LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Säkerhet gällande autonoma fordon i trafiken

En kvalitativ studie om säkerhet inom IoV, Vehicle Cloud och AI

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Susanna Nirvald
Fanny Tapper

Handledare: Miranda Kajtazi

Examinatorer: Anders Svensson
Umberto Fiaccadori

Säkerhet gällande autonoma fordon i trafiken: En kvalitativ studie om säkerhet inom IoV, Vehicle Cloud och AI

FÖRFATTARE: Susanna Nirvald och Fanny Tapper

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

FRAMLAGD: maj, 2018

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 70

NYCKELORD: Autonoma fordon, Säkerhet, Internet of Vehicles, Vehicle Cloud och Artificiell Intelligens

SAMMANFATTNING (MAX. 200 ORD):
Dagens samhälle blir mer och mer automatiserat, allt från smarta kök till autonoma bilar. Olyckor med autonoma fordon har inträffat den senaste tiden och skapat orosmoment gällande dess säkerhet. Då dessa fordon kommer spela en stor roll i vår vardag, ställer det stora krav på deras säkerhetsnivå. Denna studie undersöker vilka säkerhetsproblem som finns med autonoma fordon i dagsläget. Samt vilka åtgärder anser organisationsrepresentanter bör tas för att stärka säkerheten med autonoma fordon i trafiken. Områden som Internet of Vehicles, Vehicle Cloud och dess koppling till säkerhet samt grundläggande teorier inom artificiell intelligens undersöks. Kvalitativa intervjuer med individer som har betydande kunskap inom området har genomförts. Det visar sig att det finns säkerhetsrisker idag och lösningar till vissa av dem. Ett problemområde kommer att röra hackning då det kommer ske utan kännedom. Vi måste förstå hur den tredje parten agerar för att kunna förhindra eventuella attacker. Genom att införa gemensamma standarder och lagar gällande säkerhet för autonoma fordon kan några av dessa problem lösas samt styrka acceptansen hos användaren. Områdets utveckling sker snabbt, dock är det en lång väg kvar innan de autonoma fordonen kan köra säkert i vårt samhälle.

Innehåll

Figurer

Tabeller

1 Introduktion

I introduktionskapitlet presenteras uppsatsens bakgrund. Därefter ges problemområde som leder till forskningsfråga, syfte och avgränsningar.

1.1 Bakgrund

"*The Internet has become a minefield of crime, fakes, and terror perpetuated by anonymous users on a global scale.* " (Lee, 2015-2016).

Bright ICT initiativet föreslogs först i en MISQ konferens med många deltagande Informationssystems (IS) forskare (Lee, 2015-2016). Där diskuterades utvecklingen av den nya och kritiska infrastrukturen för Bright ICT initiativet (Lee, 2015-2016). Detta består av införandet av fyra säkerhetsprinciper för the Bright Internet Protocol som bör appliceras för att göra säkerheten bättre: *Origin Responsibility, Deliverer Responsibility, Rule-Based Digital Search Warrants* och *Traceable Anonymity* (Lee, 2015-2016).

Under den senaste tiden har flertalet olyckor skapat stora rubriker världen över om ämnet självkörande fordon. I Arizona i USA blev en kvinna påkörd av en självkörande Uber-bil och omkom (Elbied Pettersson, 2018). Efter händelsen stoppade Uber alla tester av självkörande bilarna i Nordamerika. Bara några dagar senare inträffade en ny olycka i Kalifornien i USA där föraren omkom efter att autopiloten startats och därefter kört in i mitträcket (Holmberg, 2018). Det har också inträffat olyckor där de självkörande bilarna blivit påkörda bakifrån på grund av att de kört för korrekt t.ex. de kör aldrig för fort och stannar alltid vid stoppskyltar (Kvandal, 2017). För några år sedan lyckades hackare ta sig in i systemet på en Jeep och gjorde så att bilen kraschade ner i ett dike efter att ha tagit kontroll över motorn och bromsarna (Gibbs, 2015).

I en studie av Crossler och Poesy (2017) föreslås möjligheten att rikta attacker mot personregister, potentiell misshantering av verifierade uppgifter av miljontals användare samt övervakning av verksamheten kan även den bli privata säkerhetsproblem. Vilket i sin tur kan kopplas till det ovanstående Jeep incidenten.

"You can hack baby monitors and refrigerators, fire detectors and light switches largely because the underlying software of some of these devices is left completely unprotected." (Dreyfuss, 2017).

Dagens samhälle blir mer och mer automatiserat, allt från smarta köksredskap till bilar som är kopplade med Internet of Things (Dreyfuss, 2017). Självkörande bilar har varit ett omtalat ämne de senaste åren och nu är det även dags för Sverige att införa tester av dessa (Rabe, 2016). Google i USA har använt sig av självkörande bilar i några år vilket gör att de ligger i framkanten före Europa (Brohult, 2018).

Då är frågan hur säkra de är: Finns det risk att andra tar sig in i systemet och börjar styra fordonet? Dessvärre finns det en del terror i vårt samhälle. Hade de kunnat använda sig av ett autonomt fordon för att utföra en attack som Stockholmsattacken vid Åhléns? Än så länge har inte en terrorattack av detta slag inträffat, däremot finns möjligheten att detta inträffar om inte bilföretag ständigt arbetar med säkerheten för självkörande fordon. Hur arbetar företagen för att säkerställa att denna information är säker?

Denna studie ämnar att utmana de ovanstående aspekterna med tanke på att sådana utmaningar uppstår och något måste göras för att följa upp dem. Säkerhetsfrågor hos autonoma system blir avgörande. Därför definierar följande avsnitt problemområden och relaterade frågor som denna studie lyfter fram.

1.2 Problemområde

Att arbeta för ett säkert informationsflöde mellan fordonen och molninfrastrukturen är viktigt. Då infrastrukturen för kommunikationen mellan autonoma fordon inte är helt färdigbyggd skapas svårigheter med dess säkerhet. Van der Meulen och Rivera (2015) skriver i en artikel i Gartner att vid 2020 kommer det finnas 250 miljoner uppkopplade bilar genom Internet of Vehicles. Företag måste ständigt hålla sig uppdaterade samt utveckla sina produkter kontinuerligt för att ligga steget före framtida säkerhetsrisker. Några av de säkerhetsrisker från eventuella angripare som finns i dagsläget är förfalskning, trafikstockning, imitation (Raya et al., 2006). Även virus, falska meddelanden, maskering av fordon nämns i artikeln *Social Internet of Vehicles for Smart Cities* (Maglaras et.al., 2016).

I Sveriges Television, Vetenskapens Värld togs diskussionen gällande smarta bilar i våra städer och vardag upp (Brohult, 2018). Det diskuterades allt mellan lagar, säkerhet och påverkan på oss människor (Brohult, 2018). Flera bilföretag har gått ut med att de kommer lansera nivå 5 av autonoma bilar inom de närmaste åren. Teslas VD Elon Musk nämner att de redan 2019 kommer kunna starta produktionen av nivå 5 bilar (Andersson, 2018). Volvo däremot siktar istället in sig på att lansera bilar av nivå 4 vid 2021 (Rabe, 2017). Skalan baseras på fordonets nivå av självkörning t.ex. nivå 2 innebär att bilen kan ta över vissa situationer och nivå 5 kommer vara helt självkörande utan någon mänsklig styrfunktion (Rabe, 2017). Jonas Nilsson från Zenuity, ett företag som grundades av Volvo och Autoliv som arbetar med att förse bilar med intelligens, berättar till Svenska Dagbladet att det finns mycket kvar att arbeta med. Han nämner följande:

> *"Än så länge finns inga autonoma bilar som är lika säkra som manuellt styrda bilar – framförallt inte i komplexa trafiksituationer. "* (Sundberg, 2018)

Denna studie problematiserar området kring Internet of Vehicles, då dess sensorer kommer styra majoriteten av vår framtida trafik. Studien problematiserar ytterligare aspekter genom att fokusera på hur informationsflödet från fordon till Cloud görs säkert så att ingen tredje part kan ta sig in.

1.3 Forskningsfråga

Studiens huvudfråga är, vilka säkerhetsproblem finns det med autonoma fordon i dagsläget?

För att svara på ovanstående fråga, vilken i sin natur generellt hanterar säkerhetsaspekter med autonoma fordon, anser vi att följande underfråga också behöver lösas för att kunna förstå problemet med säkerhet i dagens kontext med autonoma fordon.

Således, vilka åtgärder anser organisationsrepresentanter bör tas för att stärka säkerheten med autonoma fordon i trafiken?

1.4 Syfte

Studien ämnar att undersöka hur Internet of Vehicles, Vehicle Cloud och autonoma fordon idag samverkar för att göra trafiken säker. Den avser också att lyfta fram säkerhetsproblem som finns med autonoma fordon idag. Studien undersöker även lämpade säkerhetsteorier och om dessa appliceras i dagens industri. Den ämnar även att ta fram vilka åtgärder organisationsrepresentanter anser kunna stärka säkerheten i trafiken med autonoma fordon.

För att genomföra studien kommer relevanta individer inom områdena intervjuas för att bidra till ökat underlag till diskussionen kring hur arbetet för säkerhet av autonoma fordon ser ut i dagsläget.

1.5 Avgränsningar

Studiens ändamål avgränsar sig till att inte undersöka området beslutsstödsystem. Ämnena moral/etik kommer inte heller undersökas i denna studie. Studien kommer främst undersöka begreppet Internet of Vehicles och inte gå in djupare på det mer generella begreppet Internet of Things. Trots användning av artificiell intelligens (AI)-teorier, fokuserar inte studien på fordonens funktionalitet från ett AI-perspektiv. AI behandlas i studien för att det är en väsentlig funktion i ett autonomt fordon.

2 Litteraturgenomgång

Litteraturgenomgången kommer behandla den grundläggande kunskapen för studiens forskningsfråga. Kapitlet inleds med beskrivning av aspekter som behövs för att autonoma fordon ska fungera. Därefter behandlas grundläggande säkerhetsaspekter samt teorier inom artificiell intelligens, litteraturgenomgången sammanfattas i slutet i en undersökningsmodell. Litteraturgenomgången används för att skapa intervjuguiden i nästkommande kapitel.

2.1 Teknik

2.1.1 Internet of Vehicles

Internet of Things (IoT) består av både produkter och tjänster och kan appliceras på många olika områden (Fluchter och Wortmann, 2015). Några av områdena är smarta hem, säkerhetssystem och smart transport (Fluchter och Wortmann, 2015). Konceptet för Internet of Vehicles (IoV) är att fordon och objekt från transportinfrastrukturen som är sammankopplade genom IP-baserad infrastruktur enkelt kan utbyta information direkt eller indirekt (Dimitrakopoulos, 2011). Denna information kan lösa olika typer av problem som resulterar i en mer effektiv, säker och grönare värld inom transport (Dimitrakopoulos, 2011). IoV är tänkt att skapa värde för de trådlösa nätverken och användaren (Dimitrakopoulos, 2011). Det finns några skillnader mellan IoT och IoV (Yang, F., Wang, S., Li, J., Liu, Z. och Sun, Q, 2014). Den första skillnaden är att i trådlösa mobilnät följer många av slutanvändarnas mönster en viss modell, till skillnad från i IoV där fordonets bana är föremål för vägfördelningar i staden (Yang et al., 2014). För det andra fokuserar IoT på föremål som ger information om medvetenhet för anslutna saker och Internet ger information och tjänster till människor (Yang et al., 2014). IoV fokuserar istället på integrationen av människor och fordon (Yang et al., 2014). Genom att ansluta fordonet till ett globalt nätverk kan tjänster levereras till andra fordon och människor ombord eller runt fordonet (Yang et al., 2014).

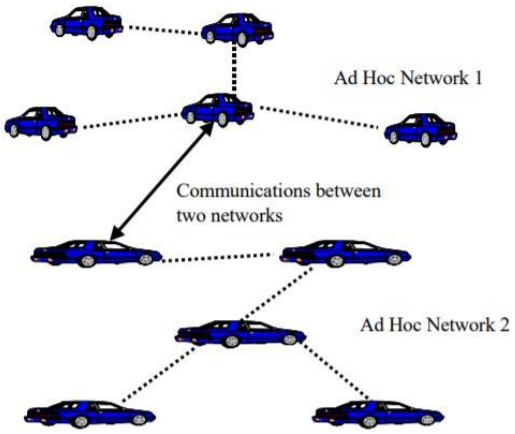
Internet of Vehicles har två olika tekniska inriktningar, *vehicles' networking* och *vehicles' intelligentialize* (Yang et al., 2014). Vehicles networking består utav Vehicular Adhoc Networks (VANET), Vehicle Telematics och Mobile Internet medan vehicles intelligence är integrationen av föraren och fordonet som en enhet med hjälp av t.ex. kognitiv databehandling och artificiell intelligens (Yang et al., 2014). IoV fokuserar på att knyta samman människor, fordon, saker och miljöer till ett öppet och integrerat nätverkssystem som har en hög hanterbarhet och består av flera användare, fordon och nätverk (Yang et al., 2014).

IoV är utvecklat från VANETs och dess vision är:

"from smartphone to smartcar"
(Kaiwartya, O., Hanan Abdullah, A., Cao, Y., Altameem, A., Prasad, M., Lin, C. och Liu, X, 2016).

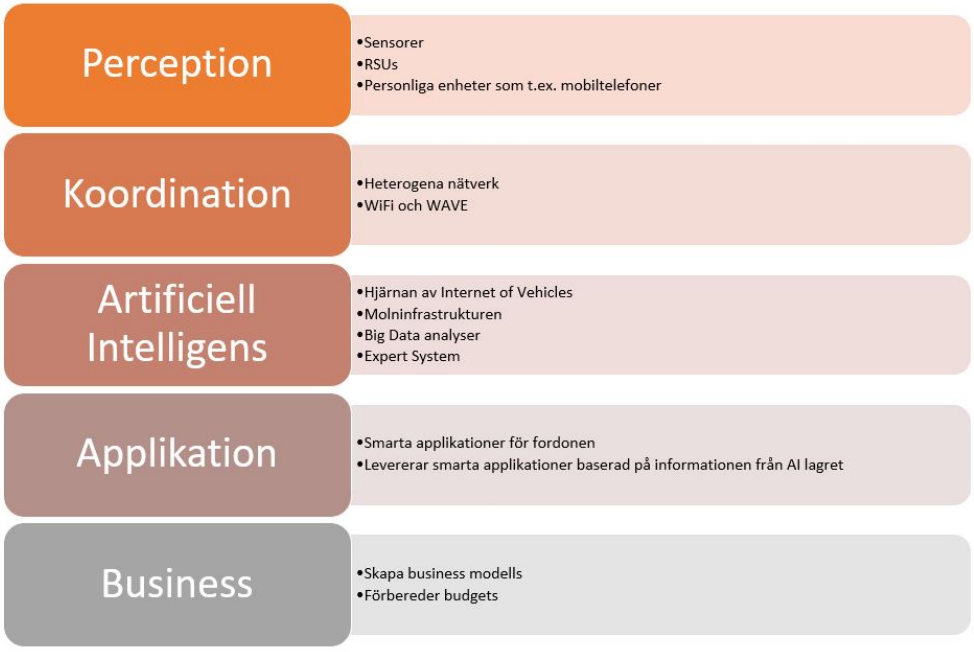
VANETs syfte var att förbättra säkerheten inom trafiken och effektiviteten med realtidskommunikation mellan aktiverade fordon (Kaiwartya et al., 2016). VANET omvandlar

fordonet till en trådlös router eller mobilnod, vilket gör det möjligt för fordonen att ansluta sig till varandra och skapa ett nätverk (Yang et al., 2014). Upkar Varshney (2005) skriver i artikeln "*Vehicular Mobile E-Commerce: Applications, Challenges and Research Problems*" att det finns svårigheter med att bygga ett bra Adhoc nätverk eftersom fordon befinner sig i rörelse och färdas i olika riktningar (se Figur 1). Det kommer vara enklare att bygga nätverket genom att skapa det hos fordon som kör i samma riktning och i någorlunda samma hastighet (Varshney, 2005).



Figur 1: Kommunikationen med Adhoc nätverk (Varshney, 2005).

Inom IoV finns det fem olika lager av arkitektur (Kaiwartya et al., 2016). Bilden nedan beskriver övergripande de fem olika lagerna (se Figur 2).



Figur 2: Lager av arkitektur (Kaiwartya et al., 2016).

2.1.2 Vehicle Cloud

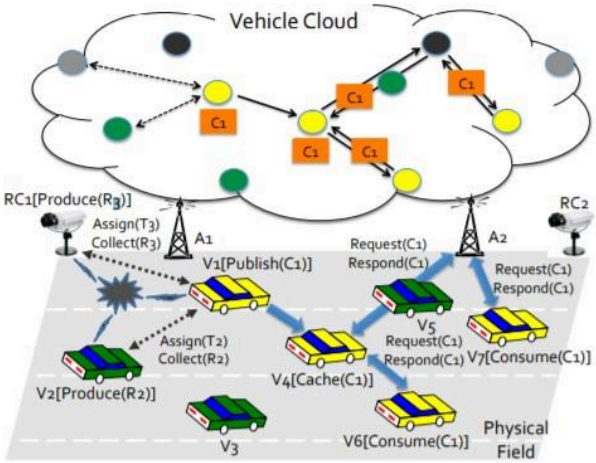
I artikeln *Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds* skriver författarna:

"We claim that the Vehicular Cloud is the core system environment that makes this evolution possible."(Gerla, M., Lee, E.K., Paul, G. och Lee, U, 2012).

För att molnet ska fungera behövs information vilket genereras genom fordon och sensorer (Gerla et al., 2012). Ett "Vehicular cloud" skapas för att kunna möjliggöra samarbeten mellan olika fordon, eftersom fordonen inte ensamma klarar av att skapa den avancerade tjänsten som behövs (Gerla et al., 2012). Till skillnad från ett vanligt moln blir vehicle cloud mer temporärt på grund av fordonen rör på sig (Gerla et al., 2012). Varje fordon har tre sorters resurser: datalagring, sensorer och möjligheten till att göra beräkningar (Gerla et al., 2012). Enligt modellen Vehicular Cloud Computing (VCC) är de ledande applikationerna i Vehicle cloud säker körning, intelligent transport och innehållsfördelning (Gerla et al., 2012). Fordonet samlar in information genom sensorer t.ex. från andra bilar och omgivning (Gerla et al., 2012). Sedan organiserar, byter mellan fordonen eller behåller de data och allt sparas (Gerla et al., 2012). Data som samlas in kan sedan användas till t.ex. beräkningar av stadsföroreningar, samla in bilder/filmer av olyckor eller identifiera eventuella terroristhot (Gerla et al., 2012).

Kaiwartya et al. (2014) beskriver ett ramverk med tre operationsnivåer. De olika operationsnivåerna baseras på trafikinformation som laddas upp, bearbetas, lagras och skickas vidare genom molnarkitekturen (Kaiwartya et al., 2016). Första nivån heter "Basic Cloud Services" och där inkluderas tjänster som t.ex. smarta trafikprogramservrar och andra samarbeten så att all information kan sparas på rätt sätt (Kaiwartya et al., 2016). Andra nivån heter "Smart ITS application servers" som inkluderar fyra kategorier: trafiksäkerhet, trafikledning, service och underhåll (Kaiwartya et al., 2016). Tredje och sista nivån heter "Information consumer and producer" där informationen bearbetas av artificiell intelligens i realtid för att kunna göra smarta beslut och klientapplikationer (Kaiwartya et al., 2016).

Information Centric Networking (ICN) skapades som en form av kommunikationsarkitektur för att uppnå effektiv innehållsfördelning på internet (Gerla et.al., 2014). Fokus ligger mer på *vad* istället för *var* för att lättare kunna ge både konsumenter och publicerare tillgång till det som behövs (Gerla et.al., 2014). Publicerare strävar efter att effektivt distribuera information till konsumenterna (Gerla et.al., 2014). För att ett så bra Vehicle Cloud som möjligt ska skapas behövs ett stabilt samarbete mellan VCC och ICN för att skapa och upprätthålla en effektiv virtuell plattform (Gerla et.al., 2014).



Figur 3: Kommunikation mellan fordon och Vehicle Cloud (Gerla et al., 2014).

2.2 Säkerhet

Liksom ett manuellt styrt fordon är även autonoma fordon utsatta för samma säkerhetsrisker som t.ex. integritet och attacker av fordonet (Gerla et al., 2014). Dock hävdar författarna att risken är större hos autonoma fordon då personen bakom ratten inte innehar kontrollen (Gerla et al., 2014).

Raya, Papadimitratos och Hubaux (2006) listar 6 vanliga risker som ofta förekommer med autonoma bilar.

Tabell 1: Säkerhetsrisker med autonoma fordon

Risker	**Förklaringar**
Trafikstockning (Jamming)	Generering av störningar förhindrar kommunikation som i vissa områden enkelt möjliggör för angripare att skapa tillgång till fordonets nätverk (Raya et al., 2006).
Förfalskning (Forgery)	För att fordonet skall fungera är korrekthet och rätt mottagande av data A och O. Förfalskning av data skapar stora säkerhetsproblem (Raya et al., 2006).
Transittrafik mixtrande (In-transit Traffic Tampering)	Varje bil har en nod som skickar information mellan varandra. Överföring av mixtrade meddelanden kan resultera i potentiella attacker (Raya et al., 2006).
Imitation (Impersonation)	En angripare använder meddelandeförfalskning för att låtsas vara någon annan (föraren) och i sin tur vilseleda andra fordon och förare till eventuella olyckor (Raya et al., 2006).
Integritetsintrång (Privacy Violation)	Informationsinsamlingen om fordonet kan i vissa fall omvandlas till personlig data om föraren. Meddelande innefattande resedetaljer, platser, betalningar mm. kan i slutändan kopplas till föraren som person (Raya et al., 2006).
Ombord mixtrande (On-board Tampering)	Istället för att angriparen tar sig in via meddelande kan denne även mixtra med fordonets data och dess källa. Manipulation av avläsning och hårdvara kan med rätt teknik orsaka stora säkerhetshot (Raya et al., 2006).

Begreppet Social Internet of Vehicles (SIoV) behandlar ett nätverk för sociala interaktioner mellan fordon och förare (Maglaras, L., Al-Bayatti, A., He, Y., Wagner, I. och Janicke, H. 2016). Att säkra detta nätverk är ett måste för att förebygga möjliga säkerhetsrisker som rör sig om: förnekande av en service attack, falsk inmatning av meddelande, virus, maskering,

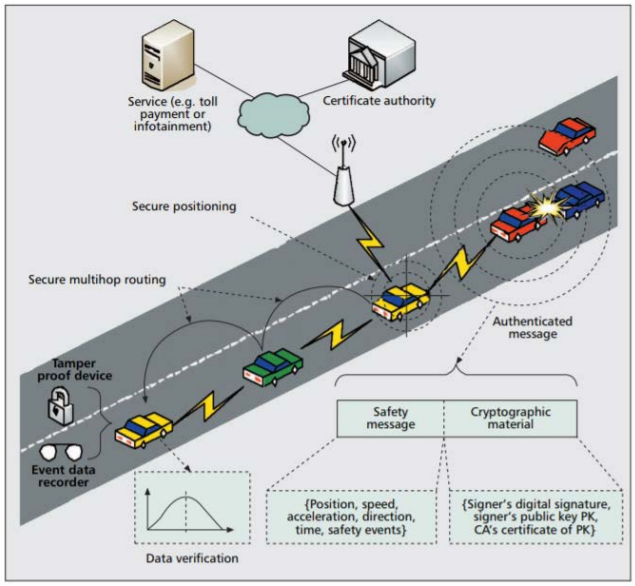
personifiering, förtroendeproblem m.fl. (Maglaras et.al., 2016). De menar att riskerna är många som i sin tur är svåra att lösa (Maglaras et.al., 2016).

Skydd mot attacker, både från externa likväl interna, måste designas med en högre säkerhetsstandard (Gerla et al., 2014). Åtkomst till on-boarding diagnostik (OBD) och CAN-bussar (Controller Area Network) kan motverka skada vid en eventuell attack (Gerla et al., 2014). Även multi-faktors skyddsstrategi har undersökts (Gerla et al., 2014). Rättigheten för dataavläsning förflyttas då från systemet och riskerna att andra fordon kan få åtkomst minskas (Gerla et al., 2014). Dock måste tillgång till känslig utrustning inuti fordonet möjliggöras till två olika instanser (Gerla et al., 2014). Varje autonomt fordon kan då prioritera access och skydd och höjer därmed skyddsfaktorn på flera nivåer (Gerla et al., 2014).

2.2.1 Säkerhetsarkitektur

För att säkra fordonet mot säkerhetsrisker krävs två hårdvarukomponenter: event data recorder (EDR) och tamper-proof device (TPD) (Raya et al., 2006). TPD har funktioner som stödjer kryptografisk analys som EDR i sin tur kan lagra tillsammans med all annan data som rör sig från och till fordonet (Raya et al., 2006). EDR är vanligt förekommande i många av dagens fordon då de lagrar säkerhetsmeddelanden kopplade till avgörande trafiksituationer (Raya et al., 2006).

För att skydda fordonets kryptografiska nycklar och dess funktioner behövs ett TPD som lagrar, utför och verifierar dessa operationer och sin tur säkerställer ansvarsskyldiga attribut inuti fordonet (Raya et al., 2006). TDP måste vara så gott som oberoende av omgivningen för att kunna utföra sina processer, men risken är att datans korrekthet blir svår att kontrollera (Raya et al., 2006). Dock medför installationen av TPD höga kostnader som hade underlättas genom att skapa en enklare variant, inflytande i uppbyggnaden av EDR samt sänkning av kostnader genom stordriftsfördelar (Raya et al., 2006).



Figur 4: Överblick av säkerhetsarkitektur (Raya et al., 2006).

2.3 Artificiell intelligens (AI)

Tegmark skriver i boken Life 3.0 (2017) följande citat som försöker förklara vad intelligens är:

"*Intelligence = ability to accomplish complex goals*" (Tegmark, 2017).

Det finns ett problem med att definiera vad intelligens egentligen är, då det kan tolkas på olika sätt (Tegmark, 2017). I boken berättar författaren att de bett en panel av ledande forskare inom artificiell intelligens (AI) att förklara ordet intelligens och de kom inte fram med ett gemensamt svar (Tegmark, 2017).

Artificiell intelligens erbjuder ett unikt och kraftfullt verktyg för att gräva djupare inom frågor gällande intelligenta beteenden (Russell och Norvig, 2010). Det är också en gren inom datavetenskap med automation av dessa beteenden (Russell och Norvig, 2010). Det handlar inte bara om att förstå utan också att bygga intelligenta enheter (Russell och Norvig, 2010). Idag omfattar AI många olika områden. Allt från det allmänna så som lärande och uppfattning till specifika områden som att spela schack eller köra bil (Russell och Norvig, 2010). Russell och Norvig (2010) berättar att historiskt sett finns det fyra olika tillvägagångssätt inom AI:

- Tänka mänskligt
- Tänka rationellt
- Agera mänskligt
- Agera rationellt

Dessa delas sen in i mänskligt och rationellt (Russell och Norvig, 2010). Tillvägagångssättet med mänskligt fokus måste vara en del av en empirisk studie där observationer och hypoteser gällande det mänskliga beteendet analyseras (Russell och Norvig, 2010). Medan en rationalists tillvägagångssätt involverar en kombination av matematik och teknik (Russell och Norvig, 2010).

Artificiell intelligens kan hjälpa till att rädda miljoner liv vid olyckor genom transport av olika slag i trafiken (Tegmark, 2017). 2015 dog 1,2 miljoner människor i bilolyckor världen över och majoriteten av dessa olyckor orsakades genom mänskliga misstag (Tegmark, 2017). Genom att använda sig av AI och självköranden fordon hade det gått att förhindra 90 % av olyckorna (Tegmark, 2017).

Sommaren 1956 samlades den tidens forskare inom artificiell intelligens, som många idag titulerats som grundare inom området (Tegmark, 2017). Några av de som deltog var: John Mccarthy, Marvin Minsky, Nathaniel Rochester, Claude Shannon m.fl., syftet med konferensen lyder:

"We propose that a 2 month, 10 man study of artificial intelligence be carried out during the summer of 1956 at Dartmouth College… An attempt will be made to find how to make problems now reserved for humans, and improve themselves. We think that a significant advantage can be made one or more of these problems if a carefully selected group of scientists work on in together for a summer." (Tegmark, 2017).

Några av konferensens deltagare har bidragit med betydande forskning inom området (Tegmark, 2017).

Tabell 2: Grundare av artificiell intelligens

Grundare av artificiell intelligens	**Kända områden**
Alan Turing	The Turing Theory (Copeland, 2001)
Allen Newell	The Chess Machine (Newell, 1955)
Allen Newell, John Clifford Shaw, Herbert A. Simon	The Logical Theory Machine (Newell et.al., 1957) General Problem solver (GPS) (Newell et.al., 1959)
John McCarthy	Lisp Programming (Childs, 2011)
Marvin Minsky	Artificial Neural Networks (Kelemen, 2007)
Arthur Samuel	Computer checkers (Samuel, 1967)

2.3.1 The Turing Theory

Alan Turing var en vetenskapsman inom information- och datavetenskap (Epstein, R., Roberts, G and Beber, G. 2009). Turing kan ses som fadern till artificiell intelligens (Epstein et.al., 2009). År 1950 publicerades hans artikel *Computing Machinery and Intelligence* där han förutspådde att vi vid år 2000 kommer att ha maskiner med högre intelligens än människan och att de skulle kunna kommunicera på mänskligt vis (Epstein et.al., 2009). Han påstod även att dessa maskiner kan *tänka* själva och att vi inte längre skulle kunna skilja dem från oss själva (Epstein et.al., 2009). "The Imitation Game" som han själv kallade det, har senare givits namnet "The Turing Test" (Epstein et.al., 2009). Turings tankegång har under decennier sysselsatt vetenskapsmän i hur vi ska verkställa denna teori (Epstein et.al., 2009).

2.3.2 The Turing Test

På 1950-talet fanns det en variant av testet som beskrev en imitation av ett spel där en intervjuare och två deltagare, en man (A) och en kvinna (B), deltog (Copeland, 2001). Under testet ska intervjuaren bestämma vem av deltagare A och B som är en man (Copeland, 2001). Detta får endast göras genom frågor och svar (Copeland, 2001). A:s uppgift är att förvirra intervjuaren så att det inte går att identifiera vem av deltagarna som är man eller kvinna (Copeland, 2001). Turing ställde en fråga i sin artikel "*What happen when a machine takes the part of A in this game?"* (Copeland, 2001). Genom detta test ska det framgå ifall en dator kan imitera en hjärna eller inte (Copeland, 2001). Russel och Norvig (2010) skriver att en dator behöver kunna sex saker för att klara av testet:

1. Naturlig språkbehandling
2. Kunskapsrepresentation samt kunna spara information
3. Resonera genom att använda den sparade informationen och dra nya slutsatser

4. Maskininlärning för att anpassa sig till nya omständigheter och upptäcka mönster
5. Datorvision för att kunna uppfatta objekt
6. Robotik för att manipulera objekt

Sedan testet skapades har det bestått utav tre väsentliga komponenter berättar Copeland (2001) i artikeln The Turing Test:

1. Turing's Principle
2. Frågeformuläret kan hjälpa intervjupersonen att avgöra om det är en maskin eller människa som svarar
3. Imitationsspel

Vid 1950 förutspådde Turing att det skulle vara möjligt att programmera datorer och då kommer intervjuaren bara ha 70 % chans att identifiera deltagarna efter fem minuters frågor i testet (Copeland, 2001).

2.3.3 The Turing Machine

Även om artikeln från 1950 ses som Turings främsta verk, har hans bidrag under tidigare år haft stor betydelse (Epstein et.al., 2009). Under hans tid på Cambridge Universitetet skapade han år 1936 definitionen av en maskin som modellerats utefter vad en människa med begränsad utrustning skulle kunna utföra genom att följa en metod baserad på imitationsprincip (Epstein et.al., 2009). Maskinen har sedan givits namnet The Turing Machine (Epstein et.al., 2009). I artikeln från 1936 namnges även konceptet om en Universal Turing Machine, som sedan blivit grunden till moderna datorer (Epstein et.al., 2009).

2.3.4 A Reverse Turing Test

Turings teorier har applicerats i många generationer och har under denna period återskapats i nya varianter (Baird, H., Coates, A. och Fateman, R. 2002). Baird, Coates och Fateman (2002) påstår att det inte existerar en maskin som enligt Turings synsätt har godkänt The Turing Test. De föreslår "Reverse Turing Test" där användaren, maskin eller människa genomför testet för att komma åt en skyddad webbsida (Baird et.al., 2002). Användaren ska tyda en genererad text i bildformat och svara i rätt ordning för att ansluta (Baird et.al., 2002). The Reverse Turing Test skiljer sig från Turings originaltest på minst fyra vis (Baird et.al., 2002).

- Maskinen bedömer, istället för människan
- Endast en användare, istället för två
- Designmålet är att särskilja, snarare än att misslyckas att särskilja människa och maskin
- Testet har en eller få utmaningar, snarare än oändligt många

The Reverse Turing test är byggt på ett så kallat *Pessimal Print*- (se Figur 5) vilket syftar på en text som är av sämre bildkvalité än vad den vanligtvis bör vara men är fortfarande läslig (Baird et.al., 2002). Deras studie undersöker om ett system som applicerar The Reverse Turing Test skyddar sig mot en attack, förutsatt att angriparen är omedveten av testet (Baird

et.al., 2002). Resultatet visar att användandet av testet kan ge en pålitlig, snabb och automatisk metod för att särskilja människor och maskiner som användare av ett GUI (Baird et.al., 2002).

Figur 5: Exempel på Pessimal Print (Baird et al., 2002)

De förmodade att Turing planerade en attack där han förutspådde att systemet enkelt skulle ge efter (Baird et.al., 2002). The Reverse Turing test har idag blivit en standard för många forskare inom AI området (Baird et.al., 2002).

2.3.5 Machine vision

Turing testet är något som de flesta forskare inom AI har som mål att kunna passera, men som i vissa fall kan ses som helt omöjligt (Putchala och Agarwal, 2009). Likt The Reverse Turing Test har testet modifierats för att beröra de problem som finns med det ursprungliga testet. Putchala och Agarwal (2009) genomförde en studie för att undersöka "Machine Vision" (Maskinernas Vision) när de genomför säkerhetstest som CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) med hjälp av The Reverse Turing Test. Syfte var att lösa nuvarande säkerhetsproblem samt diskutera hackningstekniker rörande CAPTCHA (Putchala och Agarwal, 2009).

Putchala och Agarwal (2009) utgick från The Reverse Turing Test, där datorn bedömer om användaren är mänsklig eller inte. Användaren ges en genererad CAPTCHA-bild att lösa för att besöka sidan (Putchala och Agarwal, 2009). Målet med testet är att särskilja människa och robot och samtidigt klara testet (Putchala och Agarwal, 2009). När robotar försöker få tillgång till sidan finns en risk att de registrerar tidigare test och tillslut överlistar testet (Putchala och Agarwal, 2009).

Testets formgivning gick först och främst ut på att identifiera den mjukvara som skulle utveckla det oläsliga bildspråket, där valdes: *Pixopedia 24* och *Gimp 2.6.7* (Putchala och Agarwal, 2009). Därefter utformades ett brett bibliotek av CAPTCHA-bildspråk (41 totalt) som skulle vara enkelt för en människa att lösa (Putchala och Agarwal, 2009). OCR (Optical Character Recognition) mjukvara tog rollen som "Machine Vision" (Putchala och Agarwal, 2009). 25 Alfa och 25 Alfa-Numeriska- Rå bilder: 5 bokstäver långa, 10 nummer som bas genererades, var av 29 av dessa valdes till varje test (Putchala och Agarwal, 2009).

Resultatet av testet var att bilderna var lättlästa för människor medan alla deltagande OCR-system misslyckades med att tyda bilderna (Putchala och Agarwal, 2009). OCR-systemen lyckades endast tyda två av CAPTCHA-bilderna, vilket till stor del kan bero på det mänskliga utformandet av testet (Putchala och Agarwal, 2009). Maskinerna lyckades dessvärre inte tyda

någon av bokstavskombinationerna (Putchala och Agarwal, 2009). Alltså hade maskinerna misslyckats med att imitera människan (Putchala och Agarwal, 2009).

Författarna anser att det inte bara är de OCR-system som deltog i just detta test som har problem med detta, utan att svårigheten i att imitera människan är ett generellt problem för moderna OCR-system, eftersom de OCR-system som deltog i undersökningen var bland de högst listade (Putchala och Agarwal, 2009). Även bildförrådet som användes ansågs inte kräva någon större teknisk kunskap för att lösas (Putchala och Agarwal, 2009). Användandet av Machine Vision kombinerat med ett Reverse Turing Test visade att maskinerna inte är på den säkerhetsnivå idag som de bör vara på (Putchala och Agarwal, 2009).

Trots att Turing testet har några år på nacken så används det än idag i olika variationer för att finna lösningar kopplade till artificiell intelligens (Putchala och Agarwal, 2009). Putchala och Agarwal (2009) nämner att några av de vanligaste frågorna som än idag kvarstår är:

a) Hur är relationen mellan språket och kognitiva förmågor?
b) Hur vi kan skapa datorer som kan läsa och förstå mänskliga språk?
c) Utvecklas AI-system på det vis som tidigare förutspåtts?

Att klara Turing testet kan lösa kampen mellan människan och artificiell intelligens (Putchala och Agarwal, 2009). Det kan även ge möjlighet att samla ihop kunskap inom maskininlärning som slutgiltigen kan hjälpa maskinerna att passera testet (Putchala och Agarwal, 2009).

"Machine reading (According to Alan Turing)—which he planned to attack and which he expected to yield easily— has instead resisted solution for 60 years and now is poised to provide a technical solution and in providing a combative solution for Machine/Human inter-distinguish ability." (Putchala och Agarwal, 2009).

2.4 Avslutning

Lee (2015-2016) hävdar att hackerattacker på internet idag utförs på en oacceptabel skala och därför finner sig även autonoma bilar i riskzonen.

"*It is easy to imagine that, in the not-so-distant future, malicious hackers could cause traffic accidents by taking control of self-driving cars****. "*** (Lee, 2015-2016).

De säkerhetsstandarder som används i dagsläget måste stärkas för att föra oss ur riskzonen och i denna fråga är ansvar viktigt (Lee, 2015-2016).

2.5 Undersökningsmodell

Vår undersökningsmodell styrs av vår omfattande litteraturstudie som vi presenterat tidigare. Tabell 3 nedan belyser nyckelbegreppen i resultatet från litteraturstudien. Vi börjar med att sammankoppla grundläggande aspekter samt praktiska aspekter som formulerat vår undersökningsmodell, som i sin tur har använts för att styra vårt empiriska arbete. I våra grundläggande aspekter fokuserar vi särskilt på definitionerna av Internet of Vehicles och Vehicle Cloud och de mer praktiskt inriktade aspekterna är de som hanterar säkerhetsaspekter, samt en övergripande genomgång av artificiell intelligens.

Tabell 3: Undersökningsmodell

Tema	Litteraturgenomgång gällande självkörande bilar	Referenser
Koppling mellan IoT och IoV.	• Definition av Internet of Vehicles • Skillnader mellan Internet of Things och Internet of Vehicles • Förklaring vad IoV är uppbyggt av	Fluchter & Wortmann (2015) Dimitrakopoulos (2011) Kaiwartya, et al. (2016) Varshney (2005) Yang, et al. (2014)
Existerar en vehicle cloud infrastruktur idag?	• Definition av Vehicular Cloud • Förklaring hur kommunikationen mellan IoV och Vehicular Cloud fungerar	Gerla, et al. (2014) Kaiwartya, et al. (2016)
Är IoV säkert idag? Aktuella hot/problem med IoV. Åtgärder för att styrka säkerheten inom IoV. Hackning, hur åtgärdas det?	• Säkerhetsrisker och hot med autonoma fordon • Säkerhetsåtgärder	Gerla, et al. (2014) Raya, et al. (2016) Maglaras, et al. (2016)
Är AI hjärnan av IoV?	• Definition av artificiell intelligens • Genomgång av diverse säkerhetstester	Baird, et al. (2002) Childs (2011) Copeland (2001) Epstein, et al. (2009) Kelemen (2007) Newell (1995) Putchala, et al. (2009) Russel och Norvig (2010) Samuel (1967) Tegmark (2010)

I vår litteraturgenomgång har vi övervägt flera aspekter som väglett oss. Som framgår av tabellen ovan har vi först tacklat grundläggande perspektiv som styrde våra teoretiska aspekter. Genom att göra denna litteraturgenomgång har vi också i stor utsträckning diskuterat aspekter som inte är betydande i vår undersökningsmodell, men som tillför viktig information till studien. Att arbeta med begreppet artificiell intelligens och dess tidiga utveckling gav oss grunden till att bättre förstå det övergripande sammanhanget i vår studie. Därför, trots att en del AI-bakgrund inte har använts direkt i vår empiriska studie, anses det som en grund för att vägleda för att bättre förstå sammanhanget i vår studie, vilket är säkerhet inom autonoma fordon.

Slutligen är Tabell 3 också viktig för att utforma vår intervjuguide där alla dessa teoretiska aspekter har behandlats noggrant för att se till att vår empiriska studie kunde ta itu med såväl de grundläggande som praktiska aspekterna som infördes. Nästa kapitel presenterar vår metod, där vi särskilt fokuserar på utformningen av vår intervjuguide.

3 Metod

I metodkapitlet presenteras den vetenskapliga metod och tillvägagångssätt som används för att genomföra studien. Därefter ges metodval, beskrivning av urvalsprocessen, intervjustruktur, transkribering och analys av intervjuer samt undersökningskvalitet.

3.1 Insamling av empirisk data

3.1.1 Metodval

Enligt Jacobsen (2002) finns det två olika metoder att välja mellan kvalitativ och kvantitativ när data samlas in. De tre första stegen i en undersökningsprocess är likadana för de två olika metoderna, därefter skiljer de sig åt en del (Jacobsen, 2002). Första steget är utveckling av problemställning, därefter väljs undersökningsupplägg och tredje steget är att välja metodansats (Jacobsen, 2002). I den kvalitativa ansatsen sker datainsamlingen genom intervjuer eller observationer (Jacobsen, 2002). Medan i den kvantitativa ansatsen sker datainsamlingen genom t.ex. frågeformulär (Jacobsen, 2002). Skillnaden mellan de olika studierna är att en kvalitativ studie ger mer detaljerad data till skillnad från kvantitativa studier som ger en mer generell data då det oftast är fler respondenter till dem (Jacobsen, 2002). I den kvalitativa studien används inte siffror eller tal, det är endast verbala formuleringar som är skrivna eller talade (Backman, 2016). Genom den kvalitativa studien kan ett djup kring problembeskrivningen utvecklas genom det öppna samtalet mellan respondent och undersökare (Jacobsen, 2002). Backman (2016) berättar att den vanligaste metoden i en kvalitativ studie är en intervju, men också att en intervju ofta är svår att genomföra på rätt sätt. En intervju ställer höga krav på personen som genomför den så att det sker genom ett kvalitativt perspektiv (Backman, 2016). Backman (2016) menar att ibland krävs det tränade intervjuare och dokumenterare för att få fram ett bra resultat.

I vår studie har vi valt att använda den kvalitativa metoden för att kunna få djupare svar av respondenterna. Vi har valt att intervjua personer inom olika områden för att skapa en bra bild över problemområdet. Samtliga respondenter har stor erfarenhet inom de områdena som vi undersöker. I nästkommande delar av kapitlet förklaras närmare hur vi har gått tillväga i vår kvalitativa metod.

3.1.2 Urval

I urvalsprocessen har vi utgått ifrån att tillfråga individer från två fokusgrupper: forskare och personer som arbetar inom området för autonoma fordon. Detta för att stödja vår valda teori samt att se om den stämmer överens i dagsläget. I och med detta täcks ett bredare perspektiv i gällande forskningsfrågan. Respondenterna har olika bakgrund och erfarenhet, men samtliga har kunskap inom ämnet från olika perspektiv.

Utforskandet av möjliga respondenter utgick ifrån att besöka universitets- och företagshemsidor, varefter val gjordes av de individer som var mest relevanta utefter den

beskrivning som fanns. Första kontakten skedde i form av e-postkonversation med både forskare och företagsrepresentanter utifrån de uppgifter vi fann på respektive hemsida. Vi använde även vårt kontaktnät via LinkedIn för att få kontakt med personer som vi annars inte hade hittat. Detta genomfördes genom ett inlägg på våra profiler där vi beskrev studiens upplägg. Inlägget blev väldigt lyckat och gjorde att vi kom i kontakt med många spännande kandidater. Där presenterade vi oss själva, frågan som ligger till grund för vår studie samt en kort beskrivning av uppsatsens centrala byggstenar: säkerhet med Internet of Vehicles (IoV), artificiell intelligens, autonoma fordon kopplat till informationsflöde. Vidare frågades om de hade möjlighet och intresse för en eventuell intervju eller hade kännedom om någon annan lämplig person vi kunde kontakta i frågan. Utfallet av e-postutskicket och LinkedIn inlägget resulterade i intervjuer med en forskare och fyra olika företag.

Tabell 4: Intervjukandidater

Person	Namn	Företag	Position	Plats	Intervjutyp	Appendix
IP1	Informant 1	Företag Z	Developer	Sverige	Telefonintervju	8.3.1
IP2	Jone Løvvik	Acando	SVP & Head of Strategic Programs	Norge	Telefonintervju	8.3.2
IP3	Informant 3	Företag X	Senior Software Consultant	Sverige	Telefonintervju	8.3.3
IP4	Tomas Olavsson	Chalmers Universitet	Docent och avdelningschef, Nätverk och system, Data- och informationsteknik	Sverige	Telefonintervju	8.3.4
IP5	Informant 5	Företag Y	Developer	Sverige	Telefonintervju	8.3.5

3.2 Intervjustruktur

Intervjufrågorna som ställdes under intervjun hade en tydlig struktur för att få med områdena som diskuteras i studien. Strukturen var gjord med en öppenhet så att respondenterna presenterade svaren utan någon vägledning. Frågorna var förbestämda men det lämnades utrymme för följdfrågor. Ibland bad vi även dem även förtydliga sina svar ifall något var otydlig eller att vi inte förstod innebörden.

Med hänvisning till tabell 3 i kapitel 2 har vi beaktat alla presenterade aspekter när vi utformade intervjuguiden. Vi försäkrade oss om att vi berör de grundläggande aspekterna på en mer abstrakt nivå och de praktiska aspekterna från ett mer konkret perspektiv inom autonoma fordon och säkerhet, genom att först börja med den abstrakta nivån och gå vidare

till den mer konkreta. För detaljer relaterade till intervjuguiden presenteras frågorna i appendix 8.1 samt 8.2.

I början av varje intervju frågades respondenten ifall de godkände att intervjun spelades in. Inspelningens syfte var att det skulle bli enklare att transkribera intervjun i efterhand samt även i analyseringssyfte.

De första frågorna som ställdes handlade om intervjukandidatens bakgrund som t.ex. utbildning, arbetslivserfarenhet och vad de arbetade med idag. Därefter ställdes bakgrundsfrågor om företaget ifall det var en företagsrepresentant, för att få en förståelse varför deras företag arbetar med t.ex. Internet of Vehicles. Andra delen bestod av frågor gällande IoV, Vehicle Cloud och artificiell intelligens. Slutligen ställdes frågor som kunde hjälpa oss att komma i kontakt med andra inom samma område och så vidare.

3.3 Transkribering och analys av intervjusvar

Från början bestämde vi att allt inspelat material skulle transkriberas och detta ordagrant. Undantag blev endast otydliga ord eller otydligt tal samt frågor/påståenden som uppkom och som inte egentligen var relevanta för själva studien.

Redan vid e-postkonversationen hade vi tagit upp möjligheten till att vara anonym för att intervjukandidaten skulle känna sig säker. Innan intervjun började tog vi upp ämnet igen för att kontrollera att allt gick rätt till. Vissa intervjukandidater ville vara anonyma, så därför nämns deras företag med t.ex. “Företag X” osv, så att det inte går att se vem som arbetar var.

Inspelning av intervjuer inom kvalitativa forskningsstudier används ofta på grund av det kan vara problematiskt att hinna anteckna allt som sägs och vem som säger vad (Bryman, 2008). Väntan på att sekreteraren ska hinna anteckna allt kan bli ett störningsmoment (Bryman, 2008). Under intervjun ansvarade en för anteckning av svar och en styrde intervjun, för att underlätta den slutgiltiga transkriberingen. Efter varje intervju transkriberades all information. Detta för att få en tydligare överblick och lättare kunna analysera och jämföra resultatet av intervjuerna. Innan intervjuerna numrerades alla frågor för att lättare kunna gå tillbaka till efteråt.

3.4 Undersökningskvalitet

3.4.1 Validitet och reliabilitet

Jacobsen (2002) nämner att begreppen validitet (giltighet) och reliabilitet (tillgänglighet) inte ska förbises i kvalitativa undersökningar då de kan ha en negativ påverkan på det slutgiltiga resultatet. Detta innefattar att man ska granska kvaliteten på insamlad data med ett kritiskt öga gällande intern och extern validitet (Jacobsen, 2002). Intern validitet syftar på resultatets

riktighet medan extern validitet syftar på nivån av generalisering i undersökningen (Jacobsen, 2002).

Den interna validiteten kan prövas genom två olika steg: kontroll av undersökningen och slutsats samt resultatgranskning (Jacobsen, 2002). Kontrollerna kan genomföras på flera olika vis t.ex. konfrontation av enskilda individer, diskussionsmöten, utskick av preliminär rapport (Jacobsen, 2002). Likaså kan personerna i fråga lämna kommentarer på innehållet och säkerställa att det stämmer, även kallat giltighetskontroll (Jacobsen, 2002). Detta innebär att när den slutgiltiga rapporten var sammanställd skickades dessa till respondenterna för att säkerställa validiteten och möjliggöra för dem att ta del av resultatet.

Det finns olika kontexteffekter som kan påverka den insamlade empirins reliabilitet (Jacobsen, 2002). De två olika alternativen är artificiell eller naturlig (Jacobsen, 2002). En artificiell kontext är när intervjukandidaten blir intervjuad i ett sammanhang som är ovanligt (Jacobsen, 2002). Därför är det bättre att använda sig utav en naturlig kontext för att reliabiliteten av resultatet ska bli hög (Jacobsen, 2002). En naturlig kontext kan vara t.ex. att intervjun sker på intervjukandidatens arbetsplats (Jacobsen, 2002). Jacobsen (2002) berättar att det även finns störande inslag på naturliga kontexter som att medarbetare kan knacka på för att ställa frågor och avbryta intervjun. Det kan också bli olika resultat ifall intervjun är planerad eller överraskande (Jacobsen, 2002). En planerad kan vara att intervjukandidaten har fått tid på sig att förbereda sig till medan en överraskande är att allt sker utan någon planering (Jacobsen, 2002). I vårt fall genomfördes samtliga intervjuer över telefon, därmed kunde intervjukandidaten själv välja en bekväm plats för intervjun. Självklart kan eventuella störningsmoment även uppstå vid en telefonintervju men vi ansåg att det var den mest lämpade lösningen i vårt fall då kandidaterna var utspridda utöver Skandinavien. Vi utförde planerade intervjuer då vi i god tid skickade intervjufrågor till kandidaten, så att de fick möjlighet att förbereda sig och öka bekvämligheten.

3.4.2 Etik

Utlämnande av studiens verkliga syfte för medverkande, press till deltagande och nekande till privatliv kan ses som etiskt tvivelaktigt (Jacobsen, 2002). Det kan ses som en självklarhet i dessa situationer men det finns fall där förfalskningar och manipulation förekommer (Jacobsen, 2002). Bryman (2008) nämner att det finns fyra grundläggande etiska frågor, de är informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet. Informationskravet handlar om att syftet för undersökningen tydligt ska presenteras (Bryman, 2008). Vi angav tydligt vår frågeställning och syftet med studien samt att samtliga har samtyckt medverkande i undersökningen. Möjliggörande för utfyllnad av eventuella tomrum har givits för att säkerställa att deltagarna fått med alla aspekter i sin verksamhet.

Jacobsen (2002) hävdar att det är viktigt med “informerat samtycke” som bygger på ett frivilligt deltagande, där den medverkande är fullt medveten om tillkommande risker och vinster i undersökningen. Vi har kontaktat flertal personer och företag varav en del av dessa valt att inte delta i studien. Bryman (2008) berättar att genom samtyckeskravet har deltagare rätt att själva bestämma över sin medverkan, precis som Jacobsen (2002) menar med informerat samtycke. Vissa har nämnt att de inte har kunskap inom området och hänvisat oss till mer kompetenta individer. Vi har respekterat dessa beslut och inte valt att vidare pressa någon att delta och endast gått vidare med de som valt att medverka.

Konfidentialitetskravet handlar om att behandla de deltagande personerna med största möjliga konfidentialitet (Bryman, 2008). Vissa av medverkandes namn nämns inte i studien för att säkerställa dess anonymitet. En anledning till att personer är anonyma är att de ska våga svara utan att det ska kopplas till dem personligen (Jacobsen, 2002). Anonymitet är något som i första hand inte efterfrågats men som vi inte ansåg skulle bidra med eventuellt mervärde i det slutgiltiga resultatet. Vi syftar på att ta del av den kunskap personerna i frågan besitter. Uppgifterna som samlas in under intervjuerna hamnar under nyttjandekravet, vilket menas med att de bara används i studiens ändamål (Bryman, 2008). Som tidigare nämnt fick alla informanter frågan ifall de ville vara anonyma och ifall de önskade detta så fick de vara det.

3.4.3 Plats

Intervjuerna har skett över telefon, då respondenterna suttit utplacerade på olika ställen i Skandinavien. Denna metod underlättar intervjukandidaternas dagliga arbete och de kan sitta på en för dem bekväm och naturlig plats (Jacobsen, 2001). En naturlig plats är en plats som intervjukandidaten är välbekant med (Jacobsen, 2002). Ifall en intervju hålls i en miljö som intervjukandidaten inte känner sig säker med kan det komma fram svar som inte helt stämmer (Jacobsen, 2002). Bryman (2008) nämner att telefonintervjuer kan underlätta för respondenten att svara på mer känsliga frågor då intervjun sker utan fysisk närvaro.

Under intervjuerna användes inspelningsutrustning då det gav oss möjligheten att vara mer flytande och det var lättare att få med allt (Jacobsen, 2002). Vid sidan av inspelningen togs även anteckningar för att underlätta transkriberingen senare. Ibland kan användningen av inspelningsutrustning påverka intervjun på det viset att intervjuaren slappnar av och glömmer ta anteckningar vid sidan om (Jacobsen, 2002). I vårt fall användes inspelning i kombination med anteckningar för att säkerställa att ingen information uteblev samt att underlätta den slutgiltiga transkriberingen.

4 Resultat

I detta kapitel presenteras resultatet av den genomförda kvalitativa empiriska studien. En tabell används för att presentera resultatet på intervjufrågorna. Tabellen används för att tydliggöra vem av respondenterna som svarat vad och för att sedan kunna jämföra svaren. De olika områdena från intervjuerna har blivit uppdelade i egna tabeller. Då svaren har blivit förkortade refererar vi till transkriberingarna genom referensnumrering. Ifall någon intervjukandidat inte svarat på en fråga markeras det med bokstaven X.

Tabell 5: Inställning till utveckling av autonoma fordon

Kategorier	IP1	IP2	IP3	IP4	IP5
Hur ställer sig företaget/du till utveckling av självkörande fordon?	Det är viktigt, men primärt huvudfokus för företaget är utveckling av radiobasstationer för mobiler och 5G (IP1.8).	Acando Norge var de första som tog in självkörande minibuss till den norska marknaden. Så vi ser positivt på utvecklingen (IP2.11).	Jag tycker det är kul, men det är ingen annan i företaget som har arbetat med det innan (IP3.10).	Rent allmänt tror jag att när tekniken är mogen så tror jag att det är rätt utveckling att gå på. Det ser vi i bilarna idag, det får fler och fler funktioner som höjer säkerheten (IP4.8).	Jag kan nog inte svara för företaget exakt, men jag tror inte de är negativa till det (IP5.9).
Arbetar ni något med utveckling av självkörande fordon t.ex. Internet of Vehicles, AI eller Vehicle Cloud?	Vi utvecklar cloud infrastruktur för biltillverkare och Volvo är en stor kund som vi har haft länge (IP1.12).	X	Nej, det är ingen som har kompetensen till det mer än jag och jag vill inte utveckla igen (IP3.14).	X	Vi bygger cloud infrastrukturen för hela miljön. Det finns två delar en skarp befintlig miljö som används och en ny miljö som inte är i bruk än (IP5.11).
Om ja på ovanstående: Hur kommer det sig att företaget arbetar med utveckling av självkörande fordon?	Det började med ett samarbete mellan Volvo och oss. I början var det mest media och olika tjänster runt bilen som att du har en APP som du kan sätta på värmen ifrån o.s.v.(IP1.15).	X	X	X	X

Tabell 6: Internet of Vehicles, Vehicle cloud och utveckling

Kategorier	IP1	IP2	IP3	IP4	IP5
Ser du en koppling mellan Internet of Things och Internet of Vehicles?	Jag tycker att det i stort sett är samma sak, bilen är en Thing liksom. Men det som skiljer IoV från IoT är att säkerhetsaspekterna och prestanda kraven är mycket högre inom IoV (IP1.20).	Ja det gör jag! Alla ting kommer vara knutna till internet och inte minst fordon. Många av de stora leverantörerna arbetar med det och det handlar om elektricitet och connected och då kommer du in på IoV (IP2.15).	IoV är egentligen en större form av IoT, så det är egentligen samma sak. Allting har möjliggjorts genom att man kan använda Cloudet idag. Hade inte Cloudet gått igenom så hade man aldrig kunnat använda AI (IP3.16).	Ja, man brukar räkna in fordon i Internet of Things. De är en av de prylarna som kommer vara uppkopplade (IP4.15).	Ja, det gör jag väl. I IoT har du något som är uppkopplat och det kan vara vad som helst. Kopplingen i det här fallet är cloud miljön som alla fordon ansluter sig till (IP5.13).
Hur tror ni att utvecklingen kommer se ut framöver?	Vi har certifikatlösningar med bilen, största fokus kommer nog ligga på bilen självt och om någon får kontroll över den genom lokal access till bilen (IP1.26).	Det finns redan minibussar t.ex. i Kista som kör autonomt. De närmaste 1-2 åren tror vi att det kommer vara autonoma fordon som används på förutbestämda rutter (IP2.21).	Utvecklingen går fruktansvärt snabbt (IP3.34). Det handlar om en vanesak för människor att lita på den här självkörande/självverkande bilen (IP3.36).	Allting kommer ta tid. Det är väldigt många problem som måste lösas som man kanske inte tänker på (IP4.20).	Det kommer bygga på Micro-services, istället för en stor produkt har man mindre tjänster. Sen så kommer det bli ännu mer automatiserat. Vi bygger upp automatisering av dessa olika miljöer som deployas ute hos olika kunder och tillverkare. Däremellan kommer AI komma in mer (IP5.19).

Vad tror ni behövs i dagens samhälle för en stabil vehicle cloud infrastruktur ?	5G tycker jag är mycket viktigt. Men sen är det också viktigt att standarder för när bilarna börja köra själv sätts. Det är viktigt att sätta en standard för hur bilarna ska kunna kommunicera och hur clouden ska kunna kommunicera med olika tillverkare (IP1.35).	X	Ett distruberingslager mellan cloud och device, även kallat fog lagret (IP3.46).	Det man bygger på idag är två huvudsakliga kommuikationsbitar. Det ena är att du bygger med fordonskommunikation och den andra biten där är att i städer kan det bli problem för att stora områden inte är stärkta för att ha täckning precis och man har inte täckning överallt. Idag pratas det om att 5G kan hjälpa till där (IP4.26).	5G möjliggör bättre kommunikation mellan punkter till skillnad från mot vad det är idag (IP5.30).

Fortsättning Tabell 6

Tabell 7: Säkerhet

Kategorier	IP1	IP2	IP3	IP4	IP5
Hur ser ni på säkerhetsaspekter inom Internet of Vehicles i dagsläget?	Jag tycker att det är säkert. Det absolut största fokusområdet som vi har och det kontrolleras ständigt och återkommande. Företaget gör penetrationstester där de försöker penetrera vår säkerhetslösning t.ex. (IP1.22).	Det är en definitionsfråga. Det man kan säga om självkörande fordon är att idag är de säkrare än vi människor är (IP2.17). Men toleransen för fel är mycket mindre på maskiner än människor (IP2.19).	Det är branschens största utmaning. Varje bil innehåller 119 miljoner rader kod och man räknar med att i en professionell programvara är 5-20 security leaks per 1000 rader kod (IP3.21). Många bilföretag måste börja samarbeta och sätta standarder så de sitter med samma problem (IP3.28).	Det finns alltid en risk att någon/några biltillverkare prioriterar att sälja först och sedan lösa problemen sedan Man måste designa bilen från grunden på ett sådant sätt så att den kan hantera problem, för problem kommer det bli förr eller senare oavsett vad så att då måste man bygga den på ett sådant sätt så att den kan hantera säkerhetsproblem (IP4.15). Det räcker med att en av bilens dator blir hackad, så finns det stor risk att man via den kan påverka bilen i stort (IP4.17).	Det finns team som jobbar med de sakerna, jag sitter inte aktivt med säkerhetssaker idag. Jag anser att de som är ute i skarp produktion definitivt har hög säkerhet (IP5.17).
Vad kommer behövas för att stärka säkerheten med Internet of Vehicles?	Den största angreppspunkten är bilen självt, sen är det alltid kommunikationen men den är skyddad i sig (IP1.28).	Det kommer behövas lagverk för hur autonoma bilar ska köras i vanlig trafik. Myndigheten kommer spela en stor roll (IP2.25).	Man måste designa utifrån säkerheten, det andra är att man måste ha duktiga kodare, annars blir det inte säkert (IP3.38).	Dels då att designa insidan på ett sådant sätt så de klarar av att hantera, inte om men när det blir något säkerhetsproblem, när något blir hackat och så ska de upptäcka. Måste man ha bra koll med den kommunikationen som sker med utsidan. Bygga mer relevanta system (IP4.22).	X

Vilka hot/problem ser ni som mest aktuella?	Jag tror att just bilen är nog den mest självklara angreppspunkten (IP1.28).	Kortsiktiga är hur vi ska blanda autonoma fordon i vanlig trafik. Sen också mycket säkerhet och trygghet mot teknologin (IP2.25).	Det består av 3 bitar: 1. Kvalitet och att utvecklingsprocessen måste innehålla säkerhet. 2. Organisationerna måste förändra sig. 3. Organisationerna måste drivas via data (IP3.40).	Man måste bygga skydd mot hackers. Om bilen upptäcker något problem ska den kunna stänga av de funktionerna eller begränsa skadan (IP4.24).	De största problemen är att saker kan bli utdaterade. T.ex. olika typer av verktyg och typer av infrastrukturer (IP5.22).
Om ett fordon skulle bli hackat, vad har ni för åtgärder för att hantera detta? **Tomas fick denna liknande fråga: Hur tycker du företag ska hantera en eventuell hackattack av ett eventuellt fordon?**	Vi kan stänga av specifika användare i bilar så de inte lägre kan komma in i eller komma i kontakt med cloudet. Vi har access kontroll om vad som får komma in och då kan vi säga att den bilen uppfyller inte längre säkerhetskraven(IP1.31).	Nä, det vet jag faktiskt inte svaret på. Det här är inte bara en utmaning runt självkörande bilar utan drönare hackas också t.ex. (IP2.27).	Om något händer så var det viktigaste att ta reda på hur bilen har blivit hackad och återskapa händelsen. Man måste utföra tester, man måste automatisera testning så att man hela tiden har automatisk kontroll på hur detta funkar (IP3.42).	X	Jag kan inte svara på exakt hur det går till, jag vet att det finns men jag jobbar inte extra med det (IP5.28).

Fortsättning Tabell 7

Tabell 8: Artificiell Intelligens

Kategorier	IP1	IP2	IP3	IP4	IP5
Anser ni att AI är hjärnan av Internet of Vehicles?	Det är själva kärnan i att bilen kör själv och därav är AI en drivande faktor (IP1.44).	Ja, det kan det vara ja i mång mål. Men det som aktivt är hjärnan är styrsystemen(operatingsystem) på samma sätt som du har iOS i din mobiltelefon eller Android. Det centrala för själva bilen och kalla det hjärnan om du vill men den behöver ett operativsystemet för att fungera och sen innehåller det operativsystemet väldigt mycket AI (IP2.29).	Ja det är det eftersom tittar vi på vår mänskliga hjärna handlar det om intryck hela tiden. Hela denna mjukvaran bygger på matematiska teorier från beteende vetenskap/deep learning (IP3.48).	Inte AI på det sättet. AI för mig är mer om man pratar självlärande system, och det tror jag ligger en bra bit bort om de ska börja lära sig saker och ting själva (IP4.28).	Inte idag, men jag är övertygad om att det kommer bli. Idag är det inget AI som styr infrastrukturen och det är inget AI som deployar (IP5.34).

5 Diskussion

I detta kapitel diskuteras litteraturgenomgången i relation med resultatet från den kvalitativa undersökningen. Här presenteras skillnader, likheter och nyheter som uppstått. För att göra allt så tydligt som möjligt finns det liknande rubriker som använts i både litteraturgenomgången och empirin. Intervjukandidaterna refereras till genom IP och nummer, för att tydligt visa sammanhang till resultatet.

5.1 Metodkritik

På grund av att tiden kring administration med intervjuerna och arbetet efter, har relativt få respondenter intervjuats. Detta så att kvaliteten på resterande delar av uppsatsen inte blev lidande. Det antal intervjuer som utförts i denna uppsats anser vi vara tillräckligt för att få ett högkvalitativt resultat. Intervjukandidaterna var i grunden överens i många frågor men hade unika åsikter till svaren som särskiljer dem åt. Ifall det hade varit fler intervjukandidater hade de kunnat bekräfta resultatet ytterligare eller motsatt det mer. Det hade kunnat ge nya intressanta aspekter på områdena som har behandlats.

5.2 Utveckling av autonoma fordon

Frågan som undersökte hur företag ställde sig till utveckling av självkörande fordon var till för att se hur personer från olika organisationer ser på området. Samtliga intervjukandidater tyckte det var viktigt med utveckling av autonoma fordon och alla hade en positiv inställning till det. De har alla varit involverade på olika sätt som t.ex.

"Acando i Norge är en av de absoluta ledarna på den norska marknaden och vi har pratat en del med Sverige och med Tyskland. Vi har kanske snart möjligheten att genomföra en pilot i Tyskland snart också. Men när det handlar om transport i Norge och autonom körning så pratar man om "Acando-bussen", så vi har en så pass stark position." – IP2.13

IP4 pratade mycket om att när tekniken är mogen så är det rätt väg att gå och nämnde:

"Jag tror att den utvecklingen är jättebra och kommer definitivt vara trafiksäkerhetshöjande. Så att man måste se till att man designar säkerheten på ett bra sätt så man kan lita på funktionerna också." – IP4.8

Tegmark (2017) diskuterar också frågan gällande trafiksäkerhet och menar att med hjälp av AI och självkörande fordon hade 90 % av olyckorna kunnat förhindras.

5.3 Teknik och utveckling

5.3.1 Internet of Vehicles och Vehicle Cloud

Internet of Things är ett brett begrepp som handlar om många olika områden. Fluchter och Wortman (2015) nämnde att Internet of Things kunde appliceras på många olika områden som t.ex. smart transport. Intervjukandidaterna frågades ifall de såg en koppling mellan Internet of Things och Internet of Vehicles, vilket alla gjorde. Alla svarade att på något sätt är IoV och IoT samma sak, då det kan vara vad som helst som är uppkopplat. IP1 nämnde också en skillnad:

"Men det som skiljer Internet of Things från Internet of Vehicles om man nu ska använda sig utav den termen, är att säkerhetsaspekterna och prestandakraven är mycket mycket mycket högre." – IP1.20

Detta var en skillnad som inte Yang et al. (2014) nämner när de diskuterar skillnaderna mellan IoT och IoV. De menar att IoV mer fokuserar på integrationen av människor och fordon till skillnad från vad IoT gör, men de nämner inget om säkerhetsaspekterna. Yang et al. (2014) syftar på att bygga fordonet till ett globalt nätverk som kan leverera tjänster till människor eller andra fordon.

Något som två av intervjukandidaterna tog upp var att IoV inte hade fungerat om inte Cloudet hade slagit igenom. IP5 berättade att kopplingen för IoV är cloudmiljön som alla fordon kommer ansluta sig till. Kaiwartya et al. (2016) berättar att det finns fem olika lager av arkitektur, där molninfrastrukturen faller in under artificiell intelligens lagret som en av byggstenarna för att IoV ska fungera. Vehicle cloud skapas för att kunna skapa samarbeten mellan fordon (Gerla et al., 2012). Gerla et al (2012) hävdar i sin artikel att Vehicle cloud är kärnsystemet som gör denna utveckling möjlig, vilket stödjer de två informanternas svar.

Gerla et al. (2014) berättar att kommunikationen från fordonen till Cloudet skulle kunna fungera med hjälp av arkitektur från VANET. Detta nämnde ingen utav intervjukandidaterna. Tre av dem nämnde däremot att de tror att 5G kommer behövas för att bygga upp en stabil vehicle cloud infrastruktur.

"5G möjliggör bättre kommunikation mellan punkter till skillnad från mot vad det är idag. Så att 5G är väl det som kan förbättra mer. "-IP5.32

Varshney (2005) tar upp att det finns svårigheter med att bygga ett bra Adhoc nätverk på grund av den korta kontakten mellan fordonet och nätverket. Genom att 5G lanseras kanske detta problem försvinner, som IP5 säger att med 5G kommer kommunikationen mellan punkter bli bättre.

5.3.2 Framtida utveckling

Intervjukandidaterna fick frågan om hur det tror utvecklingen kommer se ut framöver. Här svarade de lite olika. IP3 menar att utvecklingen går snabbt och att det bara handlar om en vanesak för oss människor att lita på de självkörande bilarna, medan IP4 snarare menar att allt

kommer ta tid och att det finns många olika problem som måste lösas. Ett exempel som han tog upp var:

"Vi kan titta på fotgängare och ha ögonkontakt med fotgängare, tänker de gå över eller står de med ryggen mot vägen och inse att de inte kommer gå över, men en bil kanske inte har den funktionen. Skilja mellan en fotgängare och en soptunna kan vara ett problem för en bil. Är det en fotgängare som står där eller är det ett annat objekt?" – IP4.20

IP2 berättade att han tror att de autonoma fordonen kommer vara låsta till förutbestämda rutter de närmaste åren och att det redan finns pilottester som körs. IP1 tror att utvecklingen kommer ligga på själva bilen själv genom att någon får lokal access till den medan IP5 tror att vi kommer använda oss utav Micro-services, som handlar om flera mindre tjänster istället för en produkt.

5.4 Säkerhet

5.4.1 Säkerhetsrisker

Säkerhetsrisker med autonoma fordon är högre än med icke autonoma fordon (Gerla et al., 2014). Därför ställs det idag höga krav att höja de säkerhetsstandarder för självkörande fordon som existerar i dagsläget (Lee, 2015-2016). Intervjukandidaternas svar i denna fråga visade sig vara något varierande. IP1 och IP5 ansåg att säkerheten idag är av hög nivå och god kvalitet.

"Jag tycker att det är säkert. Det absolut största fokusområdet som vi har och det kontrolleras ständigt och återkommande."– IP1.22

"Jag anser att de som är ute i skarp produktion definitivt har hög säkerhet."– IP5.17

Övriga respondenter ansåg dock att den säkerhet gällande autonoma fordon som existerar idag har vissa brister. Vi människor måste öka toleransen till dessa fordon och inse att de är säkrare än oss själva. Vilket enligt IP2 kan bli en utmaning när det sker olyckor som med Tesla incidenten som är helt oacceptabelt. IP3 nämnde att säkerheten är branschens största utmaning och att det måste ske ett bättre samarbete mellan tillverkare för att lösa de problem som existerar idag. Något som IP4 hade samtycke i.

"Man måste designa bilen från grunden på ett sånt sätt så att den kan hantera problem, för problem kommer det bli förr eller senare oavsett vad så att då måste man bygga den på ett sådant sätt så att den kan hantera säkerhetsproblem." **–** IP4.17

Putchala och Agarwals (2009) test undersökte maskinernas säkerhet med hjälp av Reverse Turing Test kombinerat med CAPTCHA. Resultatet visade just på att de inte är på den säkerhetsnivå som de bör vara på (Putchala och Agarwal, 2009). Frågan om säkerhet i dagsläget är alltså inte riktigt på den nivån som den bör vara på. Detta påpekar informant 3.

"Varje bil innehåller 119 miljoner rader kod och man räknar med att i en professionell programvara är 5-20 security leaks per 1000 rader kod." – IP3.21

5.4.2 Hot och problem

Det finns mängder av problem och risker som är kopplade till autonoma fordon. Många av dem som utförs av en tredjepartsangripare (Raya et al., 2006). Nätverken som bilarna är kopplade till måste säkras för att förebygga riskerna (Maglaras et.al., 2016). IP4 ansåg att bilen måste skyddas från hackare och kunna stänga av sig själv om en sådan situation skulle uppstå. Dock att detta blir en svår utmaning då hackning är ett stort hot, som inte gäller bara för fordon. IP3 nämnde tre problem som existerar:

"Det består av tre bitar: 1. Kvalitet och att utvecklingsprocessen måste innehålla säkerhet. 2. Organisationerna måste förändra sig. 3. Organisationerna måste drivas via data." – IP3.40

Många problem som existerar rör sig om själva bilen och dess funktioner. Skyddet för dessa måste ökas via fordonets insida (Raya et al., 2006). Även IP1 ansåg att det denna som vi måste skydda i första hand.

"Jag tror att just bilen är nog den mest självklara angreppspunkten."– IP1.28

Ett annat problem som kan uppstå är när autonoma bilar ska blandas med vanlig trafik. IP2 ansåg att detta var ett kortsiktigt problem, men att säkerheten och tillit till teknologin är mer aktuellt. Där kommer myndigheten spela en stor roll. Utdaterade verktyg och infrastrukturer kan enligt IP5 skapa problem. Utvecklingen för dessa går snabbt och där gäller det att väga mellan det som är stabilt, men samtidigt är med i utvecklingen.

5.4.3 Säkerhetsåtgärder

Något som flera av informanterna nämnde var att det är bilen i sig som måste göras säker. Dels att designa bilen utefter säkerheten och vara medveten om de risker som finns för att vara redo när en sådan situation väl uppstår.

"Dels då att designa insidan på ett sådant sätt så de klarar av att hantera, inte om men när det blir något säkerhetsproblem, när något blir hackat och så ska de upptäcka." – IP4.22

Att prioritera access och skydd med hjälp av skyddsstrategier kan höja säkerheten (Gerla et al., 2014). Om ett fordon skulle bli hackat nämnde IP1 att det finns möjlighet att kontrollera accessen för vilka som har tillgång till bilen.

"Vi har access kontroll om vad som får komma in och då kan vi säga att den bilen uppfyller inte längre säkerhetskraven." – IP1.31

Vid en attack nämnde IP3 att man måste lista ut hur detta har genomförts och kunna återskapa händelsen, och även skapa automatiserade tester för att ha en automatisk kontroll. Raya et al. (2016) beskriver vikten av att bygga en säkerhetsarkitektur i fordonet för att kunna övervaka allt som rör sig till och från fordonet, med funktioner som kan lagra data för senare analys.

5.5 Artificiell intelligens

I ett av de fem lagren nämner Kaiwartya et al. (2016) att artificiell intelligens är hjärnan av Internet of Vehicles. Därför kontrollerades det om personer i näringslivet ansåg samma sak. Resultatet blev lite varierande, tre tycker att det stämmer in bra medan två inte håller med. En av de som håller med sa:

"Ja, det är det eftersom tittar vi på vår mänskliga hjärna handlar det om intryck hela tiden. Det är tusentals intryck som en hjärna tar hela tiden. AI reagerar på information, antingen från realtid från en algoritm eller historik. Hela denna mjukvaran bygger på matematiska teorier från beteende vetenskap/deep learning." – IP3.48

Medan en av de som inte höll med sa:

"Inte AI på det sättet. AI är inte ett väldefinierat begrepp. Utan AI för mig är mer om man pratar självlärande system, och det tror jag ligger en bra bit bort om de ska börja lära sig saker och ting själva." – IP4.28

Alan Turing förutspådde att maskinerna år 2000 skulle ha högre intelligens än oss människor, och att vi skulle få svårt att särskilja oss själva från dem (Epstein et.al., 2009). Det Turing förutspådde skulle hända vid år 2000 tycker IP4 år 2018 att det fortfarande finns en del kvar att lära, han säger följande:

"Så att ha ett självlärande system om du nu menar med AI och självlärande, det ligger nog väldigt långt bort om man inte kan garantera vissa saker." – IP4.28

6 Slutsats

Detta kapitel sammanfattar uppsatsens fynd från empirin och litteraturgenomgången. Uppsatsens syfte och forskningsfråga ämnas att uppfyllas i kapitlet. Här förklaras vilka säkerhetsproblem som finns i dagsläget med autonoma fordon och vilka säkerhetsåtgärder som anses bör tas.

I vår studie har vi gjort en omfattande litteraturgenomgång som har lett oss till att förfina vårt ursprungliga definierade problemområde såväl som vår forskningsfråga och vårt syfte. Genom att göra detta har vår studie blivit styrd av två forskningsfrågor, som vi presenterar här följt av svar på dem:

Vilka säkerhetsproblem finns det med autonoma fordon i dagsläget?

Utvecklingen med autonoma fordon går väldigt snabbt och många företag tävlar mot varandra för kunna ligga i framkanten. Detta leder till att säkerheten inte blir prioriterad lika högt och bilföretagen väljer att sälja först och lösa säkerhetsproblemen när de inträffar. Det här visas tydligt i de olika olyckorna som har inträffat den senaste tiden. Som många intervjukandidater nämnt är detta oacceptabelt. Ingen ska behöva gå miste om livet i bilföretagens tävling. Ett annat säkerhetsproblem som intervjukandidaterna nämnde är att det inte finns några standarder eller lagar gällande säkerhet för autonoma fordon i dagsläget.

I de autonoma fordonen finns det mängder rader kod som också har många säkerhetsluckor. Det räcker med att ladda ner en applikation till din mobil eller surfplatta och efter det kan du som tredjepart hacka bilens system. Ifall detta skulle inträffa skulle det kunna påverka informationsflödet upp till cloudet och andra fordon i området som är uppkopplade till samma cloud vid tillfället. Fordonet i sig självt är inte heller säkert mot sådana attacker i dagsläget. Eftersom det autonoma fordonet kommer bli en del av vår vardag behöver dessa problem lösas innan det kan placeras i trafiken.

Vilka åtgärder anser organisationsrepresentanter bör tas för att stärka säkerheten med autonoma fordon i trafiken?

För att lösa ovanstående problem finns det några åtgärder som kan minska dessa. En viktig del kommer vara att skapa gemensamma standarder och lagar för biltillverkare. Det hade även varit bra ifall de hade börjat samarbeta för att lösa nuvarande säkerhetsproblem. Fordonen kommer vara uppkopplade till samma cloud och om ett bilmärke ligger efter med säkerhetsstandarder kan det komma att påverka de andra också och därmed minska säkerheten. Om det finns tydliga lagar och standarder kan detta också bidra till en ökad användaracceptans, då människor tenderar att förlita sig på lagverk. T.ex. om det finns en lag över vilken säkerhetsnivå ett fordon behöver ha för att ha tillgång till cloudet kommer inte de obehöriga in lika lätt och detta får även allmänheten veta då.

Hackning kommer alltid att förekomma och därför måste vi bli bättre på att försvara oss mot det. En lösning kan vara att försöka återskapa attacken för att förstå hur hackarna tog sig in i systemet och för att kunna bygga ett försvar mot det. Bilföretagen bör även ligga steget före

och genomföra olika sorters penetrationstester för att identifiera fordonet svaga punkter och sen kunna stärka dessa.

En säkerhetsåtgärd som kan komma att påverka informationsflödet positivt är användandet av 5G. Med 5G kommer kommunikationen mellan fordonet och cloudet att gå snabbare, vilket gör att realtidsuppdateringarna kommer vara aktuella. Då hade en eventuell attack kunna upptäckas tidigare och då kunna åtgärda säkerhetsrisken genom att ta bort fordonets access till cloudet.

Artificiell intelligens kan komma till användning i framtiden genom att lära sig av beteenden. I dagsläget är det en stor bit av fordonet, AI hade kunnat kallas för hjärnan av autonoma fordon men just nu finns det mycket kvar att lära. Intrycken som en människas hjärna hanterar måste också AI-hjärnan lära sig.

7 Förslag på vidare forskning

Uppsatsen undersöker ett aktuellt och nytt ämne så hade det varit intressant att fortsatt följa utvecklingen då den går snabbt. Ämnet är något som får mer och mer fokus i vårt samhälle och kommer beröra många människor. Som många informanter nämner behövs det standarder. Denna aspekt hade varit intressant att forska vidare inom. Detta för att det kan vara en möjlighet för företag att samarbeta för att stärka säkerheten.

Ett annat område som hade varit intressant att forska vidare inom är att undersöka människors acceptans med mixed traffic. Detta för att utslussningsfasen kommer vara blandad trafik i ett antal år innan alla i samhället har ett autonomt fordon. Det kommer bli intressant att följa denna utveckling framöver då det rör oss alla.

Som tidigare nämnts under Avgränsningar så har vi valt att inte rikta in studien på moral- och etikfrågor. Eftersom att många problem rörande autonoma fordon handlar om användaracceptans hade detta varit ett intressant område att fortsätta forska inom.

8 Appendix

8.1 Intervjuguide till företag

	Bakgrundsinformation
1.	Kan du berätta lite om din bakgrund? Utbildning osv.
2.	Kan du berätta lite om ditt arbete? t.ex. titel.
	Bakgrund gällande företaget och självkörande bilar
3.	Hur ställer sig företaget till utveckling av självkörande fordon?
4.	Arbetar ni något med utveckling av självkörande fordon t.ex. Internet of Vehicles, AI eller Vehicle Cloud?
5.	Om ja på ovanstående: a. Hur kommer det sig att företaget arbetar med utveckling av självkörande fordon?
	Teknik (IoV, Vehicle Cloud, AI)
6.	Ser ni en koppling mellan Internet of Things och Internet of Vehicles?
7.	Hur ser ni på säkerhetsaspekter inom Internet of Vehicles i dagsläget?
8.	Hur tror ni att utvecklingen kommer se ut framöver?
9.	Vad kommer behövas för att stärka säkerheten med Internet of Vehicles?
10.	Vilka hot/problem ser ni som mest aktuella?
11.	Om ett fordon skulle bli hackat, vad har ni för åtgärder för att hantera detta?
12.	Vad tror ni behövs i dagens samhälle för en stabil vehicle cloud infrastruktur?
13.	Anser ni att AI är hjärnan av internet of vehicles?
	Övrigt
14.	Har du någon fråga till oss eller något att tillägga?
15.	Har du något tips på andra personer vi kan intervjua inom området?
16.	Hade vi fått återkomma ifall vi kommer på någon följdfråga?

8.2 Intervjuguide till professor

	Bakgrundsinformation
1.	Kan du berätta lite om din bakgrund? Utbildning osv.
2.	Vi har förstått att du arbetar inom data och informationsteknik området, kan du berätta lite om ditt forskningsområde?
	Teknik (IoV, Vehicles, Cloud, AI) Fundamental?
3.	Hur ställer du dig till utveckling av självkörande fordon?
4.	Ser du en koppling mellan Internet of Things och Internet of Vehicles?
5.	Hur ser du på säkerhetsaspekter inom internet of Vehicles i dagsläget?
6.	Hur tror du att utvecklingen kommer se ut i framtiden?
7.	Vad kommer behövas för att stärka säkerheten med Internet of Vehicles?
8.	Vilka hot/problem ser du som mest aktuella?
9.	Hur tycker du företag ska hantera en eventuell hackattack av ett eventuellt fordon?
10.	Vad tror du behövs i dagens samhälle för en stabil vehicle cloud infrastruktur?
11.	Anser du att AI är hjärnan av Internet of Vehicles?
	Övrigt
12.	Har du någon fråga till oss eller något att tillägga?
13.	Har du något tips på andra personer vi kan intervjua inom området?
14.	Hade vi fått återkomma ifall vi kommer på någon följdfråga?

8.3 Intervjuer

8.3.1 Intervju 1- IP1

Intervjuare: Susanna Nirvald (SN)
Sekreterare: Fanny Tapper (FT)
Verksamhet: Företag Z
Intervjuperson: Informant1
Yrkesroll: Developer
Tid och plats: 10.30–10.50, måndagen den 24 april 2018, Telefonsamtal från Lund

Referens nr.	**Person:**	**Frågor och svar:**
IP1.1	SN:	Går det bra om vi spelar in intervjun?
IP1.2	Informant1:	Absolut!
IP1.3	SN:	**Kan du berätta lite om din bakgrund? t.ex., Utbildning osv**
IP1.4	Informant1:	Ja, jag är utbildad i elektroteknik på Chalmers. Så efter utbildningen så gick jag vidareutbildningar och grejer och sen så hamnade jag på Ericsson som konsult via Sigma, och jobbade med mobile dropbands och sen gick den avdelningen till att bli, jobba med IoT och då blev det mer utveckling. Jag var där i 7 år tror jag och sen lade de ner den avdelningen och då gick jag vidare till Zenuity och var där i tre månader som konsult innan jag blev anställd på Företag Y där jag jobbar som utvecklare på CVC som är connected vehicle cloud.
IP1.5	SN:	**Vad har du för titel?** Det kan vara bra för oss att ha med i uppsatsen.
IP1.6	Informant1:	Developer är jag.
IP1.7	SN:	**Hur ställer sig företaget till utveckling av självkörande fordon?**
IP1.8	Informant1:	Det är väldigt viktigt för oss. Vi jobbar med, det är ju ett stort företag men primärt är vårt huvudfokus ju radiobasstationer för mobiler, det och 5G. Och 5G är ju nästa generation då, det är väldigt viktigt för oss att 5G går bra, och 5G är väldigt viktigt för självkörande bilar.
IP1.9	SN:	Precis, för att det ska funka.
IP1.10	Informant1:	Även IoT och industrin då, det är väldigt viktigt för oss att detta går bra.
IP.1.11	SN:	**Arbetar ni något med utveckling av självkörande fordon t.ex. Internet of Vehicles, AI eller Vehicle Cloud?** Det har du nämnt lite om.
IP1.12	Informant1:	Ja, jag sitter på avdelningen som heter CVC som är connected vehicle clouds. Så vi gör, utvecklar cloud infrastruktur för biltillverkare och Volvo är ju en stor kund som vi har haft länge då.
IP1.13	SN:	Ja, precis dom har ju lanserat nu i Göteborg, nivå 4 bilar har vi läst till oss.

IP1.14	SN:	**Hur kommer det sig att ni hoppade på denna utveckling från början? Med själva självkörande bilar, för det har gått ganska snabbt nu de senaste åren. Hur kommer det sig att företaget arbetar med utveckling av självkörande fordon?**
IP1.15	Informant1:	Från början så var det mer Volvo, och vi började ett samarbete. Framförallt handlar det om, i början var det mest media och grejer för tjänster runt bilen som att du har en APP som du kan sätta på värmen i bilen och du kan göra såna grejer som att se var bilen är och hur långt bilen har gått osv. Det var mest sådana tjänster som det började med.
IP1.16	SN:	Ja, precis!
IP1.17	Informant1:	Och där har vi varit med länge och är, men nu är det mer logik för självkörande bilar och kartor och så vidare. Så det är egentligen bara en utveckling av det som vi har jobbat med länge.
IP1.18	SN:	Bra!
IP1.19	SN:	**Ser du en koppling mellan Internet of Things och Internet of Vehicles?**
IP1.20	Informant1:	Ja, jag tycker att det i stort sett är samma sak, bilen är en Thing liksom. Men det som skiljer Internet of Things från Internet of Vehicles om man nu ska använda sig utav den termen, är att säkerhetsaspekterna och prestandakraven är mycket mycket mycket högre. Så att det är mycket säkerhet och det ska vara robusta lösningar.
IP1.21	SN:	**Hur ser ni på säkerhetsaspekter inom Internet of Vehicles i dagsläget? Anser du t.ex. att det är säkert?**
IP1.22	Informant1:	Ja det tycker jag att det är. Det är absolut största fokusområdet som vi har, sådant som kontrolleras ständigt och återkommande. FöretagY Research gör penetrationstester och så vidare. I det här fallet då har FöretagY Research i uppdrag att försöka penetrera våran säkerhetslösning.
IP1.23	SN:	Aha, så man testar ifall någon i så fall skulle t.ex. hacka det eller ta sig in i informationsflödet?
IP1.24	Informant1:	Precis!
IP1.25	SN:	**Hur tror ni att utvecklingen kommer se ut framöver?** I och med att det expanderas hela tiden, måste det också byggas på, med tanke på hackning och så vidare.

IP1.26	Informant1:	Vi har certifikatlösningar med bilen, största fokus kommer nog ligga på bilen sig självt och om någon får kontrollen över den om man får lokal access till bilen. Där tror jag att det största jobbet kommer ligga framöver. Det andra får ni prata med biltillverkarna om, jag tycker ni kan ringa och prata med t.ex. Zenuity eller Volvo.
IP1.27	SN:	**Vad kommer behövas för att stärka säkerheten med Internet of Vehicles?** Finns det något mer specifikt? Du nämnde tidigare det med platsbaserat.
IP1.28	Informant1:	Den största angreppspunkten är bilen självt, sen är det alltid kommunikationen men den är skyddad i sig. Men jag tror att just bilen är nog den mest självklara angreppspunkten.
IP1.29	SN:	Okej då har du nästan svarat på nästa fråga så vi hoppar över till nästa.
IP1.30	SN:	**Om ett fordon skulle bli hackat, som du nämnde tidigare med ex, penetrationstester, vad har ni för åtgärder för att hantera detta?**
IP1.31	Informant1:	Vi kan stänga av just specifika användare i bilar så de inte lägre kan komma in i eller komma i kontakt med cloudet, så det går att styra. Vi har liksom access kontroll om vad som får komma in och då kan vi säga att den här bilen uppfyller inte längre säkerhetskraven.
IP1.32	SN:	Aha, så då blir den spärrad från att komma in till cloudet?
IP1.33	Informant1:	Precis! Det kan göras certificate remove på bilen då.
IP1.34	SN:	**Vad tror ni behövs i dagens samhälle för en stabil vehicle cloud infrastruktur?** Du pratade tidigare om t.ex. 5G punkter osv? Är det som du tycker är viktigast?
IP1.35	Informant1:	5G tycker jag är mycket viktigt. Men sen en annan grej är som är mycket viktigt är att sätta standarder för när bilarna börjar köra själva. Då måste bilarna kunna prata med varandra och det kommer inte vara av samma bilmärke. Det är viktigt att sätta en standard för hur bilarna ska kunna kommunicera och hur clouden ska kunna kommunicera för olika tillverkare.

IP1.36	SN:	Det är det vi har tänkt på också, då alla arbetar med detta just nu och det är väldigt aktuellt. Hur ska man få alla att samarbeta? T.ex. om det sker en trafikolycka längre fram och så ska alla som ligger efter få samma information med olika märken.
IP1.37	Informant1:	Precis! Det är det blir en stor utmaning då, då måste man standardisera protokollet så att de kan kommunicera via cloudet.
IP1.38	SN:	Är det något du vet om de arbetar med just nu i t.ex. Sverige?
IP1.39	Informant1:	Sverige är en liten marknad, men i EU och så vidare. Eller någon standardiseringsorganisation som tar det, men det jobbas med det absolut. Jag är inte så insatt i just hur det går. Vi jobbar inte med det absolut.
IP1.40	SN:	Ja, vi har läst att USA ligger lite längre fram när det gäller detta än i Europa. Där har de testat en del.
IP1.41	SN:	**Anser ni att AI är hjärnan av Internet of Vehicles?**
IP1.42	Informant1:	Jag förstår inte riktigt frågan hur AI, är det Artificiell Intelligens?
IP1.43	SN:	Precis! Vi har hittat lite i några vetenskapliga artiklar att de är många som hävdar att de tycker att det är det och därför skulle det vara lite intressant att veta om personer som verkligen jobbar med det också tycker det eller om de tycker att något annat är huvudpunkten.
IP1.44	Informant1:	Nä men asså, det är ju själva kärnan i att bilen kör själv och då är det AI en drivande faktor.
IP1.45	SN:	Så bra!
IP1.46	SN:	**Har ni någon fråga till oss eller något att tillägga?**
IP1.47	Informant1:	Nej, inte som jag kan komma på rak arm.
IP1.48	SN:	Okej, så bra!
IP1.49	SN:	**Har ni något tips på andra personer vi kan intervjua inom området?**
IP1.50	Informant1:	Zenuity, det är ett samägt bolag mellan Volvo och Autoliv. Som gör utveckling av självkörande bilar.

IP1.51	SN:	Aha coolt, det har vi faktiskt inte hittat någonting alls om. Jättebra.
IP1.52	Informant1:	Ja sedan kan ni även prata med Autoliv, de jobbar också med aktiv säkerhet och AI.
IP1.53	SN:	Ja, jättebra!
IP1.54	SN:	**Hade vi fått återkomma ifall vi kommer på någon följdfråga som kan vara viktig för uppsatsen?**
IP1.55	Informant1:	Absolut, det är bra att höra av sig
IP1.56	SN:	Jättebra. Måste dubbelkolla vill du vara anonym i uppsatsen eller hur känner du?
IP1.57	Informant1:	Ja, gärna!
IP1.58	SN:	Vad bra, vi måste alltid dubbelkolla så att folk får valet att vara det ifall de vill. Fanny har du något att tillägga?
IP1.59	FT:	Nej, jag tycker att det varit jättebra svar
IP1.60	SN:	Tack så jättemycket för hjälpen!
IP1.61	Informant1:	Ingen fara! Ni får jättegärna skicka resultatet av uppsatsen när ni blir färdiga.
IP1.62	SN:	Absolut, det ska vi göra. Vi hoppas verkligen att det ska bli bra. Det är många som har börjat bli intresserade av det, så det är väldigt kul!
IP1.63	Informant1:	Det förstår jag, det ligger i tidens anda!
IP1.64	SN:	Det känns spännande att vi lyckades få tag i detta ämne, ingen annan som riktigt skriver om det. Det blir jättebra! Stort tack för hjälpen. Så skickar vi allt till det senare. Ha det så bra!
IP1.65	NL:	Detsamma, tack hej!

8.3.2 Intervju 2- IP2

Intervjuare: Susanna Nirvald (SN)
Sekreterare: Fanny Tapper (FT)
Verksamhet: Acando Norge
Intervjuperson: Jone Løvvik
Yrkesroll: SVP & Head of Strategic Programs

Tid och plats: 15.00–15.30, tisdagen den 25 april 2018, Telefonsamtal från Lund
Obs! Intervjukandidaten pratar norska därav vissa svar lite annorlunda.

Referens nr.	**Person:**	**Frågor och svar:**
IP2:1	SN:	Hej är allt bra med er?
IP2:2	JL:	Jag här är det bra. Det är accurativt, vi har väldigt mycket aktiviteter nu för tiden. Så det är mycket!
IP2:3	SN:	Va roligt, ska vi köra då?
IP2:4	SN:	**Kan du berätta lite om din bakgrund? Utbildning osv**
IP2:5	JL:	Det kan jag, min bakgrund/utbildning är informatik och info-data från ett universitet i Oslo. Jag en till åren kommen man så jag har jobbat 30 år i branschen, i stort sett jobbat inom mer konsultbranschen och rådgivare som sådan, både internationellt och i lokala sammanhang.
IP2:6	SN:	Aha, intressant!
IP2:7	SN:	**Kan du berätta lite om ditt arbete t.ex. titel osv?**
IP2:8	JL:	Jag jobbar i stort sett med strategi och förbättringsutveckling knytet till vår teknologi och digitalisering, som driver förändringen. Jag ansvarar för en enhet i Acando som är Acando management consulting, ansvar för som vi hos oss så kallar för det strategiska program, som går ut på att tvärsta alla kapabiliteter vi har. Ett av de programmen är smart city, där vi har ett team som jobbar primärt med smart mobility. Det handlar mycket om ITS alltså intelligent transportsstyrning, och väldigt mycket om autonom körning. Men sätt då, så är en smart city en samling så vi jobbar också mycket med arkitekter och andra som ska utveckla våra städer framöver och se på hur teknologi med smartare fordon hur man planlägger och man bygger städer framåt.
IP2:9	SN:	Vad intressant!
IP2:10	SN:	**Hur ställer sig företaget till utveckling av självkörande fordon?**
IP2:11	JL:	För oss, man kan säga den rollen vi har kan jag berätta lite om. Hit by coincidence så tog vi i Acando Norge, var de första som tog in självkörande minibuss till den norska marknaden. Det fick vi mycket uppmärksamhet runt det, vi har i cirka 2-3 år nu har vi primärt kört det vi kallar demonstrationer, det vill säga att man har kört sole case på dessa bussarna, vi har varit i 14 städer i Norge. Vi har även vart i Sverige faktiskt en tur, där man har testat bussen och sett på den och sådant. Parallellt med det har vi jobbat med kunder, var vi dels har jobbat med vad vi kallar för “möjlighets studier”, vad kan autonom

		transport betyda? Vi har jobbat med norska posten, vi har jobbat med flera olika kunder. Vi har jobbat med många olika aktörer i så kallade fordonsbranschen, där vi har sett på nya förändringsmodeller som kan utvecklas knytet till autonom transport. Där snackar vi om robottaxi eller att alla transporter blir olika tjänster och att folk inte längre äger sina fordon själva. Vilka förändringsmodeller som tas fram, och vilka typer av branchspridning som sker och alltså hur ska man förhålla sig till t.ex. Uber vad kommer de att göra på den lokala marknaden. Vad gör en aktör som Volvo som introducerar något som "Volvo Care" som de har jobbat ganska mycket med autonoma bilar? Vad gör sällskap som Hertz? Avis och dem, hur kommer de positionera sig i detta? Vad betyder det för bilimpoirtörer och försäljare? Ganska intressant dynamik, som inte är så lätt att förutse men som vi har försökt att guida lite i. Det har vi gjort ett tag nu. Vid ingången av 2018 så var det flera europeiska länder t.ex. Sveriges har ändrat sitt lagverk som gör att man kan starta provkörning av piloter. I Sverige har du en pilot gående i Kista bland annat, som du säkert känner till. I Norge håller vi på att förbereda de första piloterna, där går Acando roll i det är att vi är systemintegrator, vi har rådgivning med dem och har relation med de olika aktörerna och känner till de lagverk som har auktoritet som kan producera och leverera denna typ. Så vi sätter samman det med kunden för att få genomföra en pilot. Det är vår roll i kort, i ett längre perspektiv, så ser vi också robot på hjul och det finns en hel del teknologi kopplat till det, och det ska också finnas en del stödsystem knytet till det här. Vår motivation är att se om det kan vara ytterligare intressanta saker för oss, men vi är i fortfarande ett konsultföretag som gör arbete på projekt, vi är inte produktleverantörer och kommer inte vara det utan vi har ett strategiskt partnerskap kan man säga.
IP2:12	SN:	Låter jättespännande, visste inte om att Acando jobbat med detta fören efter Peter tipsade om det.
IP2:13	JL:	Acando i Norge är en av de absoluta ledarna på den norska marknaden och vi har pratat en del med Sverige och med Tyskland. Vi har kanske snart möjligheten att genomföra en pilot i Tyskland snart också. Men när det handlar om transport i Norge och autonom körning så pratar man om "Acando-bussen", så vi har en så pass stark position.
IP2:14	SN:	**Ser ni en koppling mellan Internet of Things och Internet of Vehicles?**
IP2:15	JL:	Ja det gör jag! Alla ting kommer vara knutna till internet och inte minst fordon. Nästan alla de rikaste sällskapen i världen jobbar med autonomisk körning, du har alla de stora teknologiföretagen som Google, Apple, Amazon, kanske inte Facebook men icke minst de kinesiska aktörerna som Alibaba, Tensen, Vainu, IBM. Alla de stora teknologiföretagen jobbar nu med teknologi kopplat med autonomisk

		körning. Man undra också om någon utav dessa teknologiaktöererna kan säkert tänkas introducera produkter som kan köra sig självt. Vi tror inte att de säljer, men det kan vara Apple som är närmst. Du har ju sällskap som Tesla, och som tillägg har du alla de stora bilproducenterna, som Volkswagen, japanska och amerikanska aktörer gör mycket både inom det vi kallar electric connected och autonomous cars. Så det handlar mycket om elektricitet och connected och då kommer du in på Internet of Vehicles. Det är en viktig utveckling. Det sker väldigt mycket utveckling i de ledande teknologi länderna nu för tiden nämligen Kina, och det är mycket vi inte vet över detta. När det gäller historien på teknologin t.ex. när PC:n kom var det många operativsystem och styrsystem från olika företag främst 2, Microsoft och Apple. På mobiltelefon skedde samma sak flera aktörer med liknande operativsystem. Nu är det i regel två, Android med Google och Apple. Vi tror att det samma kommer ske i samband med bilar och smarta hem. T.ex. Google osv. positionerar sig där de önskar att producera bilar men de önskar att ta styrsystemen för det är ingången till Internet of Vehicles och in mot Internet of Things. De är de ledande teknologi aktörerna utvecklar teknologi med allt runt att vara en connected car och det finns två områden, allt om teknologin runt fordonet, det vill säga allt du kan göra inuti bilen och teknologin som handlar om att de ska uppföra sig tryggt runt om i världen. Det är definitivt en självklar koppling och vissa autonoma bilar är som robotar på hjul, och tidigare hette det även smarttelefon på hjul och de följer samma logik i teknologi och utveckling.
IP2:16	SN:	**Hur ser ni på säkerhetsaspekter inom Internet of Vehicles i dagsläget?**
IP2:17	JL:	Det är en definitionsfråga. Det man kan säga om självkörande fordon är att idag är de säkrare än vi människor är.
IP2:18	SN:	Ja, precis!
IP2:19	JL:	Men toleransen/accepten på fel är mycket mindre på maskiner än människor. Som när du får såna situationer som med denna Tesla olycka, så är det väldigt oacceptabelt. Så det är ändå kopplat med säkerhet. Man pratar om de olika autonoma nivåerna, som du kanske känner till så är det ingen som är på nivå 5 ännu, men då är det ganska säkert. Men de vill ju alltid vara som det är med alla typer av sådan teknologi att de vill alltid vara säkert. Men de är betydligt viktigare än men manuellt eller mänskligt opererade.
IP2:20	SN:	**Hur tror ni att utvecklingen kommer se ut framöver?**
IP2:21	JL:	För det första så finns det nu minibussar och små bussar som t.ex. i Kista och det är väl de som har kommit längst med autonomi. Så vi tror att de närmaste 1-2 åren så vill det vara den typen autonoma fordon som används på klara förutbestämda rutter. De vill säga att jag

		tror det är lite längre fram men för ett område så går det fortare än det vi har tänkt oss. Om du kan tänka dig ett par år fram att du ska kunna ta upp din APP och säga till din autonoma bil vart du vill bli hämtad, sätta dig i bilen och berätta vart du vill sen åka och bli körd dit. Det är den ekonomiska tyngdkraften och de rikaste länder bedriver utvecklingen. Så det är det som gör att sakerna kommer fram lite snabbare än vad som tänkt. Det kommer flera områden t.ex. lastbilar och stora lastkörningsbilar i USA. Tesla har kommit med en elektrisk lastbil som delvis är autonom, där fler lastbilar styrs och körs efter varandra. Mer eller mindre sammankopplade.
IP2:22	SN:	Det läste vi något om att Scania också arbetar med.
IP2:23	JL:	Väldigt intressant område, och kommer utvecklas mycket på bara ett par år. Om man tänker på privatbilar eller en vanlig bil har nu väldigt många av de ledande aktörerna har om man t.ex. ser på Volkswagen som har något som kallas Cedric, så ser du lite vad som kommer ske kanske 2021, 2022 kanske ända till 2025 beror lite på men detta kommer att ske. Sen beror det lite på timingen, för det ska kopplas till säkerhet och kontrollsystem också så att det är på plats för att detta ska fungera ute i trafiken.
IP2:24	SN:	**Vilka hot/problem ser ni som mest aktuella?**
IP2:25	JL:	Alltså det kortsiktiga är hur vi ska blanda autonomiska fordon in i blandad trafik, om man ser hur vi kör idag så är det en utmaning. Det är enklare att köra autonomisk trafik där de endast kör i låsta områden, eller områden bara för de autonomiska fordonen t.ex. som för flygplan och näringsområden. Att detta skulle fungera tillsammans med vanlig trafik. Det är en kort utmaning! Sen kommer det att vara mycket runt säkerhet med trygghet mot teknologi, och här är det alla möjliga frågor som kommer upp allt från personvärde till hur teknologin i sig själv fungerar. Och sen är det oss människor och vår acceptans/förståelse och tillit för att denna teknologin ska kunna fungera. Myndigheten har en stor roll och vill nog hålla igen lite. Det har varit en del tester främst i USA och Asien och en del i Europa.
IP2:26	SN:	**Om ett fordon skulle bli hackat, vad har ni för åtgärder för att hantera detta?**
IP2:27	JL:	Nä, det vet jag faktiskt inte svaret på. Det här är inte bara en utmaning runt självkörande bilar, drönare hackas och tas kontroll över. Detta är en del av något vi inte har trygghet att svara om för att vi ska acceptera fullt ut autonomisk körning, i alla fall i mixed traffic.
IP2:28	SN:	**Anser ni att AI är hjärnan av Internet of Vehicles?**
IP2:29	JL:	Ja, det kan det vara ja i mång mål. Det är ju en stor del av AI och machine learning teknologier men det är också flera typer av teknologier inne i det här. Men AI och machine learning är väldigt

		centralt, så ja det kan man säga. Men det som aktivt är hjärnan är styrsystemen(operatingsystem) på samma sätt som du har iOS i din mobiltelefon eller Android. Det centrala för själva bilen och kalla det hjärnan om du vill men den behöver ett operativsystemet för att fungera och sen innehåller det operativsystemet väldigt mycket AI
IP2:30	SN:	**Har ni någon fråga till oss eller något att tillägga?**
IP2:31	JL:	Inte direkt men kanske, det vårt team diskuterar om hur detta kommer gå och hur långt. Kommer vi inte köra bil själva i framtiden? Det vi tror att det kommer drivas mycket till det som är knutet till det urbana, så att på landsbygden men kollektiv, lång transport, och smart city tankegången med grönare stad. Det är en kombination av det elektriska och det här och en av utmaningarna idag som är knutet med privatbilism, är att en privatbil står cirka 90-95% av tiden stilla. Det drivs av det att kunna utnyttja denna access på ett bättre sätt och kanske göra det autonomt eller att göra transportsektorn mycket mer tjänsteorienterat. Att du köper en transport som en tjänst istället med autonoma bilar, du får lättare tillgång och denna accessen kan utnyttjas mer än det vi gör idag. Det är en ganska viktig poäng som en drivkraft knutet till framväxt av autonomiskt transport.
IP2:32	SN:	**Hade vi fått återkomma ifall vi kommer på någon följdfråga?**
IP2:33	JL:	Ja gör det!
IP2:34	SN:	Vill du vara anonym i uppsatsen eller går det bra att nämna ditt namn och Acando i uppsatsen?
IP2:35	JL:	Det går bra med namn och företag.
IP2:36	SN:	Okej, vad bra! Då tror jag vi tackar för oss, stort tack för att du ville vara med!
IP2:37	JL:	Lycka till och ni har valt ett jätteintressant ämne. Jag har jobbat i IT-branschen länge och det är väldigt aktuellt just nu. Det finns många stora teknologimässor i världen och en av de största i Las Vegas har de tidigare åren handlar om t.ex. mobiler osv men de senaste två åren har självkörande bilar totalt dominerat mässan. Det tar över hela IT världens fokus och det läggs väldigt mycket pengar på detta just nu.
IP2:38	SN:	Stort tack verkligen och hör av dig ifall du har några frågor!
IP2:39	JL:	Det är bara att höra av er ifall ni har några frågor och lycka till igen!

8.3.3 Intervju 3- IP3

Intervjuare: Susanna Nirvald (SN)
Sekreterare: Fanny Tapper (FT)

Verksamhet: Företag X
Intervjuperson: Informant3
Yrkesroll: Senior Software Consultant
Tid och plats: 10.30–11.10, onsdagen den 25 april 2018, Telefonsamtal från Lund

Referens nr.	**Person:**	**Frågor och svar:**
IP3:1	SN:	**Kan du berätta lite om din bakgrund? Utbildning osv**
IP3:2	Informant3:	Ja ska jag göra det enkelt så kan man säga att jag har 3 Masters. Jag har master i matte, jag har master i computer science och jag har master i fysik. Sen har jag en fyllis? i teoretisk fysik.
IP3:3	SN:	Aha oj! Det var inte dåligt!
IP3:4	Informant3:	Nej, men det är väl så att Matematik har genomsyrat det jag håller på med och ska man hålla på med det som jag håller på med så måste man vara intresserad av matematik.
IP3:5	SN:	**Kan du berätta lite om ditt arbete t.ex. titel osv?**
IP3:6	Informant3:	Ja, det är lite annorlunda idag i jämförelse med vad jag har gjort innan. Innan har jag drivit större utveckling för organisationer och jobbat som director advice för företag. Så idag är det beroende på när jag flyttade hem från Tyskland så fanns inte så mycket jobb här nere i Skåne, här finns inga jobb för mjukvara. Det är bara enklare konsultjobb, och det enda som fanns var i Stockholm och jag pallar inte ligga och pendla en gång till arbetet.
IP3:7	SN:	Ja, det kan jag förstå! Men vad arbetar du med idag?
IP3:8	Informant3:	Idag jobbar jag med security. Jag jobbar med GDPR, privacy by design och i Privacy och sedan hjälper jag organisationer att bli agila. Om man tar det väldigt kortfattat.
IP3:9	SN:	**Hur ställer sig företaget till utveckling av självkörande fordon?**
IP3:10	Informant3:	Ja, Volvo gör vad de kan för att försöka rekrytera mig, men jag vägrar. Jag tycker det är kul men det är ingen annan som har gjort det som jag har gjort innan i företaget. De flesta andra är traditionella konsulter. Jag kommer från hårdvara och programmering, reallity system/inbyggda system. Det är det som jag har hållit på med innan jag blev ledare för utvecklingsteam. Det är ingen annan som har det på företaget.

IP3:11	SN:	Jaha, det är alltid kul att vara eftertraktad.
IP3:12	Informant3:	Ja, jag är en liten annorlunda typ.
IP3:13	SN:	**Arbetar ni något med utveckling av självkörande fordon t.ex. Internet of Vehicles, AI eller Vehicle Cloud?**
IP3:14	Informant3:	Nej, det är ingen som har kompetensen till det, mer än jag men jag vill inte utveckla igen. Jag har skrivit mina miljoner rader kod och det vill jag inte göra igen. Jag vill driva och leda team. Men däremot så jobbar konsulter med Volvo när det kommer till internet security, patent och sådana bitar.
IP3:15	SN:	**Ser ni en koppling mellan Internet of Things och Internet of Vehicles?**
IP3:16	Informant3:	Internet of Vehicle är egentligen en större form av Internet of Things, så det är egentligen samma grej. Att någonting kommunicerar från en bil eller från en diskmaskin eller en brödrost det är ingen skillnad. Det är bara det att är det enormt mycket mer större datamängd, jag kommer till det i de andra frågorna. Allting har möjliggjorts genom att man kan använda Cloudet idag. Hade inte Cloudet gått igenom så hade man aldrig kunnat använda artificiell intelligens. Vi hade aldrig kunnat göra de här grejerna som vi gör idag.
IP3:17	SN:	Ja, det är väldig häftigt!
IP3:18	Informant3:	Ja, det är mycket kod i en bil, kommer ni få höra sen.
IP3:19	SN:	Ja, det har vi förstått när vi har tittat lite på det
IP3:20	SN:	**Hur ser ni på säkerhetsaspekter inom Internet of Vehicles i dagsläget?** känner du att det verkar säkert? hade du kunnat lita på det?
IP3:21	Informant3:	Det är branschens största utmaning, säkerheten. Eftersom att man ska vara klar över att bilen är en ingenjör, den härstammar från ingenjörs sidan. Mjukvarusidan har brottats med säkerhet i 20 år. Det ingenjörsföretagen har är svårt att locka med, de sockrar med vad som helst om du är en duktig utvecklare för. Det är en aspekt av det. Det är svårt att hitta den typen av människor, mer egentligen traditionellt gammaldags programmeringskunskaper som man måste ha. Varje bil innehåller 119 miljoner rader kod och man räknar med att i en professionell programvara är 5-20 security leaks per 1000 rader kod. Då kan du förstå att det är en liten utmaning. För security

		idag är inte bara hur du designar, bygga protokoll och hur du komprimerar datan, utan det är helt enkelt hur du skriver kod. Och det är det stora problemet är att utvecklare idag inte har den kunskapen. Du måste vara hardcore programmerare, du måste kunna exakt hur data och operativsystem fungerar, hur det fungerar och skriva effektiv kod om du vill kunna jobba inom bilindustrin och IoT. Det är en helt annan typ av programmering skillnaden är att en människa dör i ena fallet och överlever i det andra fallet. Det handlar helt enkelt om hur bilen använder sin drivkraft, fungerar inte det och det är för lång responstid så kommer inte bilen hjälpa människan att ta sig fram, då kommer bilen köra iväg med föraren istället. Så det är en helt annan typ av programmering. Man ska gilla matematik och man ska gilla att sätta sig in i vad som verkligen händer i ett operativsystem, det är därför det är så svårt att hitta folk. Om du utvecklar en webbtjänst idag som laddar på 30 millisekunder i svarstid på en hemsida så tycker du säkert det är bra svarstid eller?
IP3:22	SN:	Ja, det är det ju ändå snabbt.
IP3:24	Informant3:	I min värld är det fyra varv runt jorden, 16 middagsträffar osv. Så långsamt tycker jag att det är, det är bara för att du ska förstå skillnaderna när vi resonerar.
IP3:25	SN:	Man har aldrig tänkt på att det ska gå så snabbt, det är ju löjligt.
IP3:26	Informant3:	Ja, det finns ju massa olika teorier som ni säkert har läst som t.ex. design principer och design pattern. Det är skillnad mellan den programmering som ni kommer i kontakt med och den typen som behövs för denna typ av teknik.
IP3:27	SN:	Jättebra att du nämner detta, för man tänker inte att man behöver så mycket till det och vi kommer kunna lyfta upp detta med säkerheten i uppsatsen.
IP3:28	Informant3:	Säkerhet är den största utmaningen. En grej som också är kopplat till säkerheten är att varje bilföretag försöker lösa ett problem, medan egentligen sitter alla med samma problem. Att sno en bil eller kapa en bil idag, man kan man ladda ner kod på internet och så har jag kapat vilken bil som helst så enkelt är det.
IP3:29	SN:	Ja, den är lite obehaglig
IP3:30	Informant3:	Jag måste veta det annars kan jag inte utveckla något som jag är säker på. Men då sitter BMW, Mercedes, och allihopa och löser problemen var för sig istället för att samarbeta. Medan Volvo

		de har startat ett bolag som anställer ca 500 personer nu i Göteborg. Detta kan vara intressant för er att all mjukvara till China och Volvo byggs på Volvo i Göteborg. Zenuity heter företaget och de försöker jobba med en plattform som ska bli gemensam för alla i hela bilindustrin. Det är kanske lite att sikta högt men det är nästan dit vi måste gå. Det vill säga att du måste börja standardisera.
IP3:31	SN:	Jätte häftigt!
IP3:32	SN:	**Hur tror ni att utvecklingen kommer se ut framöver?**
IP3:33	Informant3:	Utvecklingen går fruktansvärt snabbt! Asså utvecklingen ligger före oss, du ska inte vara förvånad om vi redan har fullt fungerande självkörande bilar redan. Om man nu gillar det vilket jag inte gör. Men det kommer inte dröja mer än 5 år innan detta vi börjar se mer av detta. Det finns redan idag exempelvis i Asien och i andra delar av världen självkörande varuhus t.ex. som åker omkring som människor drar sitt kort och köper saker från varor och sen går de in igen. De här rullande varuhusen, de lär sig hur de ska anpassa sina vägar efter vad människor köper genom att använda artificiell intelligens. Det finns i stor skala i t.ex. Asien.
IP3:34	SN:	De har ju nu den lilla självkörande bussen i Kista, som testkörs. Och det är ju mycket mer än vad man tänker som som kör själv.
IP3:35	Informant3:	Sen idag den självkörande kapaciteten som finns i bilarna idag den är lite märklig. Det handlar om en vanesak för människor att lita på den här självkörande/självverkande bilen. Det man ska vara klar över är att de här datorerna i de Artificiella mjukvaran är bättre än vad människan är. Däremot finns det moraliska och etiska dilemman som mjukvaran måste ta hänsyn till, inklusive försäkringsmässiga problem. Ex om du är ute och kör, ska jag köra ihjäl föraren eller ska jag köra ihjäl kvinnan och barnet i barnvagnen. Det är den diskussionen man måste tänka sig. Men i teorin så är det så att mjukvaran slår människan om man ska slå ut det i över 1000 bilar. Men i enskilda fall så kommer naturligtvis mjukvaran fallera. Det kräver en komplex uppsättning med en självkörande bil det är därför det är så många rader kod. Utvecklingen kommer och det är liksom inget vi kan göra någonting åt. De flesta vet inte vad det innebär om man inte har jobbat med det. men utvecklingen ligger längre fram än egentligen vad ni ser, den ligger långt framme. De som tävlar de här stora bilföretagen som t.ex. Mercedes, Audi de kommer köra över Tesla eftersom de vet hur man bygger en bil. De här bilföretagen ligger och lurar en på

		axeln. Det kommer sen med tekniken och batteritekniken. Det är ett enda stort maktspel i bakgrunden.
IP3:36	SN:	**Vad kommer behövas för att stärka säkerheten med Internet of Vehicles?**
IP3:37	Informant 3:	Folk måste, som det är med allt annat man måste träna. Som t.ex. när du spelar fotboll och lär dig trixa du måste kunna alla mönster och rutiner. Säkerheten måste in redan i processen i när man ska bestämma vad mjukvaran göra, till hur man ska testa den och utvärdera den och hur man ska säkra upp dem. Säkerhet måste in i hela utvecklingsprocessen det är det första, så man måste designa för säkerhet från början! Man måste designa utifrån säkerheten, det andra är att man måste ha duktiga kodare, annars blir det inte säkert. Jag pratar mycket om kod, men det är kod som kommer avgöra kvaliteten. Den kommer helt avgöra kvaliteten, så det kvittar vad du har för design patterns osv. Utan det är koden och kvaliteten på koden som kommer avgöra. Det kan vara jätteenkla programmeringsfel som människor gör men som skapar öppningar för hackare, för hackare är duktiga. Vi har folk som jobbar med att ta sig in i system alltså beställningsjobb för att utvärdera säkerheten. Så att det måste få en annan push. Jag tror att det kommer bli bättre om folk på teknik och bilföretagen samarbetar för att hitta och skapa standarder. För då kan de hjälpas åt att göra det säkrare tillsammans. Det funkar inte att 10 man i ett fotbollslag spelar själv utan laget måste spela ihop.
IP3:38	SN:	**Vilka hot/problem ser ni som mest aktuella?**
IP3:39	Informant 3:	Det finns faktiskt 3 bitar för det första är naturligtvis kvaliteten på koden att man får in säkerhet i hela kedjan av utvecklingen. Speciellt när vi tänker att vi har över 100 miljoner rader kod. För det andra organisationerna är ett jättestort hinder. Organisationerna i de gamla ingenjörsföretagen handlar inte om vad som är bäst för företaget utan det handlar om att bygga upp hierarkier och se till att det finns karriärvägar för människor. d.v.s. att ha en hierarkisk organisation fungerar inte. Ta jurister t.ex. deras yrke kommer automatiseras, för de gör det bättre än vad de kan göra. Folk måste ha en organisation som är anpassad för att driva saker framåt på ett agilt sätt. Det tror jag är ett jättestort hinder. Den tredje nyckeln är att de är datadrivna, dvs. att man lyfter upp data så att datan är tillgänglig för personer på företagen så man får hjälp av alla för att alla kan bidra inom företag. Om man synliggör data kommer mer människor kunna hjälpa till. 1. Kvalitet och att utvecklingsprocessen måste innehålla säkerhet. 2. Organisationerna måste förändra sig. 3. Organisationerna måste drivas via data. Man kan inte driva en

		organisation baserat på magkänsla. Det är de 3 bitarna som måste till.
IP3:40	SN:	**Om ett fordon skulle bli hackat, vad har ni för åtgärder för att hantera detta?**
IP3:41	Informant 3:	De första grejerna att man får fejkade meddelande, exempel i datorn. Man kan få ransomware meddelande ex, Your car has been hacked. You must pay. Att man får upp nya grejer som man inte har sett tidigare. Du märker att bilen inte stannar exakt när du vill, det finns massor med olika saker. Det är inte så svårt att hacka och attackera en bil, t.ex. det är samma sak med mobiltelefon. Vissa företag vill förbjuda alla mobiltelefoner som inte är Apple. Varför? Jo för att Android är öppen för en hackare att attackera och iOS som operativsystem är ett slutet system. Idag blir fler och fler företag mer attackerade via anställdas mobiltelefoner än datorer för det är en lättare väg in.
IP3:42	SN:	Men vet du hur ett företag skulle arbeta för att hantera en eventuell hackning, t.ex. där du arbetade innan?
IP3:43	Informant 3:	Vi gjorde test i utvecklingsprocessen, men om något hände så var det viktigaste att ta reda på hur bilen har blivit hackad. Vilket alltid inte är det enklaste. Man måste utföra tester, man måste automatisera testning så att man hela tiden har automatisk kontroll på hur detta funkar. Man måste tänka vilka hot som finns när man designar sin mjukvara, och det är det här med att få in säkerhet i utvecklingsprocessen. Det är väldigt svårt att säga exakt, för det är inte så många bilar som har blivit hackade. Oftast är det GPS som enkelt kan blivit lite annorlunda och ger lite konstiga direktiv när du är ute. Åtgärden är att man direkt försöker återskapa problemet precis som allt annat, och ta reda på hur de gått tillväga. Ta reda på hur kan de attackera? Vilka punkter som finns? osv. Idag är det väldigt enkelt att ta över kontrollen på bilen t.ex. bara genom nyckeln på en modern bil. Man kan bara använda en Ipad och ladda ner valfri programvara och efter det kan man styra bilen.
IP3:44	SN:	**Vad tror ni behövs i dagens samhälle för en stabil vehicle cloud infrastruktur?**
IP3:45	Informant 3:	Något mellan molnet som du måste ha och devices som du måste ha. alltså bilar eller TV-apparater eller vad det än är för device. Vi har jobbat med något som heter fog/dimma det är helt enkelt ett intelligent och distribuerat nätverk av fog som gör att man kan ta hand om denna data och flytta den fram och tillbaka mellan cloud och device. Det blir som ett slags mellanlager. För de flesta devices kommunicerar med något uppe i Coludet ex, avläsning i hemmet. Det man måste ha är

		fog för att distribuera. Distribuera innebär att man kan städa upp det, för att ta emot och skicka data till coloudet. En annan viktig grej att veta är att alla sådana enheter ska alltid göra kopplingar via detta mellanlager och till Cloudet. Cloudet ska aldrig tillåta kommunikation in i devicen. T.ex. om man har en tvättmaskin så ska den ta initiativet att kommunicera med cloudet för då blir det säkrare. Och det är detta som dimmlagret ska hantera, som då ligger mellan den tekniska enheten och cloudet.
IP3:46	SN:	**Anser ni att AI är hjärnan av internet of vehicles?**
IP3:47	Informant 3:	Ja, det är det eftersom tittar vi på vår mänskliga hjärna handlar det om intryck hela tiden. Det är tusentals intryck som en hjärna tar hela tiden. AI reagerar på information, antingen från realtid från en algoritm eller historik. Hela denna mjukvaran bygger på matematiska teorier från beteendevetenskap/deep learning. Hidden madox kan ni googla på.
IP3:48	SN:	**Har ni någon fråga till oss eller något att tillägga?**
IP3:49	Informant 3:	Internet of Vehicles handlar inte bara om att bilar ska sända data eller ta emot data, det handlar också om att de ska producera data. Det handlar mycket om deep learning också. Googlar ni deep learning kommer ni lära er jättemycket! Varför fastnade ni för det ni ska skriva om?
IP3:50	SN:	Vi tittade på säkerhet och kom in på smarta hem. Sen kom vi in på självkörande fordon, då det skrevs en del om det innan. Vi kollade med våra lärare om de tyckte vårt ämne lät bra vilket de gjorde, så vi körde lite på det direkt.
IP3:51	SN:	**Hade vi fått återkomma ifall vi kommer på någon följdfråga?**
IP3:52	Informant 3:	Ja, om ni har följdfråga så!
IP3:53	SN:	Vill ni vara anonyma i uppsatsen?
IP3:54	Informant 3:	Ja, det vill jag vara.

8.3.4 Intervju 4- IP4

Intervjuare: Susanna Nirvald (SN)
Sekreterare: Fanny Tapper (FT)
Verksamhet: Chalmers Universitet

Intervjuperson: Thomas Olavsson
Yrkesroll: Docent och avdelningschef, Nätverk och system, Data- och informationsteknik
Tid och plats: 11.30–11.50, torsdagen den 26 april 2018, Telefonsamtal från Lund

Referens nr:	**Person:**	**Frågor och svar:**
IP4:1	TO:	Kan ni berätta kort om syftet bara?
IP4:2	SN:	Vi vill undersöka säkerheten med självkörande bilar, forskningsfrågan är fortfarande lite under utveckling. Men syftet är att undersöka Internet of Vehicles, Vehicular Cloud och smarta bilar. Se på olika säkerhetsteorier och om dessa appliceras och hur man arbetar med det idag. Vi hörde att du hade forskat lite om detta. Fick tips av en gammal student av dig, han tyckte att du var rätt person för detta.
IP4:3	TO:	Okej vi kör på!
IP4:4	SN:	**Kan du berätta lite om din bakgrund? Utbildning osv**
IP4:5	TO:	Jag jobbar på Chalmers, doktorerar i datasäkerhet för drygt 20 år sedan. Jag har varit både på Chalmers och ute i industrin, så jag har varit ute i industrin också och jobbat med högsäkerhetslösningar/säkerhetslösningar kan man säga för försvarsindustrin, försvaret, polisorganisationer ute i världen inte bara i Sverige utan utomlands också då. Sen är det högsäkerhetslösningar då också.
IP4:6	SN:	Jättebra!
IP4:7	SN:	**Hur ställer du dig till utveckling av självkörande fordon?**
IP4:8	TO:	Rent allmänt tror jag att när tekniken är mogen så tror jag att det är rätt utveckling att gå på. Det ser vi i bilarna idag, det får fler och fler funktioner som höjer säkerheten, alltså bilarna identifierar fotgängare och stannar själv om inte föraren gör det. Bilarna kan se om du håller på att göra ett filbyte utan att blinka. Du kör för fort i den där svängen där framme som du inte kommer klara av för att du kör för fort, alltså den typen. Du kan titta på navigatorn och förutse vad som kommer hända så kan de prata med varandra. Det är väldigt mycket säkerhetsförhöjande funktioner som kommer steg för steg och slutsteget blir naturligtvis att bilarna, tycker att du är värdelös som förare och du tillför inget. Vi tar över alltihop och vi kommer inte chansa någonstans. Bilarna vet vad de andra har för avsikter, var de är och vad de tänker göra. Så det är just människor som tänker jag kan nog köra om här det går nog bra, det finns liksom inte. Jag tror att den utvecklingen är jättebra och kommer definitivt vara trafiksäkerhetshöjande. Så att man måste se till att man designar säkerheten på ett bra sätt så man kan lita på funktionerna också.

IP4:9	SN:	Precis!
IP4:10	TO:	Men det tror jag nog att man kommer att göra och jobba med det.
IP4:11	SN:	Jättebra!
IP4:12	SN:	**Ser du en koppling mellan Internet of Things och Internet of Vehicles?**
IP4:13	TO:	Ja, man brukar räkna in fordon i Internet of Things. De är en av de prylarna som kommer vara uppkopplade. De ingår i detta.
IP4:14	SN:	**Hur ser du på säkerhetsaspekter inom internet of Vehicles i dagsläget?**
IP4:15	TO:	Det finns alltid en risk att någon/några biltillverkare prioriterar att sälja först och sedan lösa problemen sedan. Det gäller inte bara bilar utan det gäller alla områden egentligen. Det blir liksom tanke marketing blir ju väldigt viktigt, där måste ju alla vara med liksom och inse att utan säkerheten så riskerar man faktiskt att bilen och passageraren riskerar hälsa eller liv. Man måste designa bilen från grunden på ett sånt sätt så att den kan hantera problem, för problem kommer det bli förr eller senare oavsett vad så att då måste man bygga den på ett sådant sätt så att den kan hantera säkerhetsproblem. Detta måste nog bli en hyfsad omdesign för väldigt många biltillverkare naturligtvis. En del har börjat och kommit en bit på vägen och andra har inte ens funderat på det.
IP4:16	SN:	Ja, det är väldigt spännande hur att alla jobbar mot samma mål men alla jobbar på olika sätt verkar det som.
IP4:17	TO:	Det är ju det och som sagt vissa bilar har hackats och man ser att man kan ta över dem. Problemet är att en bil idag har i stort sett 150-200 datorer idag och de är inte självkörande i dag. Och de är uppkopplade till nätverk internt och många av de här datorerna pratar med varandra och har tjänster ute från omvärlden också. Det räcker att en egentligen av de här blir hackad så finns det stor risk att man via den kan påverka hela bilen i stort, man kan skicka ut falska kommandon och gör saker och ting inne i bilen. Så det måste börja delas upp i säkra domäner och man delar upp dem i interna nätverk. För 200 datorer blir liksom om man jämför ett kontor med 200 personer det räcker att en får ett virus, det fungerar liksom inte. Man måste dela upp/segmentera näten internt också, det är samma sak i bilen då.
IP4:18	SN:	Jättebra!
IP4:19	SN:	**Hur tror du att utvecklingen kommer se ut i framtiden?**
IP4:20	TO:	Allting kommer att ta tid det tror jag, men det är en gissning. Jag tror inte att det kommer gå så jätte jätte fort. Jag tror att i vissa situationer kommer bilarna kunna köra, vi ser denna stegvisa utvecklingen att

		som nu t.ex. kan bilarna hålla hastighet och avstånd till bilen framför dig i en bilkö, där kan bilen i princip köra själv på motorvägen och den kan följa markeringarna osv men det krävs nog en hel del utveckling innan man kan lita på det fullt ut. Det är väldigt många problem som måste lösas som man kanske inte tänker på som kan vara väldigt luriga. Men vi tar för givet att om du kör i en stad exempelvis och du ser en boll komma ut på vägen, då inser vi kanske att okej snart kommer en unge springa ut här, och då sakta in men en bil kanske inte har den funktion. Vi kan titta på fotgängare och ha ögonkontakt med fotgängare, tänker de gå över eller står de med ryggen mot vägen och inse att de inte kommer gå över, men en bil kanske inte har den funktionen. Skilja mellan en fotgängare och en soptunna kan vara ett problem för en bil. Är det en fotgängare som står där eller är det ett annat objekt? Det är inte alltid lätt att identifiera som gör att det är nog en hel del bitar kvar innan de är helt självkörande i varje fall. Tror jag, men det är en gissning alltså men det är nog min bild av det just nu.
IP4:21	SN:	**Vad kommer behövas för att stärka säkerheten med Internet of Vehicles?**
IP4:22	TO:	Dels då att designa insidan på ett sådant sätt så de klarar av att hantera, inte om men när det blir något säkerhetsproblem, när något blir hackat och så ska de upptäcka. De har interna brandväggar som ska segmentera, det måste finnas intrång system som ska upptäcka. Precis som när vi själva upptäcker att nu gör bilen konstigt så ska bilen själv upptäcka att här är något som inte är riktigt. Sen så måste man ha bra koll med den kommunikationen som sker med utsidan och veta vem de pratar med och i vilket mån man kan lita på den informationen man får. Sedan så bygger man mer relevanta system så man litar inte bara på kommunikation utan man blandar in sensorer, radar och kameror och massa andra saker också. Så att bygga den där verklighetsuppfattningen eller vad man nu ska kalla det för är väldigt viktigt för det måste vara många system som samverkar, så att om ett system har fel så ska de andra.
IP4:23	SN:	**Vilka hot/problem ser du som mest aktuella?**
IP4:24	TO:	Man måste bygga skyddet mot hackers förstås så man kan hantera den trafiken och de försök som sker utifrån, det ska vara i stort sett omöjligt även om allting kommer att hackas för eller senare. Men det ska ändå vara oerhört svårt. Och bilen ser bilen att det här är ett problem så ska den stänga av de funktionerna eller kunna begränsa skadan. Det kan vara så enkelt att vissa bilar säger att tills det här problemet är fixat kommer vi inte prata med omgivningen och är inte självkörande på ett tag. Sånt kan man tänka sig men man måste ha de mekanismerna på plats. Och när man väl har detta kan det bli väldigt bra, men det är en liten bit kvar.

IP4:25	SN:	**Vad tror du behövs i dagens samhälle för en stabil vehicle cloud infrastruktur?**
IP4:26	TO:	Det man bygger på idag är två huvudsakliga kommuikationsbitar. Det ena är att du bygger med fordonskommunikation och den idag rådande standarden, som är gammalt hederligt Vlan och det är fordon till fordon kommunikation och räckvidden är inte speciellt långt men typ ett 100 tal meter. Där kan man prata med varandra vad man ska göra när man kommer till en korsning att bilarna kan tala om för varandra att jag kommer här, min avsikt är att jag kör rakt fram eller jag tänker köra höger i korsningen. Så kan de koordinera med varandra. Den andra biten där är att i städer kan det bli problem för att stora områden inte är stärkta för att ha täckning precis och man har inte täckning överallt. Då pratas det idag att man ska få support och man kan hjälpa till att använda 5g t.ex. där, 4g, 5g framför allt. Som bygger man kan tänka sig trafikljus inne i stan ligger på support där man använder den strukturen istället. Så man kan prata runt hörnet så man vet vilka som är där och vilka som kommer osv.
IP4:27	SN:	**Anser du att AI är hjärnan av Internet of Vehicles?**
IP4:28	TO:	Inte AI på det sättet. AI är inte ett väldefinierat begrepp. Utan AI för mig är mer om man pratar självlärande system, och det tror jag ligger en bra bit bort om de ska börja lära sig saker och ting själva. Och med det som begrepp är det lurigt i fordon sammanhang för att om ett system rent allmänt lär sig något och det ser ut som det fungerar så vet du egentligen inte, du har ingen garanti för vad det är de har lärt sig, den kunskapen kanske har stora hål. Så att ha ett självlärande system om du nu menar med AI och självlärande, det ligger nog väldigt långt bort om man inte kan garantera vissa saker. Utan vi vill veta om de har tänkt in något komplett. T.ex. en kollega som hade ett anti-sand system som skulle vara självlärande. Man tittade noga på all e-post på engelska, det såg ut som det fungerade men om man tittade på vad är det egentligen den har lärt sig, så va det inte riktigt tänkt så kanske. Det är samma med en bil, det verkar som de kan köra men vad är det egentligen den har lärt sig. Så fort något ändras så kan det bli totalt katastrofalt resultat. Så i den aspekten tror jag inte att AI, inte på det sättet inte för det själva självkörande aspekten. Inte för den kritiska funktionen, där måste man lära föraren. Det är min bild iallafall i och med att alla inte har samma begrepp va AI är så att AI för vissa kan vara bara att den kör själv så är det AI, men du har ju lärt den/programmerat den på förhand hur den ska agera i dessa situationerna.
IP4:29	SN:	**Har du någon fråga till oss eller något att tillägga?**
IP4:30	TO:	Oj! Nej, det har jag nog faktiskt inte.
IP4:31	SN:	**Hade vi fått återkomma ifall vi kommer på någon följdfråga?**

IP4:32	TO:	Ja, absolut gör det!
IP4:33	SN:	Vill du vara anonym i uppsatsen?
IP3:34	TO:	Du kan skriva det är ok.
IP3:35	SN:	Så bra, då tackar vi för oss och hejdå!
IP3:36	TO:	Ingen fara, stort lycka till!

8.3.5 Intervju 5- IP5

Intervjuare: Susanna Nirvald (SN)
Sekreterare: Fanny Tapper (FT)
Verksamhet: Företag Y
Intervjuperson: Informant 5
Yrkesroll: Developer
Tid och plats: 13:15-13:45, torsdagen den 26 april 2018, Telefonsamtal från Lund

Referens nr:	**Person:**	**Frågor och svar:**
IP5.1	SN:	**Kan du berätta lite om din bakgrund? Utbildning osv**
IP5.2	Informant5:	Ja, jag har jobbat inom fordonsbranschen i typ 7 år, specifikt mest inom fleet management. Jag har en högskoleingenjörsutbildning inom datateknik som är det primära. Sen har jag jobbat med olika system sedan 2011 lite drygt, så att det är väl det grundläggande.
IP5.3	SN:	**Kan du berätta lite om ditt arbete t.ex. titel osv?**
IP5.4	Informant5:	Ja, som det ser ut idag så jobbar vi med att ta fram nya lösningar på en befintlig plattform, kan man säga. Så det innefattar allt från att göra research på olika teknologier till att testa dem och implementera saker som ännu inte finns i produktion. Det är ganska brett vilket kanske är typiskt ingenjörsarbete. Det är inte bara en grej så, det kan vara allt ifrån dels att researcha och dels utveckla och allt där emellan också.
IP5.5	SN:	Kul att variera lite!
IP5.6	Informant5:	Det svänger snabbt, det är det korta svaret på vad jag gör.
IP5.7	SN:	Men det blir jättebra!
IP5.8	SN:	**Hur ställer sig företaget till utveckling av självkörande fordon?**

IP5.9	Informant5:	Jag kan nog inte svara för företaget exakt, men jag tror inte de är negativa till det. Däremot har vi samarbetat med bolag som kanske riktar in sig lite mer på de delarna.
IP5.10	SN:	**Arbetar ni något med utveckling av självkörande fordon t.ex. Internet of Vehicles, AI eller Vehicle Cloud?**
IP5.11	Informant5:	Vi sitter i cloud. Där bygger vi infrastrukturen för hela miljön. Men det är just det att det är 2 delar, en skarp befintlig miljö som används och den nya miljön som inte är bruk än. Det är då där jag sitter, så att vi bygger hela infrastrukturen och sätter upp hela miljön där applikationer deployas i typ appar för självkörande bilar eller olika typer av kommunikationer. Och när det gäller AI osv så tittar vi på det internet för våra egna miljöer. Men jag kan inte riktigt säga exakt vad vi gör, men vi jobbar med det.
IP5.12	SN:	**Ser ni en koppling mellan Internet of Things och Internet of Vehicles?**
IP5.13	Informant5:	Ja, det gör jag väl. Men det är väl mer att det kan bli lite flummiga begrepp. För att Internet of Things har du något som är uppkopplat och det kan vara lite vad som helst. Kopplingen i det här fallet så har vi hela cloud miljön som alla fordon ansluter till och de är uppkopplade kan man säga. Men det är mot cloud och hela den miljön, så att det finns absolut en relation mellan dem. Men det blir en ganska filosofisk fråga om man säger så.
IP5.14	SN:	Det är bara att vi har hittat massa i teorin så måste vi koppla svaren till det, så det är därför den är kanske lite filosofisk.
IP5.15	SN:	**Hur ser ni på säkerhetsaspekter inom Internet of Vehicles i dagsläget?**
IP5.17	Informant5:	Det finns team som jobbar med de sakerna, jag sitter inte aktivt med säkerhetssaker idag. Men man har ju det tänket aktivt hela tiden. Jag anser att de som sitter ute i skarp produktion har definitivt väldigt hög säkerhet, men det sitter som sagt folk som gör det heltid. Är tyvärr inte helt insatt i det.
IP5.18	SN:	**Hur tror ni att utvecklingen kommer se ut framöver?**
IP5.19	Informant5:	Det kommer bygga på Micro services, att man istället för att ha en stor produkt har man mindre tjänster. T.ex. en fordonstillverkare kanske redan har någon form av cloudlösning där man har fordon uppkopplade. Där har de olika moduler som har olika tjänster som man kan handplocka beroende på vad man vill ha. Och det kommer vara mer sånt! Man kallar det Micro-services, tänk dig att du har att någon säljer till dig en lösning med 100 funktioner men du använder kanske bara två men du betalar ändå för de 100. Så nu väljer du att du bara vill ha dessa

		två sakerna och inte de andra, så istället säger man att man kan plocka ut det man behöver. Det är det som hela vinsten/poängen med att ha cloud lösningar är och det kommer bli ännu mera sådant. Sen så kommer det bli ännu mer automatiserat och vi bygger upp automatisering av dessa olika miljöerna som deployas ute hos olika kunder och tillverkare. Det kommer bli mer automatiserat vad det gäller att få upp miljöerna och mindre manuellt arbete. Däremellan kommer AI komma in mer och mer, dels över monitorering och dels framöver kommer det nog innefatta vad jag själv tror även när man deployar saker. Det kommer bli mindre och mindre att någon fysiskt trycker på en knapp. Utan det kommer bli mer och mer automatiserat och så när man är ute hos en kund så kan infrastrukturen balansera sig själv istället. Det kommer gå mot mer sånt är jag helt övertygad om, men det kan bli lite flummigt nu vad jag menar.
IP5.20	SN:	Nejdå, ingen fara jag förstår exakt vad du menar.
IP5.21	SN:	**Vilka hot/problem ser ni som mest aktuella?**
IP5.22	Informant5:	De största problemen är att saker och ting kan bli utdaterade. Asså att olika typer av verktyg och olika typer av infrastrukturer samt olika saker att bygga upp infrastrukturen på. Sådana saker kan gå väldigt snabbt och man måste hålla sig lite till det som är senaste men ändå är stabilt.
IP5.23	SN:	Exakt!
IP5.24	Informant5:	Det måste finnas en balans där emellan.
IP5.25	SN:	Så det måste finnas t.ex. att alla bilar måste ha samma nivå på uppdateringarna, så att inte någon bil ligger back tre uppdateringar?
IP5.26	Informant5:	Så kan det också vara, men det jag syftar på nu är snarare mer det som faktiskt gör att den blir uppdaterad. Det finns ju dels själva uppdateringen av mjukvaran men sen också hur mjukvaran blir uppdaterad alltså själva flödet. Till det finns det också utveckling till infrastrukturen, det kan också vara något man måste balansera. T.ex. bilarna ska kunna klara av att ta emot data osv till ett antal år, så man måste matcha bilens mjukvara med deras hårdvara. Det är mycket att väga emot så det är viktigt att ha en balans. Jag tror inte det är ett problem utan det är mer en utmaning.
IP5.27	SN:	**Om ett fordon skulle bli hackat, vad har ni för åtgärder för att hantera detta?**
IP5.28	Informant5:	Jag kan inte svara på exakt hur det går till, jag vet att det finns men jag jobbar inte extra med det.

IP5.29	SN:	**Vad tror ni behövs i dagens samhälle för en stabil vehicle cloud infrastruktur?**
IP5.30	Informant5:	Man kan se det såhär att det finns om man tittar på fleat managementsystem, asså 3 parts system där man har fordonsmontering osv. Då sätter man upp en hårdvara som har en egen router som kan vara uppkopplad dygnet runt hela tiden. Medan t.ex. fordonstillverkare då kan sätta ut hårdvara som ansluter när tillfälle ges. Så att det beror lite på vad man använder och vad man har. Jag menar jag ser inga, det är något som kommer av sig självt lite grann t.ex. 5G är på gång. Vet inte om jag har något bra svar på din fråga egentligen.
IP5.31	SN:	Det är alltså på gång?
IP5.32	Informant5:	Ja, det som du beskriver stämmer in på t.ex. fordonstillverkarnas egna hårdvara i bilarna och den kommer bli förbättrad i samband med 5G. 5G möjliggör bättre kommunikation mellan punkter till skillnad från mot vad det är idag. Så att 5G är väl det som kan förbättra mer.
IP5.33	SN:	**Anser ni att AI är hjärnan av internet of vehicles?**
IP5.34	Informant5:	Inte idag, men det kommer bli det är jag övertygad om men inte idag. Idag är det inget AI som styr infrastrukturen och det är inget AI som deployar osv. Det börjar med att man använder AI för monitorering, för att kunna se hur olika instanser jobbar mot varandra och om det behövs anpassas. T.ex. om något ligger och drar mer minne än vad det behövs, så kan man prediktera olika förbättringar inom cloud infrastrukturen. Men det är inte hjärnan på något sätt idag. Men det kommer definitivt bli om ett tag.
IP5.35	SN:	Jättebra! Det är alltid intressant att höra vad personer som arbetar inom detta tycker då många forskare anser att det är det.
IP5.36	Informant5:	Det beror på hur man ser på frågan, ser man det rent praktiskt hur systemet är uppbyggt är inte AI som är hjärnan. Det beror ju på hur man anfaller frågan och beror på vem du pratar med och vad de jobbar med. Men jag skulle inte säga att det är hjärnan idag.
IP5.37	SN:	**Har ni någon fråga till oss eller något att tillägga?**
IP5.38	Informant5:	Jag hade något här innan men… Ni tittar på uppkopplade fordon precis och olika former. Du nämnde det här med självkörande bilar innan, är ett något slags tema på det ni gör nu?
IP5.39	SN:	Ja, vi skriver ju då vår kandidatuppsats och halva klassen skriver om GDPR i olika former och det är ganska många som skriver om Internet of Things. Så vi ville hitta något som sticker ut lite och vi var inne på lite säkerhetsområdet och så var det mycket

		skriverier om självkörande bilar. Vi har lärt oss extremt mycket måste jag säga.
IP5.40	Informant5:	Jag utvecklade en machine learning applikation som dedikerade felaktiga däck på bussar. Det har ju lite med uppkopplade fordon och cloud att göra, det jag tänkte nämna var att ni kan slänga öga på det arbetet om ni vill ha?
IP5.41	SN:	Ja, jättegärna! Vad heter den uppsatsen?
IP5.42	Informant5:	Jag kan maila dig vart du hittar den. För jag tror att det kan vara något i den som kan underlätta för er när ni ska referera till lite olika saker framförallt inom AI och IoT eventuellt.
IP5.43	SN:	**Hade vi fått återkomma ifall vi kommer på någon följdfråga?**
IP5.44	Informant5:	Ja!
IP5.45	SN:	Vill du vara anonym i uppsatsen?
IP5.46	Informant5:	Kör på anonym så länge.
IP5.47	SN:	Absolut, då kör vi på det. Stort tack verkligen, du får ha en jättebra dag så hör vi av oss ifall det är något mer.
IP5.48	Informant5:	Absolut, tack hej!

9 Referenser

Böcker

Backman, Jarl. *Rapporter och uppsatser*. 3.e uppl. Lund. Studentlitteratur 2016.

Bryman, Allan. *Samhällsvetenskapliga metoder*. 2.2 uppl. Malmö. Liber AB 2008.

Epstein, R., Roberts, G and Beber, G. *Parsing the Turing Test*. 1. uppl. Berlin. Springer Science. 2009.

Jacobsen, D I. *Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen*. Lund. Studentlitteratur 2002.

Russell, Stuart och Norvig, Peter. *Artificial Intelligence A Modern Approach*. 3 edition. New Jersey. Pearson Education 2010.

Schött, K., Melin, L., Strand, H and Moberg, B. *Studentens skrivhandbok*. 2. uppl. Stockholm. Liber 2012.

Tegmark, Max. *Life 3.0 : being a human in the age of artificial intelligence.* 1. uppl. New York: Alfred A. Knopf 2017.

Artiklar

Baird, H., Coates, A. och Fateman, R. 2002. *PessimalPrint: a reverse Turing tes*t. Palo Alto Research Center.
https://link.springer.com/article/10.1007/s10032-002-0089-1 (Hämtad 2015-03-20)

Brohult, Linus. 2018. *Forskare: ”Självkörande bilar förändrar städerna inom bara några år”*. SVT Nyheter. https://www.svt.se/nyheter/vetenskap/forskare-sjalvkorande-bilar-forandrar-staderna-inom-bara-nagra-ar (Hämtad 2018-03-21)

Childs, Martin. 2011. *John McCarthy: Computer scientist known as the father of AI*. Independent UK. https://www.independent.co.uk/news/obituaries/john-mccarthy-computer-scientist-known-as-the-father-of-ai-6255307.html (Hämtad 2018-03-06)

Copeland, B, Jack. 2001. *The Turing Test*. Kluwer Academic Publishers.
https://link.springer.com/content/pdf/10.1023/A:1011285919106.pdf (Hämtad 2018-03-25)

Crossler, Robert E och Posely, Clay. 2015. *Robbing Peter to Pay Paul: Surrendering Privacy for Security’s Sake in an Identity Ecosystem*. Journal of the Association for Information Systems. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1776&context=jais (Hämtad 2018-04-10)

Dimitrakopoulos, George. 2011. *Intelligent Transportation Systems based on Internet-Connected Vehicles: Fundamental Research Areas and Challenges*. Harokopion University of Athens

https://pdfs.semanticscholar.org/cdfd/7f6e1f69ec2fb50b73d7f5cace0e845489f6.pdf (Hämtad 2018-04-08)

Dreyfuss, Emily. 2017. *Security news this week: A whole new way to confuse self-driving cars.* Wired, Security. https://www.wired.com/story/security-news-august-5-2017/ (Hämtad 2018-02-20)

Elbied Pettersson, Gabriella. 2018. *Kvinna påkörd av självkörande bil-dog*. GP. http://www.gp.se/nyheter/v%C3%A4rlden/kvinna-p%C3%A5k%C3%B6rd-av-sj%C3%A4lvk%C3%B6rande-bil-dog-1.5411970 (Hämtad 2018-04-09)

Fluchter, Kristina och Wortmann, Felix. 2015. *Internet of Things*. Bus Inf Syst Eng. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1338&context=bise (Hämtad 2018-04-08)

Gerla, M., Lee, E.K., Paul, G. och Lee, U. 2014. *Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds*. http://www.kresttechnology.com/krest-academic-projects/krest-mtech-projects/IOT/Mech%20IOT-2016-17/ABSTRACT%20AND%20BASE%20PAPERS/25.Internet%20of%20Vehicles%20From%20Intelli/25.pdf (Hämtad 2018-04-02)

Gibbs, Samuel. 2015. *Jeep owners urged to update their cars after hackers take remote control*. The Guardian. https://www.theguardian.com/technology/2015/jul/21/jeep-owners-urged-update-car-software-hackers-remote-control (Hämtad 2018-04-09)

Holmberg, Kalle. 2018. *Dödsolycka med självkörande Tesla väcker frågor om varningssystem*. Dagens Nyheter. https://www.dn.se/ekonomi/dodsolycka-med-sjalvkorande-tesla-vacker-fragor-om-varningssystem/ (Hämtad 2018-04-09)

Kaiwartya, O., Hanan Abdullah, A., Cao, Y., Altameem, A., Prasad, M., Lin, C. och Liu, X. 2016. *Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges and Future Aspects.* IEEE Access. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7562526 (Hämtad 2018-04-06)

Kelemen, Jozef. 2007. *Artificial Neural Networks*. Acta Polytechnica Hungarica. https://www.uni-obuda.hu/journal/Kelemen_12.pdf (Hämtad 2018-03-06)

Kvandal, Magnus. 2017. *Självkörande bilar blir påkörda för att de kör för bra*. Teknikens Värld. http://teknikensvarld.se/sjalvkorande-bilar-blir-pakorda-for-att-de-kor-for-bra-541982/ (Hämtad 2018-04-10)

Lee, Jae Kyu. 2015. "Guest Editorial: Research Framework for AIS Grand Vision of the Bright ICT Initiative," *MIS Quarterly*, (39: 2) (Hämtad 2018-03-28)

Maglaras, L., Al-Bayatti, A., He, Y., Wagner, I. och Janicke, H. 2016. *Social Internet of Vehicles for Smart Cities.* School of Computer Science and Informatics, De Montfort University. http://www.mdpi.com/2224-2708/5/1/3/html (Hämtad 2018-04-09)

Newell, Allan. 1955. *The Chess Machine: An Example of Dealing with a Complex Task by Adaptation.* The Rand Corp., Santa Monica, California. Western Joint Computer Conference. https://dl.acm.org/citation.cfm?id=1455312 (Hämtad 2018-03-05)

Newell, A., Shaw, J. och Simon, H. 1957. *Empirical Explorations of the Logic Theory Machine: A Case Study in Heuristic*. The RAND Corp., Santa Monica, California. Western Computer Proceedings. https://dl.acm.org/citation.cfm?id=1455605 (Hämtad 2018-03-05)

Newell, A., Shaw, J. och Simon, H. 1959. *A Variety of Intelligent Learning in a General Problem Solver.* The RAND Corp., Santa Monica, California. http://www.mirrorservice.org/sites/www.bitsavers.org/pdf/rand/ipl/P-1742_A_Variety_Of_Intelligent_Learning_In_A_General_Problem_Solver_Jul59.pdf (Hämtad 2018-03-05)

Putchala, Santosh och Agarwal, Nikhil. 2009 *Machine vision: an aid in reverse Turing test.* Springer-Verlag London Limited. https://link.springer.com/content/pdf/10.1007%2Fs00146-009-0231-4.pdf (Hämtad 2018-03-27)

Rabe, Mattias. 2016. *I dag börjar Volvos självkörande bilar användas av vanliga bilister*. Teknikens Värld. http://teknikensvarld.se/i-dag-borjar-volvos-sjalvkorande-bilar-anvandas-av-vanliga-bilister-562640/ (Hämtad 2018-03-15)

Rabe, Mattias. 2017. *Volvo hoppar över Level 3-autonoma bilar*. Teknikens Värld. http://teknikensvarld.se/volvo-hoppar-over-level-3-autonoma-bilar-459155/ (Hämtad 2018-04-11)

Raya, M., Papadimitratos, P. och Hubaux, J. 2006 *Securing Vehicular Communications.* EPFL, IEEE Wireless Communications. https://infoscience.epfl.ch/record/87501/files/SecVehCom.pdf (Hämtad 2018-04-06)

Samuel, Arthur. 1967. *Some Studies in Machine Learning Using the Game of Checkers. II-Recent Progress*. IBM Journal. http://users.auth.gr/kehagiat/Research/GameTheory/12CombBiblio/Checkers_Samuels_ibmrd1106C.pdf (Hämtad 2018-03-06)

Sundberg, Simon. 2018. *Människan orsakar 90 procent av alla olyckor*. Svenska Dagbladet. https://www.svd.se/manniskan-orsakar-90-procent-av-alla-olyckor (Hämtad 2018-05-07)

Van der Meulen, Rob och Rivera Janessa. 2015. *Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities*. Gartner. https://www.gartner.com/newsroom/id/2970017 (Hämtad 2018-04-11)

Varshney, Upkar. 2005. *Vehicular Mobile Commerce: Applications, Challenges, and Research Problems*. Georgia State University. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3033&context=cais (Hämtad 2018-04-08)

Yang, F., Wang, S., Li, J., Liu, Z. och Sun, Q. 2014. *An Overview of Internet of Vehicles*. Beijing University of Posts and Telecommunications, Beijing, China. http://sguangwang.com/PDF/An%20Overview%20of%20Internet%20of%20Vehicles.pdf (Hämtad 2018-04-08)