tema är återkommande bland respondenter av samtliga kön och kategorier.

Användaracceptans är kritisk för framgången med passiv biometri som autentiseringsmetod. Om användare inte litar på tekniken eller känner sig obekväma med att använda den, kommer de sannolikt att undvika att använda den eller föredra andra autentiseringsmetoder som pinkod/lösenord. För att öka användaracceptansen är det viktigt att kommunicera fördelarna med passiv biometri tydligt och att adressera användarnas oro för integritet och säkerhet genom att implementera starka säkerhetsåtgärder och tydliga integritetspolicyer som formuleras ut och där transparens är viktigt (Rui and Yan, 2019). Detta stämmer överens med hur viktig denna fråga är bland respondenterna. Frågan om förtroende för passiv biometri som autentiseringsmetod svarade grupperna som följande:



Figur 4 – Stapel 3

Vi ser att **K2** överlag har ett högre förtroende kring än dem andra två kategorierna men inte en allt för stor sådan. Däremot ser vi att männen i **K3** har ett mycket lägre förtroende till detta och det kan bero på att antalet deltagare som är män i **K3** är 3st och att en persons negativa upplevelser har stor påverkan på det slutgiltiga genomsnittspoängen vilket standardavvikelsen förtydligar i figuren. Det som avviker är att svaren är väldigt blandade och en gemensam konsensus inte finns bland kategorierna.

Förtroende för passiv biometri påverkar även organisationernas rykte samt varumärke. Om användaren inte litar på organisationen för att hantera deras biometriska data på ett säkert sätt kan det skada organisationens förtroende och rykte. Det kan leda till förlorade affärsmöjligheter, minskad kundlojalitet och negativ publicitet vilket dessa verksamheter vil undvika i högsta mån. Därför är det avgörande för organisationer att bygga förtroende för sin hantering av biometriska data genom att implementera starka säkerhetsåtgärder, transparenta integritetspolicyer och effektiv kommunikation med sina användare (Akhtar, Michelon and Gian Luca Foresti, 2014).

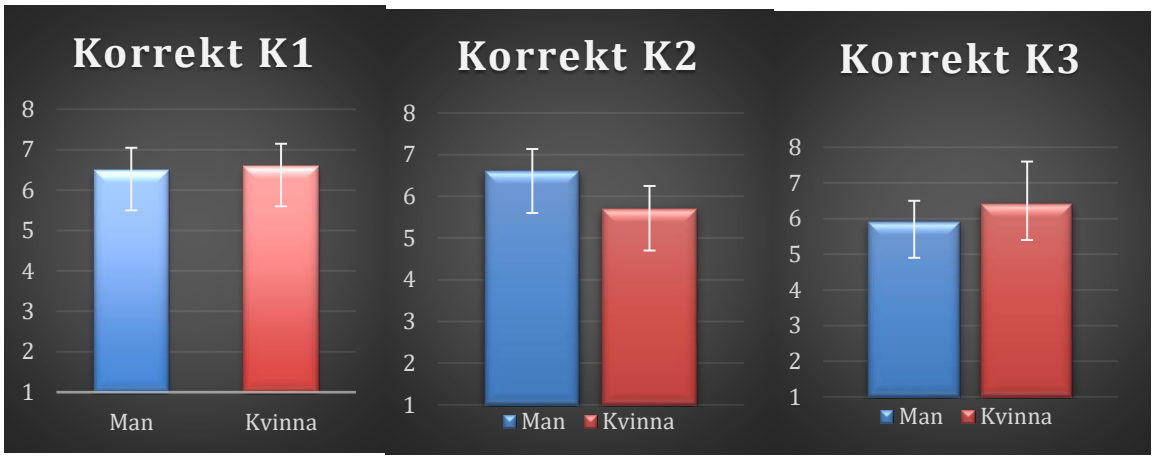
6.4 Den framtida synen på passiv biometri som autentiseringsmetod

I framtiden kan vi förvänta oss att passiv biometri blir allt vanligare som autentiseringsmetod på grund av dess fördelar med användarvänlighet och säkerhet. Med passiv biometri kan användarna snabbt och enkelt låsa upp sina enheter, logga in på sina konton och genomföra transaktioner utan att behöva komma ihåg komplicerade lösenord eller PIN-koder. Detta gör användarupplevelsen smidigare och mer bekväm, vilket i sin tur kan öka antagandet av passiv biometri (Anil et al., 2008).

Samtidigt kan vi se en ökad villighet från användarna att lämna över mer information för att förbättra användarupplevelsen. Med passiv biometri kan användarna vara beredda att dela med sig av sina biometriska data, såsom ansiktsigenkänning, fingeravtryck eller röstigenkänning, för att få tillgång till en mer personlig och anpassad upplevelse. Till

exempel kan biometrisk data användas för att anpassa gränssnitt, rekommendationer eller tjänster baserat på användarens unika preferenser och beteenden.

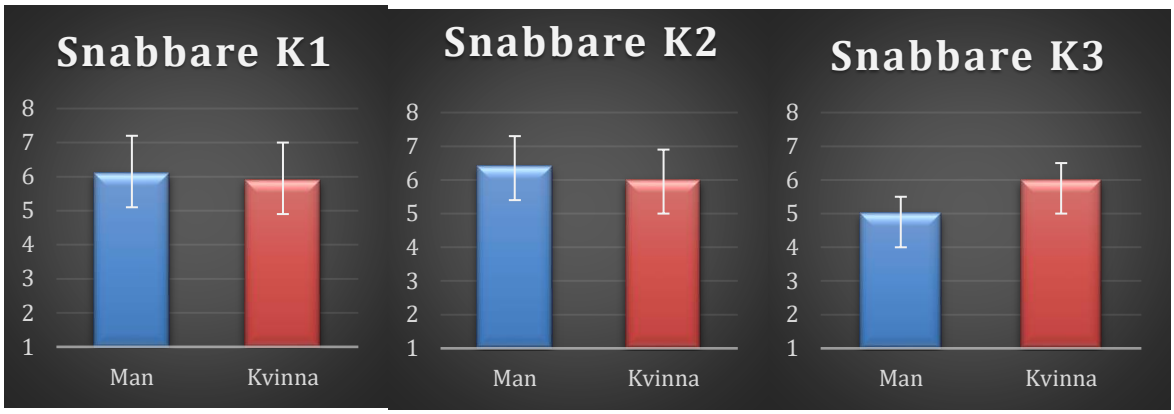
- Är du villig att lämna ifrån mer biometrisk data till din enhet för att öka autentiseringsprocessens korrekthet vid autentisering.



Figur 5 – Stapel 4

Respondenterna är mer benägna att lämna ifrån sig mer av sin biometri för att göra processen mer korrekt och att undvika felaktig autentisering eller en falsk negativ autentisering. Detta indikerar en ökad betoning på användarupplevelsen och behovet av en smidig och tillförlitlig autentiseringsprocess. Genom att öka precisionen i autentiseringsmetoden kan användarna känna sig tryggare med att deras identitet korrekt verifieras utan onödiga hinder eller störningar (Lyu, 2020). Det är emellertid viktigt att balansera denna ökade tillit med hänsyn till integriteten hos den biometriska data som samlas in. Det krävs en tydlig och transparent hantering av biometrisk information för att säkerställa användarnas förtroende och integritet samtidigt som autentiseringsprocessens korrekthet förbättras. Därför är det avgörande att implementera robusta säkerhetsåtgärder och strikta integritetsrutiner för att garantera att användarnas biometriska data hanteras på ett ansvarsfullt och säkert sätt. Genom att göra detta kan man skapa en balans mellan autentiseringsprecision och integritetsskydd, vilket möjliggör en smidig och säker autentiseringsupplevelse för användarna.

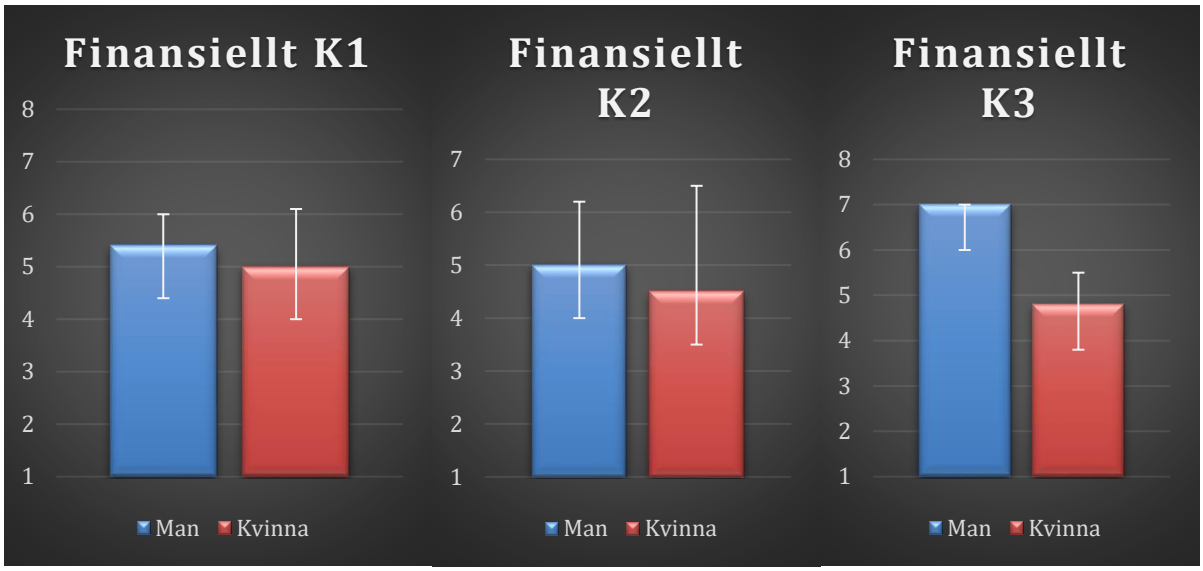
- Är du villig att lämna ifrån mer biometrisk data till din enhet för att autentiseringsprocessens ska bli snabbare



Figur 6 – Stapel 5

Respondenterna är mer benägna att dela med sig av ytterligare biometrisk data för att snabba på autentiseringsprocessen och minska tiden för autentiseringsåtgärder. Denna tendens pekar på en ökad betoning på användarvänlighet och önskan att undvika långa väntetider eller fördröjningar vid inloggning. Trots önskan om snabbhet är det viktigt att bevara en balans mellan hastighet och integritet, och att säkerställa att den biometriska datahanteringen är robust och följer strikta integritetsnormer. Genom att sträva efter snabbare autentiseringsmetoder kan användarna uppleva en mer effektiv användarupplevelse samtidigt som deras integritet skyddas på ett tillfredsställande sätt (Rui and Yan, 2019). Kvinnor i **K3** och män i **K2** vill i större utsträckning lämna ut mer biometrisk data för att effektivisera och förbättra autentiseringsprocessen. Även om samtliga grupper verkar ha högt förtroende mot dessa men även villiga att lämna ut mer är tecken på att deltagarna uppskattar denna typ av autentisering och har en positiv syn på företagen som hanterar denna data.

- Hur bekväm skulle du vara med att använda passiv biometrisk autentisering för att godkänna finansiella transaktioner?



Figur 7 – Stapel 6

Det finns en tydlig könsskillnad när det kommer till förtroendet för passiv biometrisk autentisering för finansiella transaktioner. Kvinnorna i studien tenderar överlag att ha lägre förtroende för denna autentiseringsmetod i jämförelse med män. Denna skillnad kan delvis bero på olika risktoleransnivåer och upplevelser av säkerhet relaterade till finansiella transaktioner. Män, särskilt de i åldersgruppen **K3** verkar vara mer benägna att omfamna passiv biometrisk autentisering för att godkänna finansiella transaktioner, möjligen drivna av en högre tolerans för teknologisk innovation och en ökad bekvämlighetsnivå med digitala betalningsmetoder. Å andra sidan kan kvinnor vara mer försiktiga när det gäller att använda biometrisk autentisering för finansiella ändamål på grund av oro för säkerhet och integritet. Det är viktigt att ta hänsyn till denna könsskillnad i förtroende för att utforma autentiseringsmetoder som passar olika användarbehov och preferenser. Detta gentemot hur villiga kvinnorna svarade i frågan om effektivitet och korrekthet är en obesvarad faktor ifall tilliten till företagen som hanterar biometriska data idag mer pålitliga än de företag som ska hantera finansiella transaktionerna som finns. Männen överlag verkar ha liknande syn bland utbildningskategorierna medan kvinnorna har högre standardavvikelse och variation i sina svar.

Den framtida synen på passiv biometri som autentiseringsmetod och villigheten att lämna över mer information för ökad användarupplevelse kan ses som en avvägning mellan användarvänlighet och integritet. Användarna kan vara villiga att dela med sig av mer information om de ser klara fördelar och värde i utbyte mot en förbättrad användarupplevelse eller som Watt (2017) nämner, kommer detta ge en trygghet. För användaren att teknologin förstärks. Samtidigt är det viktigt att säkerställa att användarnas integritet och personuppgifter skyddas på ett säkert och ansvarsfullt sätt för att bygga och upprätthålla förtroende för passiv biometri som autentiseringsmetod.

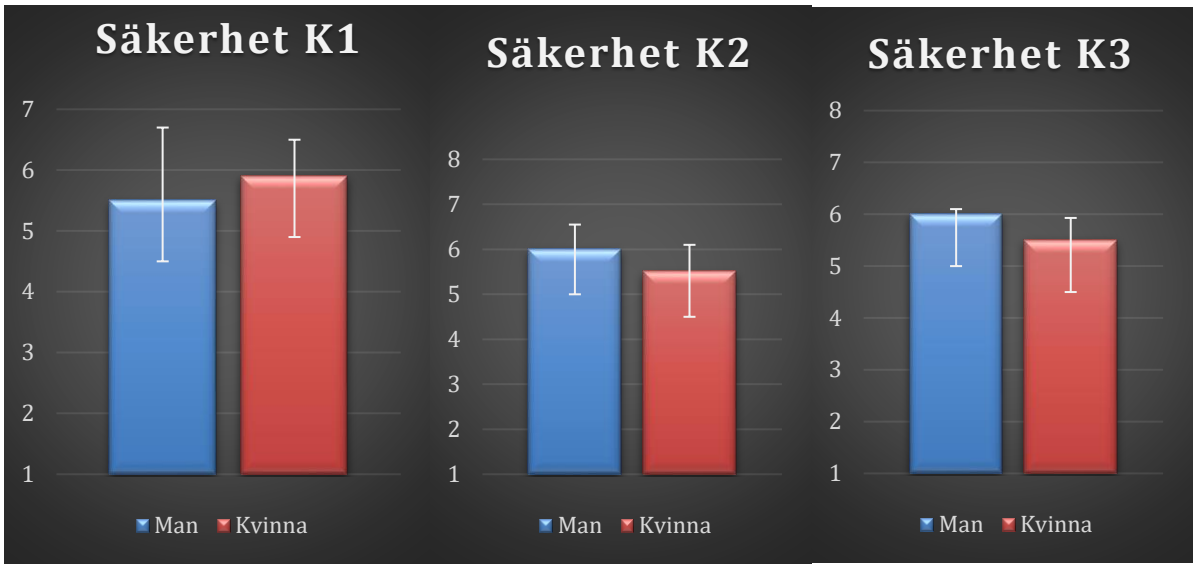
6.5 Informationssäkerhet

Från intervjuerna har insikt i deras synpunkter och bekymmer kring informationssäkerhet i samband med passiv biometrisk autentisering och dess relevans för integritet och användning av telefoner. Många av respondenterna uttryckte en övergripande oro för säkerheten kring insamling och hantering av biometriska data, och särskilt dess koppling till integritet. **R13** uttryckte sin oro*: "Jag har väl haft en oro för att min biometriska data kan komma i fel händer. Går ju inte direkt att byta biometrin"* Om bristen på säkerhet kring passiv biometrisk autentisering existerar, kan detta ha betydande konsekvenser för samhället i stort. För det första kan en sådan brist leda till ökad risk för identitetsstöld och bedrägeri. Om biometriska data komprometteras kan detta möjliggöra för angripare att genomföra olagliga transaktioner eller få obehörig åtkomst till känslig information om användare. Dessutom kan en brist på säkerhet kring passiv biometrisk autentisering underminera förtroendet för digitala tjänster och teknologier som använder denna autentiseringsmetod. Om användarna inte känner sig säkra på att deras biometriska data skyddas på ett tillförlitligt sätt, kan detta leda till ökad skepsis och tveksamhet att använda sådana system. Detta kan i sin tur hämma utvecklingen och antagandet av innovativa teknologier som är beroende av passiv biometrisk autentisering.

Denna oro för integriteten hos den biometriska data som samlas in och används för autentisering var tydlig hos många av respondenterna. De uttryckte en önskan om att ha tydliga garantier för att deras biometriska data skulle hanteras på ett säkert och ansvarsfullt sätt som Venkatesh, Thong and Xu (2012) nämner.

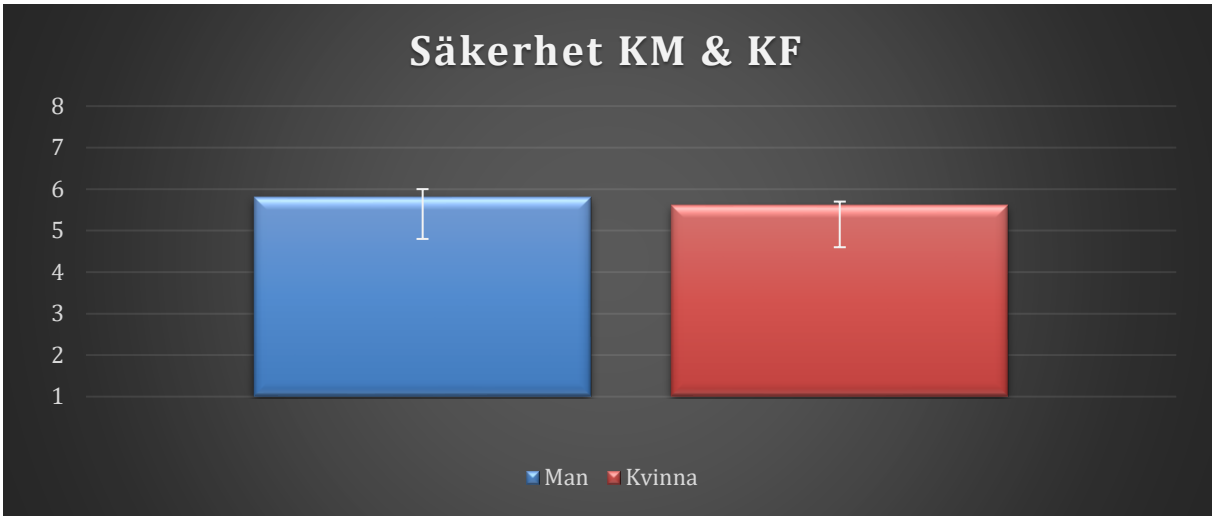
Vidare uttryckte respondenter oro för säkerhetsrisker relaterade till potentiella attacker på autentiseringsmetoden i sig, särskilt när det gäller användning av telefoner. **R9** säger "*Jag är rädd för att någon ska försöka lura systemet med fejkade biometriska data, särskilt när det gäller min telefon. Det är viktigt att tekniken är tillräckligt stark för att hantera sådana attacker*.". En brist på säkerhet kring passiv biometrisk autentisering ha allvarliga konsekvenser för integriteten hos användarna. Biometriska data är ofta kopplade till personliga och unika egenskaper hos individer, och exponering av denna data kan leda till allvarliga integritetsintrång. Detta kan inkludera risker för övervakning, missbruk av personlig information och andra former av kränkningar av användarnas integritet. bristen på säkerhet kring passiv biometrisk autentisering skapa en osäker digital miljö där användarna känner sig utsatta för potentiella hot och risker Detta kan ha en negativ inverkan på användarnas tillit till digitala tjänster och teknologier, vilket i sin tur kan hämma tillväxten och utvecklingen av digitala samhällen och ekonomier.

- Hur säker känner du dig över säkerheten när du använder passiv biometri som autentiseringsmetod



Figur 8 - Stapel 7

K2 och **K3** har lika förtroende för säkerheten av passiv biometri där männen har en lite mer förtroende för säkerheten av teknologin än kvinnorna. Det är i **K1** där kvinnorna har haft större förtroende för säkerheten på enheterna. Att allt fler använder denna metod och att det blivit mer socialt acceptabelt påverkar kanske besluten för männen att använda detta system likt det Kim (2016) påpekar. K1 och K2 svara i större grad liknande med varandra med medan i K1 är avvikelsen större och att respondenterna inte är lika överens med varandra.

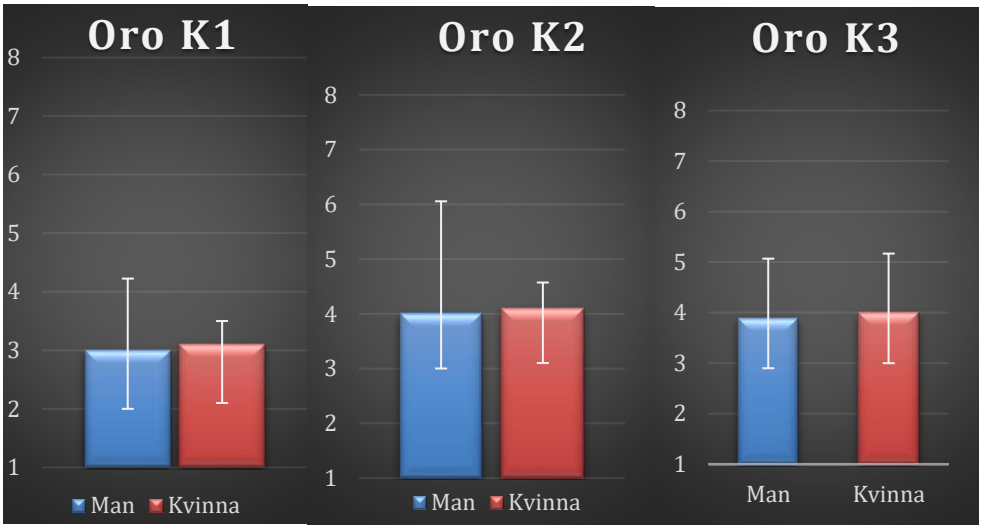


Figur 9 – Stapel 8

Skillnaderna är inte markanta och standardavvikelsen är inte något märkvärdigt mellan könen utan säkerhetsmässigt skiljer det sig lite mellan könen och kategorierna. Genom den tematiska analysen har det framkommit att använda sig av denna metod anses väldigt

säkert för annars hade denna inte använts något som **R12, R18** och **R23** nämner i intervjun.

- Är du orolig att någon aktör oavsett avsikt kommer åt din biometriska data med hjälp av diverse verktyg.



Figur 10 - Stapel 9

Intervjuerna att informationssäkerhet är en central oro för individer när det gäller användningen av passiv biometrisk autentisering och dess relevans för integritet, särskilt i samband med användning av telefoner för att skydda bilder, data, biometri och annat som lagras på enheterna. För att öka användarnas förtroende och säkerställa en säker och pålitlig autentiseringsupplevelse är det avgörande att implementera robusta säkerhetsåtgärder för både insamling och hantering av biometriska data samt för att motverka potentiella attacker på autentiseringsmetoden i sig, särskilt när det gäller användning av mobila enheter som exempelvis telefoner och laptops (Venkatesh, Thong and Xu, 2012). För att undvika sådana negativa konsekvenser är det avgörande att implementera säkerhetsåtgärder och regleringar för att skydda biometriska data och säkerställa en säker och pålitlig användning av passiv biometrisk autentisering. Detta inkluderar utveckling av avancerade krypterings- och autentiseringsalgoritmer, strikta integritetspolicyer och regleringar för hantering av biometriska data samt kontinuerlig övervakning och utvärdering av säkerhetslösningar för att identifiera och åtgärda potentiella sårbarheter (Akhtar, Michelon and Gian Luca Foresti, 2014).

7 Resultat

I detta kapitel ska resultatet från analysen och studien presenteras. De två frågeställningarna besvaras var för sig i olika delkapitel.

7.1 Användning av passiv biometri som autentiseringsmetod

Den första frågeställningen som ska besvaras är *"I vilken utsträckning påverkar olika demografiska attribut, såsom kön och utbildningsbakgrund, individernas attityd gentemot användningen av passiv biometrisk autentisering?*".

Analysen av olika demografiska attribut, inklusive kön och utbildningsbakgrund, ger en djupare förståelse för hur dessa faktorer kan påverka människors attityder gentemot passiv biometrisk autentisering även om den inte är representativ för hela gruppen. Enligt resultatet av undersökningen är kön en betydande faktor även om antal deltagare inte är tillräckligt hög för att kunna dra en definitiv slutsats. Kvinnor visar i allmänhet en något lägre benägenhet att lita på passiv biometrisk autentisering för finansiella transaktioner jämfört med män med den begränsade underlag som finns. Denna könsskillnad kan delvis förklaras av olika upplevelser, attityder och risktolerans gentemot teknologiska innovationer och säkerhet men även de sociala normer vilket Kim (2016) påpekar.

Vidare spelar utbildningsbakgrund också en roll. Resultaten indikerar att vissa demografiska grupper med högre utbildningsnivå, som till exempel K2 (en grupp som antas ha en högre grad av utbildning), tenderar att ha större förtroende för passiv biometrisk autentisering. Detta kan bero på att de är mer bekanta med teknologi och har en djupare förståelse för dess funktioner och risker men även beroende på hur det används i det dagliga arbetet.

Överlag var det en väldigt positiv syn på passiv biometri som autentiseringsmetod där användarna brukade detta i någon form idag vare sig det var i form utav en telefon (till störst del Apple och Samsung) men även andra mobila enheter som en Laptop. Just ansiktsigenkänning var den primära autentiserinsgmetoderna som 26/28 respondenterna använde och föredrog vilket påvisar en hög grad förtroende till systemet och teknologi i allmänhet. De traditionella autentiserinsgmetoderna var inte populära bland deltagarna där oro över att någon kommer åt lösenordet eller mönstret som matas in den största faktorn och som då biometrisk autentisering i stort inte har detta problem.

När denna metod testades på den begränsade antal respondenter visar det sig att när det kommer till oron över detta visar det sig att en viss skillnad existerar bland de olika kategorierna medan den gemensamma nämnaren faktiskt är att kvinnorna i varje kategori har en lite högre grad oro än männen i respektive kategori. Detta är dock inte representativt för alla kvinnor men med det tillvägagångssätt som arbetet utförts med, har detta resultat tagits fram och är ett förarbete för framtida forskning kring temat.

7.2 Kompromiss utav integritetsaspekter bland användare

Den andra frågeställningen som besvaras är *"Hur varierar demografiska grupper i sin beredvillighet att kompromissa med integritetsaspekter för att uppnå en förbättrad användarupplevelse och användarvänlighet i samband med passiv biometrisk autentisering?*"

Variationen mellan olika demografiska grupper i deras beredvillighet att kompromissa med integritetsaspekter för en förbättrad användarupplevelse och användarvänlighet i samband med passiv biometrisk autentisering är mångfacetterad. Resultaten tyder på att män, särskilt de i K3, är mer benägna att omfamna passiv biometrisk autentisering för finansiella transaktioner. Denna grupp även om begränsad i antal för denna studie kan vara mer mottaglig för teknologiska innovationer och bekvämligheten med digitala betalningsmetoder.

Å andra sidan kan kvinnor vara mer reserverade när det gäller att använda biometrisk autentisering för finansiella ändamål på grund av oro för säkerhet och integritet. Deras benägenhet att kompromissa med integritetsaspekter för att uppnå en förbättrad användarupplevelse kan vara lägre jämfört med män och andra demografiska grupper.

I båda fallen är det viktigt att beakta dessa variationer i beredvillighet när man utformar autentiseringsmetoder för att säkerställa en balans mellan användarupplevelse, säkerhet och integritet för olika användargrupper. Att ta hänsyn till dessa demografiska faktorer kan bidra till att skapa mer inklusiva och användarcentrerade autentiseringslösningar.

Att integriteten är viktigt är något som inte går obemärkt förbi men samtliga grupper är villiga att kompromissa med att dela med sig av ännu mer biometrisk data för att både effektivisera samt göra den mer korrekt för att minska falska positiva och falska negativa. Männen med högre utbildningsbakgrund har mer fokus på säkerhet som visas i figur 6 än kvinnorna i **K2** samt **K3** men i **K1** är trenden tvärtemot.

Därefter finns en oro bland kvinnorna som i högre utsträckning än männen i respektive kategori för att hanteringen av biometriska datan ska kompromissas. Exempelvis då åsikter som *"att det inte går att byta ut sina biometri*" är åsikter som framförts av kvinnor. Männen generellt sätt har högre förtroende till dessa företag som just hanterar denna teknologi och data men ändå har kvinnorna högre förtroende än männen när det kommer till denna autentiseringsmetod. Ju högre förtroende av användare ju mer data är dessa redo att lämna ifrån sig datan och i detta fall är det kvinnorna oavsett utbildningsbakgrund. Detta är i led med det som Zhaleh Semnani-Azad et al (2019) påpekar att olika dimensioner finns till detta förtroende och att flera olika faktorer spelar roll som individuella upplevelser och åsikter som en användare har och hur olika individer har haft negativa eller mindre positiva upplevelser.

För att ytterligare fördjupa förståelsen för integriteten kan man undersöka de olika aspekterna som användarna anser vara viktiga. Till exempel är möjligheten att kunna radera eller begränsa användningen av sin biometriska data en central oro för många

användare. Detta understryker behovet av användarkontroll över deras egna data för att säkerställa integriteten. Dessutom är säkerheten för biometriska data avgörande för att skydda användarnas integritet mot potentiella angripare. Genom att förstå och adressera användarnas bekymmer kring integritet kan företag och organisationer bygga förtroende för sina autentiseringsmetoder och säkerställa en positiv användarupplevelse.

Vad som sedan presenterades i analysen är att bland annat transparens och säkerhet. Samtliga demografiska attribut som studerats har i det stora hela varit mer benägna att dela med sig av biometrin om man visste mer exakt hur den hanterades och olika protokoll samt att den är säker. Totalt sätt var det männen som ansåg att integriteten var mindre relevant än kvinnorna när man jämför könen sinsemellan där männen som demograf är mer beredvilliga att kompromissa med sin integritet där avläsning av biometri är fokuset för att simplifiera detta än kvinnorna. Kvinnorna är mer benägna att skydda sin personliga data som finns lagrad i sin enhet än vad männen är och att denna data inte missbrukas.

Något att påpeka är att resultatet mot all förmodan inte speglar en hel befolkning eller demografisk grupp. Detta är med stor anledning till den begränsning i deltagare som finns och därav finns underlag hur en mindre grupp reagerar och uppfattar denna teknik men inte något som kan jämföras med en hel grupp.

8 Diskussion

Detta kapitel ska diskutera de olika aspekter kring arbetet och dess fynd för att objektivt framhäva innehållet och dess eventuellt framtida forskning.

8.1 Metoddiskussion

I denna studie valdes både den kvalitativa och kvantitativa metodansatsen med strukturerade intervjuer med likertskalor för att undersöka skillnader bland olika demografiska grupper kring ämnet av passiv biometri som autentiseringsmetod. Valet av denna metod motiverades av behovet av att utforska deltagarnas subjektiva upplevelser av teknologin, vilket krävde både likertskalor för att kunna förstå en bredare syn på en grupp som helhet men även öppna frågor för att kunna få en mer förståelse bakom vissa upplevelser som kan påverka resultatet.

För att säkerställa tillförlitligheten i mina resultat använde jag mig av en noggrant utformad intervjuguide, som utvecklades baserat på tidigare forskning och teorier om biometrisk och traditionella autentiserinsgmetoder samt förståelse om teknologi bland demografiska attribut. Genom att använda en strukturerad intervjuformat var samtliga intervjuer väldigt lika upplagda och med de öppna frågor gav det deltagarna möjlighet att uttrycka sina upplevelser fritt, samtidigt som jag kunde behålla en viss grad av styrning över samtalet för att säkerställa att relevanta teman och frågor täcktes enligt Oppenheim (1992).

En av de främsta utmaningarna jag stötte på under genomförandet av studien var att säkerställa antal deltagare och representativitet i mitt urval. Målet var egentligen att ha runt 50st deltagare för att få ett bredare underlag och mer representativt för de olika demografiska grupperna men brist på intresse blev det inte den mängd som förväntat. Det kan eventuellt ha påverkat resultatet då vissa kategorier endast innehöll 3st individer vilket inte är representativt. Även om målet inte är att få en uppfattning för en hel grupp i samhället var detta mening att få en grund till att förstå om denna metod och tillvägagångssätt är rätt väg att gå framöver.

Jag använde de öppna frågorna för att korsvalidera svaren på de kvantitativa frågorna genom en tvåstegsprocess. Först genomförde jag en tematisk analys av de öppna svaren för att identifiera mönster och teman. Därefter jämförde jag dessa teman med resultaten från de kvantitativa frågorna för att se om de överensstämde eller avvek från varandra. Genom denna metodik kunde jag säkerställa att resultaten från de kvantitativa frågorna stöddes av och var i linje med de kvalitativa svaren, vilket bidrog till en ökad validitet och tillförlitlighet i min analys.

Trots denna utmaningar anser jag att den valda metoden var lämplig för att uppnå syftet med studien och besvara min forskningsfråga. Genom att använda strukturerade intervjuer kunde jag få både en djupare förståelse men även ren statistik för hur de olika upplevelser kring passiv biometri som autentiseringsmetod, vilket ger värdefulla insikter

ge en förståelse för användare och företaget om hur de kan samspela för att kunna göra en effektivare och mer integritetsvänligt system.

För att förbättra studien och säkerställa att den kan generera mer pålitliga och signifikanta resultat, kan studenten vidta flera åtgärder. För det första är det viktigt att öka urvalsstorleken för att minska risken för slumpmässiga variationer och öka tillförlitligheten i resultaten. Detta kan uppnås genom att inkludera fler respondenter eller använda en slumpmässig urvalsmetod för att säkerställa representativitet. Vidare är det avgörande att minimera standardavvikelsen genom noggrann planering och genomförande av studien för att minimera variansen i datainsamlingen och eliminera eventuella felkällor. Användningen av adekvata statistiska metoder är också viktig för att korrekt analysera data och dra relevanta slutsatser baserade på studiens design och variabler av intresse. Slutligen bör urvalsmetoden valideras genom en pilottest eller valideringsstudie för att säkerställa att den är lämplig och genererar tillförlitliga resultat. Genom att genomföra dessa åtgärder kan studenten förbättra studiens metodik och öka dess förmåga att generera signifikanta och tillförlitliga resultat. Det är väsentligt att vara medveten om både de praktiska och teoretiska aspekterna av forskningsdesignen och att använda lämpliga statistiska metoder för att uppnå de önskade forskningsmålen.

För att uppnå en rimlig representativitet i studien av exempelvis kvinnliga befolkningen i Sverige, kan en urvalsstorlek på några tusen respondenter vara en startpunkt. Det är däremot viktigt att komma ihåg att ju större urvalsstorleken är, desto mer tillförlitliga och generaliserbara blir resultaten. Det är dock viktigt att balansera mellan att ha tillräckligt med respondenter för att vara representativ och att ha resurser och tid för att genomföra studien på ett effektivt sätt. Slutligen bör den exakta urvalsstorleken noga övervägas i samband med studiens syfte, forskningsfrågor och tillgängliga resurser (Institute for Work and Health, 2008; Coursera, 2023). Skulle exempelvis studien begränsas till kvinnor i Skövde där studien genomförts kan sampel size minskas markant men ändå behöva vara kring ett tusen deltagare.

8.2 Resultatdiskussion

Att många använder passiv biometri som autentiseringsmetod är inget som förvånar en och specifikt inte ansiktsigenkänning då denna är det som vanligtvis rekommenderas av företagen att använda. Att det ska gå fort, ingen ska kunna se över axeln när man ska öppna telefonen eller komma åt datan om personen som äger telefonen fysiskt inte är där var vanliga teman.

Även om kvinnor är mer oroliga över användningen kring denna teknologi i varje kategori vilket kan beror på att innehållet på telefonen kanske är viktigare av olika skäl som sentimentala anledningar exempelvis.

Bland utbildningsgruppernas kategorier var de högre utbildade deltagarna tillhörande K3 mer benägna att använda denna autentiseringsmetod för att hantera finansiella transaktioner. Detta ansågs vara lite motsägelsefullt då även om oron är hög bland

kvinnor, men även var de villiga att lämna ifrån sig mer data för att göra detta mer användarvänligt men ändå mindre fokus på säkerheten. Detta är något som framtida forskning bör kunna få svar på men inte gjordes i denna studie. Veta varför oron är hög, fokus på säkerhet lägre men ändå villiga att dela med sig av mer data. Detta kan framtida forskning kunna fördjupa sig inom. Varför jag valde att dela upp olika utbildningarna till olika kategorier var för att undvika att ha för lågt deltagande och svar från vissa grupper. Även med denna metod blev grupperna relativt låga men bättre än var för sig. Därav blev grupperna delade i 3 olika kategorier som då kan representera låg, mellan och hög utbildningsbakgrund för att förenkla uttrycket. Sedan för at separera könen tilldelades de också varsin roll som KF och KM.

Något som överraskade var att standardavvikelsen inte alls var stor mellan vissa kategorier men på samma fråga kunde avvikelsen vara mycket höra hos en annan kategori. Exempelvis att förtroendet bland samtliga grupper var ganska koncentrerat vid lika punkter medan männen i K3 hade större differens på skalan. Denna avvikelse kan bero på brist på antal deltagare och vid en större studiegrupp kan detta inte ha lika stor påverkan på resultatet.

Tidigare forskning, som Kim (2016), har påpekat att könsskillnader i attityder till teknologiska innovationer och säkerhet kan bero på olika upplevelser och sociala normer. Resultaten visar dock att kvinnor generellt har en lägre benägenhet att lita på passiv biometrisk autentisering för finansiella transaktioner jämfört med män, även om detta baseras på ett begränsat antal deltagare. Detta nyanserar tidigare forskning genom att specifikt koppla denna skillnad till passiv biometrisk autentisering

En annan viktig observation var att deltagarna uttryckte en hög grad av tillit till passiv biometri som autentiseringsmetod. Trots vissa bekymmer kring integritet och oro framkom det att många såg biometriska faktorer som pålitliga och svårare att manipulera än traditionella autentiseringsmetoder. Denna höga tillit kan vara avgörande för antagandet och användningen av passiv biometri i praktiken och pekar på vikten av att adressera eventuella oro- och förtroendefrågor i framtida implementeringar.

Männen tenderar överlag att fokusera på säkerhet och har en större oro kring detta ämna medan kvinnorna lägger mindre vikt på dessa två faktorer och är mer fokuserade på integriteten av datan. Tidigare studier har fokuserat på användbarhet och acceptansen likt det Venkatesh, Thong and Xu (2012) nämner är det den sociala normen starkare för män att bruka nya teknologier. Detta ses exempelvis att fler män är mer intresserade att bruka passiv biometri vid finansiella transaktioner. Det nämner att männen är intresserade av att experimentera och testa ny teknik. Kvinnorna litar mer på teknologin något Gefen and Straub, (1997) hävdar men enligt den kvantitativa studien är oron högre. Detta betyder nödvändigtvis inte att kvinnorna litar mindre på teknologin men att andra orsaker har en påverkan. Detta är något som vid en större studie möjligtvis ska inkludera och söka efter flera orsaker till denna oro.

Framtida studier bör också undersöka hur olika demografiska grupper är villiga att kompromissa med integritet för att uppnå förbättrad användarupplevelse. Detta kan inkludera experimentella designstudier som manipulerar olika nivåer av transparens och säkerhetsåtgärder för att se hur dessa påverkar användarnas vilja att kompromissa med integriteten. Slutligen kan longitudinella studier undersöka hur långvarig användning av biometrisk autentisering påverkar användares attityder och förtroende över tid. Detta kan inkludera att följa användare över flera år för att se om och hur deras förtroende för teknologin förändras.

Resultatet är begränsad av antalet deltagare och speglar inte befolkningen i helhet. Resultatet visar att metoden som brukats fungerar för att få fram den data som behövs för att kunna göra en studie men denna studie och all resultat är inte representativ utan har gett en liten inblick hur olika grupper tänker och vad deras åsikter kring tekniken är.

Genom att fokusera på dessa specifika forskningsområden kan framtida studier bygga vidare på de insikter som studien har bidragit med och ytterligare fördjupa förståelsen för hur passiv biometrisk autentisering uppfattas och används av olika demografiska grupper. Detta bidrar inte bara till att validera de egna resultat, utan också till att vägleda framtida forskning i rätt riktning och utveckla mer inkluderande och användarcentrerade autentiseringslösningar.

Vidare bör ytterligare forskning fokusera på hur olika nivåer och typer av utbildning påverkar acceptansen av biometrisk autentisering. Specifika studier kan undersöka hur utbildningsprogram inom teknologi och säkerhet påverkar attityder och beteenden över tid. Det behövs också mer forskning kring hur användare upplever kontroll över sin biometriska data. Studier kan inkludera utveckling och testning av användargränssnitt som ger användare bättre kontroll och insikt i hur deras biometriska data hanteras, samt hur detta påverkar deras förtroende och vilja att dela data.

När det kommer till integritet och säkerhet är etiken och dess aspekter viktiga. Att följa de etiska aspekterna som Vetenskapsrådet (2018) rekommenderar har varit grunden till studien för att försäkra om deltagarnas säkerhet och integritet. Information om rättigheter och medverkan har tryggat deltagarna i sin medverkan i studien. Samtliga deltagare är och kommer förbli anonyma men där kön och utbildningsbakgrund har skrivits ut för att kunna publicera de fynd och analyser som gjorts under studiens gång.

Samtliga intervjuer har hållit tidsramen och ingen har valt att avbryta sitt deltagande och inga otydligheter framkom då detta hanterades vid de två testintervjuer som skedde innan resterande 28 intervjuer gjorts. Efter varje intervju har deltagarna fått gå igenom sina svar för att inga missförstånd ska ske eller eventuella förändringar i svar som deltagaren vill göra där båda parterna lämnar intervjun nöjda med de svar som givits och tagits emot.

Den data som samlats in under intervjuerna ska och får endast användas till denna studie och den rådata som samlats in kommer att raderas och ej kunna brukas för framtida bruk när arbetet är klart och godkänt.

8.3 Olika aspekter att beakta

8.3.1 Vetenskapliga aspekter

Individernas säkerhet och integritet bör fortsättningsvis prioriteras när det kommer till passiv biometrisk autentisering. Då detta verkar bli allt mer vanligt kan detta ämne bli ännu mer relevant. Den forskning fokuserar på en begränsad grupp individer och dess demografiska bakgrund. Men en hårfin linje måste beaktas då oron som bland respondenterna och speciellt kvinnor i högre grad finns där och om säkerheten och transparensen inte är något som erbjuds av dessa företag kan det istället för att flera använder detta ha en mer avskräckande effekt i framtiden, även om allt fler är villiga att dela med sig av sin data för att effektivisera och skynda på processen.

I framtiden bör en större grupp individer intervjuas där flera attribut inkluderas för att kunna söka efter mönster som är positiva och/eller negativa bland demografiska grupper för att kunna göra denna funktion mer användarvänlig med respekt utav integritet. Frågorna till intervjuerna kunde ha utvecklats mer i form utav flera frågor i båda kategorier (poängfrågor samt de öppna frågorna) för att få mer data att analysera och få mer relevant information. Vissa frågor som ställdes var inte helt väsentliga för denna studie och kan bytas ut till mer relevanta frågor om just integritet och villigheten att lämna ifrån mer biometrisk data.

8.3.2 Etiska aspekter

En av de mest betydande etiska riskerna med passiv biometrisk autentisering är möjligheten för missbruk av biometrisk data. Biometri, till exempel ansiktsigenkänning, kan användas på fel sätt av både företag och myndigheter, vilket kan leda till allvarliga konsekvenser för individers integritet och säkerhet. Eftersom biometrisk data är unik och oföränderlig, till skillnad från lösenord som kan ändras, är risken stor att sådan data, om den hamnar i orätta händer, kan användas för att permanent kompromettera en individs identitet.

Med resultaten från min forskning framkommer att användare tenderar att ha högt förtroende för teknikföretag som hanterar biometrisk autentisering. Detta förtroende, även om det är positivt för teknologins adoption, innebär också en stor risk. Om användare blint litar på dessa företag utan att förstå de potentiella säkerhets- och integritetsriskerna, kan de bli sårbara för dataintrång och missbruk av deras biometriska information. Till exempel kan företag använda den insamlade biometriska datan för övervakning eller sälja den till tredje parter utan användarnas samtycke.

En annan etisk risk är att biometrisk data kan användas för diskriminering eller profilering. Teknologi för ansiktsigenkänning har redan kritiserats för att ha högre

felmarginaler för personer av vissa etniska bakgrunder eller för kvinnor jämfört med män. Detta kan leda till ojämlik behandling och stärka befintliga sociala orättvisor.

Resultaten visar också att kvinnor är mer oroliga över integritets- och säkerhetsaspekterna jämfört med män. Detta kan tyda på en bristande förtroende för hur deras data hanteras och en rädsla för att deras information kan missbrukas. Denna oro är välgrundad, eftersom kvinnor historiskt sett har varit mer utsatta för olika former av digitala kränkningar och trakasserier.

För att hantera dessa etiska risker bör framtida forskning och utveckling av passiv biometrisk autentisering inkludera starka säkerhetsåtgärder och transparenta policys om hur data samlas in, lagras och används. Det är också viktigt att utveckla mekanismer för att ge användare mer kontroll över sin biometriska data, inklusive möjligheten att radera eller begränsa användningen av deras information.

Sammanfattningsvis, medan passiv biometrisk autentisering erbjuder stora fördelar för användarvänlighet och säkerhet, medför den också betydande etiska risker. Dessa risker inkluderar missbruk av biometrisk data, överdriven tillit till teknikföretag, potentiell diskriminering och bristande integritetsskydd. För att minimera dessa risker krävs en noggrann balansering av teknologins fördelar med robusta etiska överväganden och användarskydd.

8.3.3 Samhälleliga aspekter

Jag tror att min forskning om passiv biometrisk autentisering kan bidra till att skapa säkrare och mer användarvänliga autentiseringslösningar. Teknikbolag kan använda mina resultat för att anpassa sina produkter och strategier efter olika användargrupper, medan myndigheter kan använda insikterna för att utveckla regleringar som säkerställer en etisk hantering av biometrisk data. För medborgare kan min forskning öka medvetenheten om riskerna och fördelarna med biometrisk autentisering och inspirera till att kräva bättre integritetsskydd och datakontroll. Sammantaget tror jag att min forskning har potential att göra betydande samhällsbidrag genom att förbättra teknologiska lösningar och öka medvetenheten om digital säkerhet och integritet. Jag är övertygad om att detta kan leda till en tryggare och mer ansvarsfull användning av biometriska autentiseringsmetoder i samhället. Detta kan dock endast ske ifall en mer omfattande studie görs.

9 Referenser

Abed, M.E., Giot, R., Hemery, B. and Rosenberger, C. (2012). Evaluation of biometric systems: a study of users' acceptance and satisfaction. International Journal of Biometrics, 4(3), p.265. doi: https://doi.org/10.1504/ijbm.2012.047644.

Akhtar, Z., Michelon, C. and Gian Luca Foresti (2014). Liveness detection for biometric authentication in mobile applications. International Carnahan Conference on Security Technology. doi: https://doi.org/10.1109/ccst.2014.6986982.

Anil, A., Flynn, P., Ross, A.A. and Springerlink (Online Service (2008). Handbook of Biometrics. Editorial: New York, Ny: Springer Us.

Bryman, A. (2018). Samhällsvetenskapliga metoder. 3rd ed. Stockholm: Liber.

Chaudhari, A., Pawar, A., Pawar, A., Pawar, A. and Pawar, G. (2023). A Comprehensive Study on Authentication Systems. doi: https://doi.org/10.1109/iccubea58933.2023.10392029.

Chopra, A. (2019). Analysis of Biometric Systems in Mobile devices. [online] Semantic Scholar. www.ijlemr.com. 4(6) pp.132-137.
Available at: https://www.semanticscholar.org/paper/Analysis-of-Biometric-Systems-in-Mobile-devices-Chopra/1ef4bddab554170445fa17ddd41df43535200f34.
[Accessed 13 Feb. 2024].

Clancy, R.F. (2021). The Merits of Social Credit Rating in China? An Exercise in Interpretive Pros Hen Ethical Pluralism. Journal of Contemporary Eastern Asia, [online] 20(1), pp.102–119. Doi: https://doi.org/10.17477/jcea.2021.20.1.102.

Coursera (2023). What is sample size? [online] Coursera. Available at: https://www.coursera.org/articles/what-is-sample-size.

Dargan, S. and Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143, p.113114. doi: https://doi.org/10.1016/j.eswa.2019.113114.

Di Wen, Hu Han and Jain, A.K. (2015). Face Spoof Detection with Image Distortion Analysis. IEEE Transactions on Information Forensics and Security, 10(4), pp.746–761. doi: https://doi.org/10.1109/tifs.2015.2400395.

Gefen, D. and Straub, D.W. (1997). Gender Differences in the Perception and Use of E-Mail: An Extension to the Technology Acceptance Model. MIS Quarterly, 21(4), p.389. doi: https://doi.org/10.2307/249720.

Inkster, N. (2016). China's cyber power. Abingdon: Routledge; London.

Institute for Work and Health (2008). Sample size and power. [online] www.iwh.on.ca. Available at: https://www.iwh.on.ca/what-researchers-mean-by/sample-size-and-power#:~:text=Sample%20size%20refers%20to%20the.

Kim, J. (Sunny) (2016). An extended technology acceptance model in behavioral intention toward hotel tablet apps with moderating effects of gender and age. International Journal of Contemporary Hospitality Management, 28(8), pp.1535–1553. doi: https://doi.org/10.1108/ijchm-06-2015-0289.

Li, F., Clarke, N., Papadaki, M. and Dowland, P. (2013). Active authentication for mobile devices utilising behaviour profiling. International Journal of Information Security, 13(3), pp.229–244. doi: https://doi.org/10.1007/s10207-013-0209-6.

Liang, F., Das, V., Kostyuk, N. and Hussain, M.M. (2018). Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. Policy & Internet, 10(4), pp.415–453. doi: https://doi.org/10.1002/poi3.183.

Lyu, S. (2020). Deepfake Detection: Current Challenges and Next Steps. [online] IEEE Xplore. doi: https://doi.org/10.1109/ICMEW46912.2020.9105991.

Mamonov, S. and Benbunan-Fich, R. (2015). An empirical investigation of privacy breach perceptions among smartphone application users. Computers in Human Behavior, 49, pp.427–436. doi: https://doi.org/10.1016/j.chb.2015.03.019.

Meng, W., Wong, D.S., Furnell, S. and Zhou, J. (2015). Surveying the Development of Biometric User Authentication on Mobile Phones. IEEE Communications Surveys & Tutorials, 17(3), pp.1268–1293.doi: https://doi.org/10.1109/comst.2014.2386915.

Mo, Y. and Sinopoli, B. (2009). Secure control against replay attacks. [online] IEEE Xplore. Doi: https://doi.org/10.1109/ALLERTON.2009.5394956.

Nandhini Anbalagan, Abbas, A., Hameed, A. and Jamal, A. (2020). Trusted Application Using Biometrics for Android Environment. doi: https://doi.org/10.1109/cspa48992.2020.9068715.

Oppenheim, A.N. (1992). Questionnaire Design, Interviewing and Attitude Measurement. London.

Patel, V.M., Ratha, N.K. and Chellappa, R. (2015). Cancelable Biometrics: A review. IEEE Signal Processing Magazine, 32(5), pp.54–65. doi: https://doi.org/10.1109/msp.2015.2434151.

Ratjeana Malatji, W., van Eck, R. and Zuva, T. (2020). Acceptance of Biometric Authentication Security Technology on Mobile Devices. 2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC). doi: https://doi.org/10.1109/imitec50163.2020.9334082.

Riley, C., Buckner, K., Johnson, G. and Benyon, D. (2009). Culture & biometrics: regional differences in the perception of biometric authentication technologies. AI & SOCIETY, 24(3), pp.295–306. doi: https://doi.org/10.1007/s00146-009-0218-1.

Rui, Z. and Yan, Z. (2019). A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. IEEE Access, 7, pp.5994–6009. doi: https://doi.org/10.1109/access.2018.2889996.

Savvides, M., Kumar, V. and Khosla, P.K. (2004). Cancelable biometric filters for face recognition. International Conference on Pattern Recognition. Doi: https://doi.org/10.1109/icpr.2004.1334679.

Smith, M. and Miller, S. (2021). The Future of Biometrics and Liberal Democracy. Biometric Identification, Law and Ethics, pp.79–95. doi: https://doi.org/10.1007/978-3-030-90256-8_5.

Shukla, R. and Kaur, H. (2023). Deep learning based cancelable biometric system. doi: https://doi.org/10.1109/icccnt56998.2023.10307990.

Srite, M. and Karahanna, E. (2006). The Role of Espoused National Cultural Values in Technology Acceptance. MIS Quarterly, 30(3), p.679. doi: https://doi.org/10.2307/25148745.

Venkatesh, V., Thong, J.Y.L. and Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), pp.157–178. doi: https://doi.org/10.2307/41410412.

Vetenskapsrådet (2018). Etik i forskningen. [online] www.vr.se. Available at: https://www.vr.se/uppdrag/etik/etik-i-forskningen.html.

Vinogradov, A. (2023). Social Credit System in China. Problemy Dal'nego Vostoka, (3), pp.125–125. doi: https://doi.org/10.31857/s013128120026254-0.

Wang, X., Yu, T., Mengshoel, O.J. and Tague, P. (2017). Towards continuous and passive authentication across mobile devices. doi: https://doi.org/10.1145/3098243.3098244.

Watt, E. (2017). 'The right to privacy and the future of mass surveillance'. The International Journal of Human Rights, 21(7), pp.773–799. doi: https://doi.org/10.1080/13642987.2017.1298091.

Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review, [online] 9(11), pp.39–52. doi: https://doi.org/10.22215/timreview/1282.

Wu, Z., Evans, N., Kinnunen, T., Yamagishi, J., Alegre, F. and Li, H. (2015). Spoofing and countermeasures for speaker verification: A survey. Speech Communication, [online] 66, pp.130–153. doi: https://doi.org/10.1016/j.specom.2014.10.005.

Xu, H., Zhou, Y. and Lyu, M.R. (2014). Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones. pp.187–198.

Yang, X., Li, Y. and Lyu, S. (2019). Exposing Deep Fakes Using Inconsistent Head Poses. ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). doi: https://doi.org/10.1109/icassp.2019.8683164.

Zhaleh Semnani-Azad, Chien, S.-Y., Forster, Y., Schuckers, S. and Gan, H. (2019). Development of Trust Measure in Biometric Technology. doi: https://doi.org/10.24251/hicss.2019.699.

Zhang, X. and Gao, Y. (2009). Face recognition across pose: A review. Pattern Recognition, 42(11), pp.2876–2896. doi: https://doi.org/10.1016/j.patcog.2009.04.017.

Bilaga

Bilaga 1 - Intervjumall

Intro till intervju;
Innan vi påbörjar vår intervju, låt mig ge en snabb förklaring av begreppen passiv och aktiv biometri. Tänk på biometri som ett sätt att använda unika kännetecken för att identifiera och autentisera en perso**n.**

Passiv biometri:
Passiv biometri är som att ha en hemlig vän som känner dig så väl att de kan känna igen dig bara genom hur du rör dig eller pratar. I teknikens värld innebär passiv biometri att systemet lär sig känna igen dig genom att ständigt observera och analysera ditt naturliga beteende, som hur du använder din telefon eller hur ditt ansikte ser ut.

Aktiv biometri:
Å andra sidan är aktiv biometri lite som att du visar ID-kortet när du går in på en nattklubb. Du måste medvetet ge systemet något, som ditt fingeravtryck, göra en aktiv rörelse med ansiktet eller säga en specifik fras för att bekräfta att du verkligen är den du säger att du är. Aktiv biometri kräver din delaktighet för att autentisera dig själv.
Så, i grund och botten, passiv biometri handlar om att systemet lär känna dig över tid, medan aktiv biometri handlar om att du aktivt deltar i autentiseringsprocessen genom att ge systemet något unikt.
Att exempelvis skapa ett Face ID på en Apple enhet är en form av aktiv biometri men att själva autentiseringen i det senare skedet är passiv då användaren ej behöver utföra någon handling utan denna sker som en naturliga interaktionen mellan användaren och enheten utan behov av specifika användarinitierade handlingar för autentisering.

Kön:

Utbildningsbakgrund:

Frågeställning 1:

Har du tidigare använt passiv biometrisk autentisering för att låsa upp en enhet, till exempel en smartphone? Ja/Nej

Om ja, Nämn gärna vilka enheter

Hur tror du att dina personliga upplevelser och perspektiv kan påverka din syn på användningen av passiv biometrisk autentisering? 1 = låg och 7 = hög

Hur skulle du bedöma din upplevelse av hur företag behandlar din biometriska data med fokus på integritet? 1 = låg och 7 = hög

Följd fråga: Något speciellt som du tänker på när du besvarade tidigare fråga.

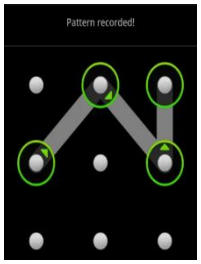
Hur betydelsefull anser du integriteten vara vid användning av biometriska autentisering teknologier? 1 = låg och 7 = hög

Följd fråga: För att fördjupa oss i ditt svar, kan du beskriva några specifika aspekter av integritet som du anser vara särskilt viktiga eller mindre viktiga i detta sammanhang?

Påverkas din personliga attityd gentemot passiv biometrisk autentisering avsevärt om det implementeras mer omfattande i samhället?" 1 = låg och 7 = hög

Tycker du att passiv biometrisk autentisering är mer praktisk än traditionella autentiseringsmetoder som lösenord? 1 = låg och 7 = hög

Vilken autentiseringsmetod föredrar du? : Visa bild




Hur skulle du påstå att din kunskap var kring ämnet aktiv biometri som autentiseringsmetod och passiv biometri innan intervjun? 1 =låg och 7 = hög

Hur mycket förtroende har du för passiv biometrisk autentisering som en säkerhetsmetod? 1 =låg och 7 = hög

Tror du att passiv biometrisk autentisering är mer eller mindre integritets vänligt än andra autentiseringsmetoder såsom lösenord/pin kod? 1 = mindre och 7 = högre

Kan du dela med dig av några positiva upplevelser du har haft med autentiserings teknologier och vilka specifika aspekter gjorde dem positiva för dig? Frisvar:

Hur ofta har du upplevt negativa situationer eller utmaningar i samband med passiv biometrisk autentisering? 1 = sällan och 7 = ofta

Följd Fråga: Om hög, vänligen beskriv dem och hur de påverkade din användarupplevelse

Vilken autentiseringstyp föredrar du vanligtvis och varför? Finns det några specifika

Känner du någonsin oro eller tvekan kring användningen av vissa autentiserings teknologier? Ja/Nej

Följd fråga: Om ja, Vad var det som väckte dessa känslor .

Frågeställning 2:

Upplever du olika bekymmer kring integritet vid brukande av passiv biometrisk autentisering. 1 = låg och 7 = hög

Hur tror du att dina olika livserfarenheter kan påverka dina attityder och eventuella bekymmer gällande integriteten vid användning av passiv biometrisk autentisering? 1 = låg och 7 = hög

Har du någonsin känt dig orolig över att använda passiv biometrisk autentisering på grund av integritets bekymmer? 1 = låg och 7 = hög

Följd Fråga: Ge gärna exempel på dessa?

Har du någonsin diskuterat integritetsaspekterna av passiv biometrisk autentisering med andra personer? Ja/Nej

Följd Fråga: Om ja, Är det vänner, kollegor osv?

Hur viktig anser du integritet vara när det gäller autentisering teknologier? 1 = låg och 7 = hög

Hur mycket oro känner du när det gäller integriteten vid användning av passiv biometrisk autentisering? 1 = låg och 7 = hög

Hur bekväm skulle du vara med att använda passiv biometrisk autentisering för att godkänna finansiella transaktioner? 1 = låg och 7 = hög

Hur bekväm känner du dig överlag med användningen av passiv biometrisk autentisering? 1 = låg och 7 = hög

Är du orolig över hur din biometriska data används? 1 = låg och 7 = hög

Varför är säkerheten viktigt för dig? Frisvar:

Finns det något som oroar dig med passiv biometrisk autentisering? Frisvar:

Är du villig att lämna ifrån mer biometrisk data till din enhet för att öka autentiseringsprocessens korrekthet vid autentisering. 1 = låg och 7 = hög

Är du villig att lämna ifrån mer biometrisk data till din enhet för att autentiseringsprocessens ska bli snabbare. 1 = låg och 7 = hög

Hur mån är du över din biometriska data. 1 = låg och 7 = hög

Kontrollfrågor:

Hur viktigt anser du att digital säkerhet är i ditt dagliga liv? 1 = låg och 7 = hög

Hur mycket oroad är du över säkerheten när det gäller användningen av biometriska autentiseringsmetoder? 1 = låg och 7 = hög

Hur positiv är du till användningen av biometrisk autentisering som en metod för att säkra dina digitala enheter? 1 = låg och 7 = hög

Hur väl är du informerad om hur biometriska autentiseringssystem fungerar? 1 = låg och 7 = hög

Hur mycket förtroende har du för biometriska autentiseringsmetoder när det gäller att skydda dina personliga uppgifter? 1 = låg och 7 = hög

Bilaga 2 – Respondenter

Respondent	**Kön**	**Utbildningsbakgrund**
R1	Man	Gymnasial
R2	Man	Gymnasial
R3	Kvinna	Kandidat
R4	Man	Gymnasial
R5	Kvinna	Gymnasial
R6	Kvinna	Kandidat
R7	Man	Gymnasial
R8	Kvinna	Master
R9	Kvinna	Yrkesutbildning
R10	Kvinna	Gymnasial
R11	Kvinna	Kandidat
R12	Kvinna	Grundskola
R13	Man	Kandidat
R14	Man	Kandidat
R15	Man	Gymnasial
R16	Kvinna	Kandidat
R17	Man	Gymnasial
R18	Kvinna	Kandidat
R19	Kvinna	Gymnasial
R20	Man	Grundskola
R21	Man	Yrkesutbildning
R22	Kvinna	Folkhögskola
R23	Man	Yrkesutbildning
R24	Man	Yrkesutbildning
R25	Kvinna	Gymnasial
R26	Man	Gymnasial
R27	Man	Kandidat
R28	Kvinna	Folkhögskola