Examensarbete

HÖGSKOLAN I SKÖVDE

Kartläggning av cybersäkerheten på uppkopplade bilar: Sårbarheter

Examensarbete för kandidatexamen inom huvudområdet informationsteknologi med inriktning mot nätverks- och systemadministration

Grundnivå 30 högskolepoäng

Vårtermin 2023

Pontus Claesson

Handledare: Marcus Birath

Examinator: Joakim Kävrestad

ABSTRACT

The future is here with interconnected computers on four wheels - connected cars! Just like regular computers in networks, there is also a huge amount of cybersecurity challenges regarding vehicles. With the large amount of data transmitted between vehicles and other devices, a proper way of securing the connections is important. It is clear that the connected components and technologies in modern cars have a large amount of vulnerable points, and more research is needed for further studies. Several modern vehicle technologies such as electrical control units, over the air updates and lidar radars etc are discussed in this work. The most prominent way of securing the stored personal data and the constant flow of transmitted data is encryption, and with the use of blockchains. There are also suggestions on different types of new framework and standards to lock in an even keel for the cybersecurity environment. This work investigates the passive vulnerabilities existing in these connected vehicles systems. There will be a mapping of the most prominent and relevant surfaces vulnerable to for example cyber attacks. This will take the form of a literature study with thematic analysis. Scientific articles will be searched for in databases to find relevant data to code into different themes, answering the research question. The work aims to look at different sources describing ways of implementing cryptographic blockchains in order to achieve the level of security necessary. There will also be some proposals of future frameworks, and to put in standards to secure the future of vehicle cybersecurity. The purpose of this work is to gain a wide view of how the connected vehicles landscape looks like in the form of vulnerabilities, and how we could negate them in the future.

Innehållsförteckning

1 Introduktion

I samband med teknikens språngande utveckling har städer blivit allt smartare. Smart mobilitet är ett viktigt element i smarta städer, och uppkopplade autonoma fordon är en väsentlig del av smart mobilitet. Sårbarheter i autonoma fordon kan dock skada livskvaliteten och människors säkerhet. Hackare skulle kunna via fjärrstyrning kapa fordonets styrenheter och till exempel stanna fordonet mitt på motorvägen. (Kim, K. et al. 2021). Som en del av IoT-miljön är uppkopplade bilar lika sårbara för säkerhetsrisker, såsom cyberattacker från icke-auktoriserade tredje parter och dataintrång från auktoriserade tredje parter. En global rapport har avslöjat att under 2019 skedde mer än 80 cyberattacker på ekosystemet för smart mobilitet, många av de relaterade till uppkopplade bilar. En angripare med illa avsikter kan inte bara stjäla data, utan också inaktivera dess säkerhetsfunktioner eller till och med få kontroll över en bil (Rebiger, S., et al., 2019).

Moderna bilar är idag utrustade med all möjlig form av teknik, allt från sensorer, kameror och artificial intelligence (AI). Många av dessa verktyg underlättar körupplevelsen och säkerheten då fordonet automatiskt kan hålla sig till trafikregler, skiftande miljöer och även kommunicera med andra fordon på vägen (Noh, J., et al., 2020). Potentialen är enorm och kan drastiskt förbättra säkerheten i trafiken, effektivisera transport och sänka luftförorening. Detta kan uppnås med hjälp av mer effektiva och självlärande system som konstant kan välja optimalt sätt att köra, välja bäst väg och förebygga trafikolyckor med hjälp av sensorer och kameror. (Joy, Gerla. 2017).

Med ny teknik finns det dock även en baksida. Med stor kraft kommer ännu större ansvar, och ännu större möjligheter för saker att gå snett. Utvecklingen går fort inom hela fordonsindustrin och transportindustrin vilket leder till att utmaningarna blir fler. En av dessa utmaningar är just hur cybersäkerheten ska implementeras rätt. (Trafikverket, 2021). Nya fordon har blivit datacenter på hjul. Dagens bilar stöder upp till 150 elektroniska styrenheter och upp till 100 miljoner rader kod. Som ett resultat flödar data in och ut ur fordonet från flera källor. Det finns redan 107 miljoner uppkopplade bilar på vägen (Thales, 2021). Uppkopplade fordonsnätverk har flera säkerhetsproblem som integritetsbevarande, säker autentisering och systemtillförlitlighet (Noh, J., et al., 2020). Säkerhetsproblemen gäller även självkörande fordon, som i nuläget blir fler och fler. Förutom att öka säkerheten och komforten i transporten, kommer dessa fordon att vara anslutna till olika externa system och använda avancerade inbyggda system för att uppfatta sin omgivning och fatta intelligenta beslut. Men denna ökade anslutning gör dessa fordon sårbara för olika cyberattacker som kan ha katastrofala effekter (Ahlberg. 2023). Attacker mot fordonssystem är redan på uppgång i dagens fordon och förväntas bli vanligare i framtida självkörande fordon. Det finns därför ett behov av att stärka cybersäkerheten i framtida självkörande fordon. Fordon kommer att vara del av ett extremt tätt-sammankopplat ekosystem med kritisk infrastruktur (EY, 2020).

Den befintliga elektroniska arkitekturen inom uppkopplade och autonoma fordon var från början inte avsedd för cybersäkerhet (Wang, Y., et al., 2023). Det visar sig även att trots pågående forskning för fordonssäkerhet är vissa delar av den anslutna fordonsarkitekturen fortfarande sårbara i sin design. Till exempel så använder sig styrenheterna sig av ett “broadcast”-nätverk som används för kommunikation av mikrokontroller i bilen, men det tillhandahåller inte grundläggande säkerhetsfunktioner som autentisering eller kryptering. (Bajpa, P., et al., 2020).

Den potentiella attackytan som angripare siktar in sig på blir större och större med de utökande nätverksuppkopplingarna (Cali, U., et al., 2023). På grund av närvaron av fler mjukvarusäkerhetsfel i uppkopplade fordon betonas nödvändigheten av mjukvarusäkerhetstestning i uppkopplade fordon. Det är av stor vikt att upptäcka sårbarheter i ett tidigt skede. Det är dock mycket utmanande att täcka mjukvarusäkerhet och säkerhetskrav eftersom fordon innehåller så många komponenter där mjukvara är integrerad. Detta gör jobbet för mjukvarutestare svårare eftersom det aldrig kommer att finnas tillräckligt med tid att testa varje komponent uttömmande i något mjukvarusystem. Dessutom är uppkopplade fordon utplacerade i en känslig miljö som kan vara livshotande, vilket gör jobbet för mjukvarutestare mer avgörande (Moukahal, L. & Zulkernine, M., 2019).

Innan varje fordon är redo att säljas på marknaden behöver säkerhetsingenjörer verifiera systemets säkerhet för att undvika katastrofala händelser. Bristen på kvalitetssäkring och testningsprocedurer i fordonsindustrin är en av de främsta faktorerna som bidrar till existensen av sårbarheter. Säkerhetstestning en avgörande fas för att identifiera sårbarheter och systemsvagheter. Olika säkerhetsgarantimetoder används i fordonsindustrin, inklusive statisk kodanalys, dynamisk programanalys, sårbarhetsskanning, penetreringstestning och fuzztestning. Dessa säkerhetstesttekniker minskar sårbarheterna i ett system. Trots detta är säkerhetstestning av fordonsprogramvarusystem en komplex uppgift som lämnar tillverkarna med flera utmaningar. Fordonsprogramvarusystemet är ett komplext system med cirka hundra miljoner rader kod som bor och körs på dussintals elektroniska styrenheter. Dessa styrenheter fungerar baserat på inmatningar från radar, kamera, ultraljudssensorer, temperatursensorer, däcktryckssensorer och många andra sensorer. Eftersom fordon opererar i en kontinuerligt utvecklande miljö varierar inmatningar till styrenheter drastiskt. Det är därför svårt att förutsäga alla möjliga inmatningskombinationer av styrenheter (Moukahal, L. & Zulkernine, M., 2021).

En viktig komponent inom uppkopplade fordon är den pågående 5G-tekniken och den kommande 6G-tekniken kommer att förvandla inteligenta transportsystem till nya dimensioner, men till priset av en mängd sårbarheter. Till skillnad från ortodoxa reaktiva metoder är det nödvändigt att proaktivt utveckla och utvärdera den skalbara cybersäkerhets-arkitekturen i den kommunikationsstandard som möjliggör kommunikation mellan fordon och allt annat i dess omgivning. Det innebär att implementera tvärindustriella kunskapsdelningsmekanismer och nya cybersäkerhetsmetoder som kryptografi och blockkedjestrategier (Khan S., et al., 2021).

Uppkopplade och autonoma fordon producerar, lagrar och kommunicerar en stor mängd personuppgifter (vägen som tagits, stopppunkterna, hem och arbetsadresser, etc.). Utvecklingen av denna typ av fordon ger möjlighet att erbjuda nya tjänster till trafikanter, med fler mjukvaru och hårdvarukomponenter på fordonet. Många av dessa komponenter lider av sårbarheter som kan utnyttjas. Problemet är att en enda sårbarhet i en del av systemet kommer att hota integriteten för fordonets användare (Chah B., et al., 2022). De sårbara ytorna på fordonet ökar avsevärt i form av nätverk och komponenter, vilket gör uppkopplade fordon mer mottagliga för skadliga attacker. Trenderna mot automatisering och anslutningsmöjligheter i uppkopplade fordon har fört fordonsindustrin in i en ny era av cybersäkerhetsutmaningar (Wang, Y., et al., 2023).

Cybersäkerhet är en väldigt bred term och det kan ibland vara svårt att förstå exakt vad det innefattar. Inom detta arbete kommer cybersäkerhet defineras av: skyddet av elektroniska fordonssystem, kommunikationsnätverk, kontrollalgoritmer, programvara, användare och underliggande data från skadliga attacker, skada, obehörig åtkomst eller manipulation (NHTSA, 2022).

Arbetet kommer måla upp en kartläggning på vart sårbarhetsområdena finns i uppkopplade bilar, samt intressanta förslag på lösningar och framtidsförslag på hur vi kan gå vidare i framtiden. Svaren bygger på en litteraturstudie byggd av deduktiv tematisk kodning. Arbetet har förberetts genom att söka igenom de största databaserna inom området för att sålla ut så relevant information som möjligt. Kodningarna har format teman som besvarar två viktiga delfrågor (som tillsammans knyter ihop kartläggningen). Arbetet kommer besvara vart sårbarhetsområdena finns i uppkopplade bilars infrastruktur och vad det finns för eventuella skyddsmetoder till sårbarheterna. Sammanfattningsvis presenteras ett resultat med tre sammanhängande teman, därefter diskuteras hur samhället kan påverkas av arbetet och varför arbetet är viktigt. Arbetet ger en bred och klar bild i hur cybersäkerhetsmiljön ser ut idag gällande uppkopplade fordon med en bra grund byggd på analys av relevanta och viktiga forskningsartiklar.

1.1 Forskningsfråga

Målet med detta arbete är att få en klarare bild av de olika cybersäkerhetsbrister som råder i dessa nya system. Arbetet bygger en kartläggning av de sårbarheter som kan orsaka problemen, och hur tillverkare kan gå tillväga för att väga förebygga att något går snett till. Arbetet kommer rikta in sig på de konstanta stadie dagens uppkopplade bilar befinner sig i gällande av vilka brister som finns i cybersäkerheten. Arbetet kommer gå ut på att upptäcka vad det finns för sårbarheter i bilars moderna sammankopplade teknik. Det innebär integritetsutmaningar och underliggande system som utsätter cybersäkerheten för sårbarhet. Arbetet kommer genomföras genom att besvara frågorna med hjälp av en litteraturstudie med tematisk kodning där publicerad och relevant forskning granskas. Detta är relevant för att se vilka håll utvecklingen pekar åt och vilka utmaningar som vi borde ta på stort allvar i nutid. Det gäller att se en bred bild av denna cyber-miljö i god tid innan för mycket komplicerad teknik redan är involverat, vilket kan bli svårt att gå tillbaka och ändra på. Det som är intressant och spännande med detta arbetet är vetskapen av en omfamnande värld av ny teknik finns på horisonten, och vi är just i tid för att bevittna hur det spelas ut. Vi kan då också lägga upp för tekniken att ta så bra bana som möjligt. Detta arbete kan i bästa fall bidra till en mer hållbar framtid inom informationstekniken och cybersäkerheten i fordon genom att peka på uppkommande brister, nuvarande sårbarheter och förbättringsmöjligheter. Det ger förståelse för hur cybermiljön ser ut för fordon idag. Målet är att kartlägga de underliggande sårbarheterna som existerar inom uppkopplade bilar, tillsammans med aktuella eller möjliga skyddssystem för sårbarheterna. På så vis kan arbetet även ge en insikt hur vi kan skapa en mer hållbar framtid med denna extraordinära teknik.

Forskningsfrågan är uppdelad i två delfrågor för att lättare bearbeta och förstå området. Delfrågorna är:

- Vart finns sårbarhetsytorna i uppkopplade bilars infrastruktur?
- Vad finns det för eventuella skyddsmetoder till sårbarheterna?

Forskningsfrågan blev uppdelad i dessa två delfrågor för att lättare hantera och förstå informationen. Det är också lättare att dela upp frågan i separata, men ändå sammanhängande delar när det kommer till datainsamling och presentationen då det ger en mer lätthanterlig och lättläst struktur.

1.2 Avgränsningar

I ämnet cybersäkerhet på uppkopplade bilar kommer arbetet att vara begränsat till en viss del av cybersäkerheten, sårbarheter och dess eventuella lösningar eller skydd. Kartläggning av denna delen är viktig för arbetet då den inte endast riktar in sig på attacker av hackare. Detta arbete undersöker sårbara områden inom cybersäkerheten, vilket en vanlig användare inte tänker på. Arbetet kommer alltså inte att rikta in sig på de olika typer av attacker som genomförts, utan punkterna som är sårbara för att bli utnyttjade för attacker, läckor eller systembrister. Information kopplat till aktiva attacker uppkommer endast för att effektivt beskriva ett koncept som är kopplat till något relevant för arbetet. Avgränsningen gäller endast de relevanta delar av varje ämne, alltså vad som är aktuellt idag. Mindre relevanta problem eller gamla typer av cybersäkerhetsfrågor tas inte upp i detta arbete då det finns alldeles för mycket information i ett så brett område. Att viss fakta är mindre relevant avgörs genom att granska omfattningen, och hur bra den stämmer in på resterande information i arbetet. Är det något som sticker ut längre än vad frågan innebär eller om det finns andra tydliga publicerade fortsättningar eller utvecklingar på faktan kan den även anses som irrelevant. Denna avgränsning implementeras med hjälp av inkluderingskriterier.

För att svara på forskningsfrågan är arbetet uppdelat i två olika delfrågor som spelar sina egna roller i arbetet. Inom de olika områdena har sedan avgränsningar gjorts för att få fram den mest relevanta informationen inom varje delfråga. För att samla in så relevant och ny information som möjligt inkluderas endast artiklar skrivna år 2020 eller senare. Detta är ett rimligt år då det som skrivits oftast inte blivit för irrelevant då internationella regulationer gällande cybersäkerhet inom fordon publicerades det året. Samtidigt så bör det finnas en bra andel forskning inom området på de dryga tre åren. Avgränsningen gällande publiceringsår gäller inte på artiklar som beskriver grundläggande koncept eller sätter perspektiv, då publiceringsåret är i så fall irrelevant för att informationen som mest sannolikt inte kommer förändras inom snar framtid. Observera att de utvalda databaserna endast används för att svara på de stora delarna av arbetet. För att förklara olika koncept eller förkortningar i bakgrunden förekommer det relevanta artiklar utanför akademiska databaser. Detta är på grund av att få kort och koncis information om ett specifik liten del som hjälper till att förstå den röda tråden i arbetet.

En annan avgränsning som är bestämd är att inte gå in på det tekniska djupet när det kommer till att redovisa de olika säkerhetsmetoderna, eller möjliga cyberattacker. Det kommer ske nyttig och väl informativ information och bakgrund hur de olika komponenterna fungerar och samspelar, men det är i slutändan endast själva konceptet vad de olika systemen gör som är intressant. Det är därför en avgränsning att fokusera mer på vad systemen gör i ett samspel, och mindre exakt hur tekniken bakom fungerar om det inte är en relevant bit i analysen. En relevant teknisk del skulle kunna vara något som är fundamentalt i systemet som avgör varför det fungerar i samspelet.

Arbetet kommer först presentera bakgrundsinformation för att ytterligare redovisa varför arbetet är viktigt, och allmän relevant information inom uppkopplade bilar idag. Det kommer även presenteras en lista av viktiga termer och koncept för att förstå

arbetet i sin helhet. En metod redovisas för att visa hur arbetet gick till väga vid datainsamling, kodning etc, och varför metoden är vald. Till sist kommer resultaten av arbetet presenteras i form av hur källorna bidrar till forskningsfrågorna, vad resultaten betyder och varför arbetet är viktigt för framtiden.

2 Bakgrund

Ett viktigt framsteg i bilbranschen är anslutna och självkörande bilar , som bidrar till ett säkrare, smartare och effektivare transportsystem. Dessa bilar har många positiva effekter på både samhället och miljön, som färre trafikolyckor, mindre trängsel på vägarna, lägre utsläpp av skadliga ämnen osv. Den moderna tekniken medför också vissa risker för säkerheten. En av dem är hotet från cyberangrepp. Vanliga bilar är inte så utsatta för sådana attacker, men uppkopplade bilar kan lätt hackas eftersom de har kontakt med infrastrukturen runt omkring sig och andra bilar (Elliott et al., 2019). För att kunna uppfatta sin omgivning bättre har uppkopplade fordon avancerade sensorer och enheter som datorer ombord, kameror etc. Sensordata från dessa enheter kan störas eller ändras av hackare, terrorister eller sabotörer som också kan ta över kontrollen över bilen genom cyberangrepp. Bilbranschen behöver därför skapa ett starkt skydd mot cyberintrång för att göra uppkopplade fordon till ett tryggare och mer pålitligt sätt att resa. Den moderna bilen är en dator på fyra hjul. Dagens bilar bearbetar och överför ständigt data om sig själva, sin omgivning och människorna i den. Detta sker i de flesta fall utan förarens vetskap. Datan används i navigering, för att hantera bilsystem som motorn eller för att leverera kommunikations och informationstjänster till passagerare (EDPS, 2019).

Det finns flera typer av känslig data som samlas in och behandlas av uppkopplade bilar. Data som samlas in är till exempel personlig information, fordonsinformation, lokalisering och körbeteende (Nawrath, T. et al., 2017).

Det är absolut nödvändigt att mildra sårbarheter för att upprätthålla fordons cybersäkerhet. Utnyttjande av sårbarheter kan resultera i avslöjande av integritet, ekonomisk förlust eller till och med mänsklig skada eller problem med allmän säkerhet. Samtidigt i de förordningar och standarder som nyligen utfärdats så uppmanas tillverkare att svara inom en rimlig tidsram när det gäller cybersäkerhetssårbarheterna inom fordon (Wang, Y., et al., 2023).

Uppkopplade fordon delar en stor mängd data för att få korrekt uppkoppling och uppfatta rätt information från omgivningen. Delande av data gör dessa fordon sårbara för fysiska attacker och cyberattacker. Konsekvenserna av attacken mot dessa fordon kan vara dödliga och även skadliga för infrastrukturen. Det sätter många saker på spel som förarens integritet, liv och säkerheten för andra fordon och infrastruktur (Yadav, N., et al., 2022).

Det är ofta inte bara själva bilen som är en sårbarhet i sig, det kan även gälla uppkopplade mobilappar utan intrångsskydd som är kopplade till fordonet. När du köper en bil är det viktigt att se till att den tidigare ägaren är bortkopplad från användarkontot (Kaspersky, 2017).

Vissa uppkopplade fordon skulle kunna jämföras med vanliga datorer med betydligt mindre beräkningskraft. Således kan anslutna fordon utnyttjas “baklänges” för att komma åt själva infrastrukturen (Kumar, S., et al., 2021).

2.1 Datakommunikation

2.1.1 CAVs (Connected Automated Vehicles)

Connected Automated Vehicles (CAV) innebär fordon som kan ersätta föraren för vissa eller alla köruppgifter (Ferrovial, 2023). En ansluten bil är ett fordon som använder internetanslutning för att kommunicera med externa system. Dessa system kan innehålla appar som kan låsa upp din bil, GPS och fordon till fordonskommunikation (Powers, J., 2022).

2.1.2 ECU (Electronic Control Unit)

En styrenhet för ett fordon eller en ECU (Electronic Control Unit) är en elektronisk enhet med hårdvara och programvara som styr ett eller flera funktionsområden i ett fordon. Syftena är att erbjuda fler och bättre funktioner för användarna av fordonen och att reducera kablarna så att kostnaderna minskar. Styrenheten är kopplad till och kontrollerar andra elektroniska komponenter i bilen. Det agerar som hjärtat i bilen och ser till att bilen fungerar optimalt. Detta inkluderar spjällhus, turbotryck och andra komponenter (Wikipedia, 2023).

Varje ECU ansvarar för en deluppgift i ett fordon och är sammankopplade via en gemensam buss som kallas “CAN Bus” (Kumar, S., et al., 2021).

Nätverket i fordonet hänvisar till det lokala kommunikationsnätverket som består av elektroniska styrenheter (ECU) och olika bussprotokoll, som kan realisera överföringen av olika statusinformation och styrsignaler (Luo, F., et al., 2021).

Dagens fordon kan innehålla 100 eller fler styrenheter som styr funktioner som sträcker sig från det väsentliga som motor och servostyrning till komforts som säten och ventilation, till säkerhet och åtkomst(som dörrlås och nyckelfri entré. ECU: er styr också passiva säkerhetsfunktioner, som airbags, och till och med grundläggande aktiva säkerhetsfunktioner, som automatisk nödbromsning. Varje ECU innehåller vanligtvis en dedikerad chip som kör sin egen programvara eller firmware och kräver ström- och dataanslutningar för att fungera. En ECU tar emot ingångar från olika delar av fordonet, beroende på dess funktion. Till exempel skulle en dörrlås-ECU ta emot ingång när en passagerare trycker på dörrlås/upplåsningsknappen på en bil eller på en trådlös nyckelbricka. En airbag-ECU skulle ta emot ingångar från kraschsensorer och från sensorer som upptäcker när någon sitter på en särskild stol. Och en automatisk nödbroms-ECU skulle ta emot ingångar från framåtvända radar som upptäcker när fordonet närmar sig ett hinder för snabbt (Aptiv, 2020).

2.1.3 Moderna, smarta bilar

Den nya tekniken som finns i smarta bilar ligger i takt med transformationen från 4G till 5G. Det kommer att vara hyper-uppkopplat och totala cloud-baserade nätverk och applikationer. Istället för en radio-anslutning åt gången kommer det vara flera samtidigt. Nätverket kommer delas upp i olika delar som riktar in sig på olika behov.

4G var första steget till molnbaserade anslutningar. Med 5G tas steget mot självkörande och helt sammankopplade fordon (EY, 2020).

Kontrollsystemen i en bil genererar i snitt över 2 miljoner händelser per dag. Vad skulle hända om något meddelande i systemet inte fungerar som det ska, eller blir manipulerat? Cybersäkerheten i bilsystemen behöver säkerställas, vare sig det gäller kritisk infrastruktur eller potentiellt dödliga mekanismer (Javier, F., 2022).

2.1.4 IOT (Internet Of Things)

IoT står för "Internet of Things" vilket innebär att fysiska enheter som är anslutna till internet kan samla och utbyta data med varandra. Detta kan ske genom sensorer som är inbyggda i enheterna och som samlar in data som sedan kan användas för att styra eller övervaka enheterna. Det relevanta sammanhanget i detta arbete är fordonskomponenter som är uppkopplade, vilket gör dem en del av IoT (IoT Sverige, 2023).

2.1.5 IPFS (Interplanetary File System)

IPFS står för InterPlanetary File System och är ett distribuerat filsystem som används för att lagra och hämta filer på ett sätt som är oberoende av plats och enhet. IPFS kan användas i samband med uppkopplade bilar för att lagra och hämta data från ett distribuerat nätverk av datorer istället för att lagra all data på en centraliserad server. Detta kan öka säkerheten och minska risken för dataförlust om en server går ner eller hackas (volkswagen, 2023).

2.1.6 Back Box

En "black box" är en elektronisk enhet som används i fordon för att samla in data om hur fordonet har använts. I en bil används black-boxen för att spela in information om hastighet, bromsning och andra parametrar som kan hjälpa till att avgöra vad som hände vid en olycka (Parling, A., 2011).

2.1.7 OBD (On-Board Diagnostics)

OBD är ett system som kan hjälpa mekaniker och bilägare att få tillgång till status på systemen i ett modern fordon. För att läsa av OBD används en OBD läsare. Med den nyare generationen OBD2 finns det fler standardiserade felkoder. Det går även att ansluta till systemet via bluetooth eller nätverk
(MyCarly, 2023). Det gör det möjligt för alla bilens yttre elektronik att kommunicera med den. När det gäller bränsleövervakning, motortemperatur, föroreningskrav etc. är denna pryl avgörande. Tillsammans med att fungera som ett pålitligt bilövervakningssystem, används OBD-enheten mest för att avgöra om fordonet fungerar effektivt eller inte (Yadav, N., et al., 2022).

OBD-II är avsedd att användas som ett diagnostiskt hjälpmedel för tekniker för mer avancerad fordonstelematik. Den används också för att hämta data från bilens OBD-II-anslutning för att analysera körvanor och ge en "rabatt" för lågriskbeteende (Malik, S. & Sun, W., 2020).

2.1.8 Hur IoT och bilar hänger ihop - IoT 5G

För att förstå vart saker kan gå fel är det även viktigt att förstå hur saker och ting är sammankopplat. Många av de traditionella cyber-säkerhetslösningar som brandväggar och simpla antivirusprogram kommer inte vara effektiva längre. För att framtiden ska vara säker och kunna blomstra inom branschen så är cybersäkerhet den uppenbara nyckeln till framgång. “Cybersecurity är en hörnsten av ansluten rörlighet.” - Matthias Bandemer (EY Cybersecurity Leader).

IoT sträcker sig brett inom uppkopplade fordon. Exempel på funktioner som del av uppkopplade bilar är till exempel:

- Prediktiv vetskap om när bilen behöver underhåll och service.
- OTA (Over The Air), där du får viktiga mjukvaruuppdateringar.
- Autonomisk körning (självkörande fordon).
- Avancerad navigation.
- Övriga interiöruppleveIser.

För att säkerställa skydd mot de komplexa hot som råder på IoT-ekosystem, krävs det att biltillverkare implementerar säkerhetsåtgärder vid hela livscykeln av uppkopplade fordon. Säkerhetsfrågor som måste tas upp inkluderar:

- Säker produktion.
- Etablering av mjukvara.
- Säkerhetshantering.
- Enhetsautentisering.
- Datasäkerhet.
- Enhetsbunden identitet.
- Enhetsbunden datasäkerhet.
- Intergration (med mobil-applikationer).
- Avveckling.
- Återupptagande i drift (om bilens ägare skulle ändras).

Trots den positiva utvecklingen av IoT så kvarstår cybersäkerheten som ett primärt hinder i integrationen. Det förväntas vara cirka 75 miljarder IoT enheter vid 2025 (EY, 2020), varav 400 miljoner är uppkopplade bilar (Placek, M., 2021). vilket är extremt betydelsefullt för cybersäkerheten. Vid 2020 visade det sig att 25% av alla cyberattacker riktades mot IoT-enheter. Samtidigt så får IoT mindre än 10% av säkerhetsbudgeten inom IT. Redan i 2020 stöter en uppkopplad bil på 300 000 cyberattacker per månad, av 3500 olika hackare. Angripare finns i olika former och är ofta bots som söker efter eventuella styrenhetssårbarheter som de kan avslöja för att få kontroll över det anslutna systemet. Enligt (EY, 2020) behöver problemen lösas i olika dimensioner eller “lager”. Först måste det lösas på det tekniska lagret, sen på organisations-lagret. På det tekniska lagret måste bilen och användaren av bilen identifieras så det är säkert att anslutningen är avsiktlig. Det måste införas policys för tillgång av applikationerna i bilen. Detta innebär nätverket i bilen, kopplingen från bilen till molnet, vad som finns i molnen etc. Det krävs ett säkerhetskoncept som dynamiskt kan reagera och angripa på cyberattacker i en skiftande miljö. På organisationslagret krävs det ett integrerat ledningssystem som arbetar med det komplexa systemet och sätter alla delar under ett tak. Det innebär cybersäkerhet, riskhantering och överensstämmelse i ett system där både de tekniska och organisations-aspekterna finns (EY, 2020).

Data som lagras tar form av många attributer som plats, motorstatus, hastighet, om en dörr är låst etc. Bildata genereras från fordonets elektroniska styrenheter, Controller Access Networks och till och med infotainmentsystem. (Jim Vurpillat, 2021).

En av de största utmaningarna för uppkopplade bilar är dataskydd. Precis som med alla tekniska framsteg som bygger på att samla in stora mängder data finns det oro för integritet. Om data samlas in om hur fort du kör och hur ofta du bromsar, är det inte troligt att ditt försäkringsbolag skulle betala en stor summa för att få tillgång till den?

Eftersom biltillverkarna i allmänhet kontrollerar datan bör konsumenterna utbilda sig så mycket som möjligt. En passande fras är "När du köper en bil överlämnar du dina uppgifter till din biltillverkare". Det är biltillverkarens ansvar att se till att de behandlar dina data på "rätt sätt". Samtidigt ökar dataskyddsregleringarna i takt med ökande datamängder och skyddsfrågor. Den kaliforniska konsumentdataskyddslagen trädde i kraft i januari 2020 och har potential att bli en de facto-standard för biltillverkare i USA. På andra sidan Atlanten har den allmänna dataskyddsförordningen varit i kraft sedan 2018. Den ger konsumenterna större kontroll över sina data och ger en ram för tunga böter mot företag som bryter mot protokollet (Stephen Gossett, 2022).

Data kan lagras lokalt i bilen och i molnet. Det är inte bara kördata som kan bli lagrat, även information om personen och dess enheter. Data kan samlas in från bilen och synkade mobila enheter. Det kan inkludera: namn, adresser, telefonnummer, mejl, betalningsinformation, körkort mm. Om den uppkopplade bilen levereras komplett med en egen applikation, kommer all information som skickas automatiskt att kopplas till bilen och hjälper till att bygga en profil av användaren, särskilt när detta matchas med data från infotainmentsystemet i bilen.

Information som samlas in om fordonet inkluderar: Telematikloggdata, inklusive prestandaanvändning, infotainmentsystemdata, hastighetsinformation, batterianvändningshantering och vägmätaravläsningar. Det samlas även in fjärranalysdata, inklusive kontakter, webbhistorik och navigationshistorik och fordonets aktuella plats. Säkerhetsanalysdatan som samlas in inkluderar olycksdata, start och stopphistorik mm.

Det finns fyra parter som kan komma åt användarens uppgifter, både lagligt och olagligt, inklusive:

Biltillverkare: Den mest uppenbara parten som kan komma åt din data är tillverkaren av din bil. På grund av att data finns på deras servrar har de direktåtkomst.

Det finns två typer av tredje parter som bilföretag delar information med: Tredje parter som föraren bestämmer sig för att auktorisera. Tredje parter som tillverkare är skyldiga att dela data med enligt lag, till exempel polisen om föraren är inblandad i en olycka.

Nästa ägare: Om informationen är lagrat lokalt på bilens interna system och föraren glömmer att radera det innan bilen får ny ägare. Den nya ägare kan ha tillgång till den privata informationen.

Hackare: Uppkopplade bilar har oftast data lagrat i molnet. Det finns alltid liten risk att hackare kan komma åt informationen om användaren inte är försiktig med säkerhetsinställningarna, till exempel lösenord (Abhilasha Singh, 2021).

"It's time for people to treat their cars like a computer or a smartphone. They do not specify data sharing and use practices, and they offer limited individualized controls to consumers. In the end, consumers had trouble understanding how they can limit the data that is being shared." (Lauren Smith, 2021).

2.1.9 V2X (Vehicle-To-Everything)

Uppkopplade bilar har tillgång till Internet och innehåller vanligtvis någon form av trådlöst LAN. Specialtjänster i dessa bilar använder internet för att tillåta ytterligare funktioner för förare. Den här kommunikationen är märkt som fordon-till-allt (V2X) i allmänhet, och inkluderar fordon-till-fordon (V2V), fordon-till-passagerare (V2P) och fordon till infrastruktur (V2X). Tjänsterna inkluderar förarsäkerhet, meddelanden relaterade till krockar och fortkörning, infotainment i fordon etc. Tyvärr innebär tillgängligheten till Internet också en sårbarhet som kan bli måltavla för externa hot (Bajpa, P., et al., 2020).

V2X-tekniken tillåter uppkopplade fordon att dela information med varandra, men även med saker som trafikljus, vägskyltar och annan infrastruktur. Detta är för att förbättra säkerheten och göra körupplevelsen mer effektiv. Till exempel kan ett uppkopplat fordon få en varning från ett annat fordon om en potentiell olycka framför eller information från ett trafikljus om när det kommer att ändras till grönt. Men som med all teknik som förlitar sig på datainsamling och delning finns det oro för digital integritet och cybersäkerhet. Eftersom uppkopplade fordon ständigt skickar och tar emot information om plats, hastighet och annan data så finns det en risk att informationen kan kommas åt eller användas av obehöriga parter och att fordonets system blir kompromissat (Cali, U., et al., 2023).

2.1.10 V2V (Vehicle-To-Vehicle)

Vehicle-to-vehicle (V2V) gör det möjligt för fordon att trådlöst utbyta information om sin hastighet, plats och riktning. Tekniken bakom V2V-kommunikation gör att fordon kan sända och ta emot data från alla håll (upp till 10 gånger per sekund), vilket skapar en 360-graders "medvetenhet" om andra fordon i närheten. Denna teknik kan förhindra olyckor genom att tillåta ett fordon att utbyta information i realtid. Fordon utrustade med lämplig programvara kan använda meddelanden från omgivande fordon för att fastställa potentiella krockhot när de utvecklas. Tekniken kan sedan använda visuella, taktila och hörbara varningar för att varna förare. Dessa varningar ger förare möjlighet att vidta åtgärder för att undvika krascher. Dessa V2V-kommunikationsmeddelanden har en räckvidd på mer än 300 meter och kan upptäcka faror som skyms av trafik, terräng eller väder. V2V-kommunikation utökar och förbättrar för närvarande tillgängliga system för undvikande av kraschar som använder radar och kameror för att upptäcka kollisionshot. Den här nya tekniken hjälper inte bara förare att överleva en krasch, den hjälper även att undvika kraschen helt och hållet. Fordon som kan använda V2V-kommunikationsteknik sträcker sig från bilar och lastbilar till bussar och motorcyklar. Även cyklar och fotgängare kan en dag använda V2V-kommunikationsteknik. för att förbättra deras synlighet för bilister. Tekniska kontroller finns tillgängliga för att avskräcka fordonsspårning och manipulering av systemet. V2V-kommunikationsteknik kan öka prestandan hos fordonssäkerhetssystem och hjälpa till att rädda liv. Det uppskattningsvis inträffade 6,8 miljoner polisrapporterade krascher under 2019, vilket resulterade i 36,096 dödsfall och uppskattningsvis 2,7 miljoner människor skadades. Teknik för uppkopplade fordon kommer att ge förarna de verktyg de behöver för att förutse potentiella olyckor och avsevärt minska antalet förlorade liv varje år (NHTSA, 2022).

Fordon-till-fordon-kommunikation (V2V) kommer att förbättra trafiksäkerheten, eftersom den gör det möjligt för bilar att interagera och överföra information som GPS, hastighetsdata för att hjälpa förare att undvika olyckor, filbyte och mycket mer. Fordon kan reagera på varandra och kommunicera mer effektivt genom att förbli sammankopplade. V2V möjliggör viktiga säkerhetsapplikationer som nödbromsljus, kooperativa kollisionsvarningar, döda vinklar och stöd för filbyte (Wang, Y., et al., 2023).

2.1.11 V2I (Vehicle To Infrastructure)

V2I är istället för kommunikation mellan olika fordon, innebär det kommunikation mellan fordon och infrastruktur. V2I, fångar in data som trafikstockningar, vädermeddelanden, brofrigångsnivåer, trafikljusstatus och sänder den sedan trådlöst för att informera förare om förhållanden som de behöver vara medvetna om vilka hjälper till med säkerheten. Smarta trafiksignaler som drivs av V2I hjälper förare att förstå trafikförhållandena bättre, vilket hjälper till att uppskatta exakta ankomsttider (Kevin Aries, 2021).

2.1.12 LiDAR (Light Detection and Ranging)

Ett LIDAR-instrument består huvudsakligen av en laser, en skanner och en specialiserad GPS-mottagare. Den har egenskap att generera exakt, tredimensionell information om jordens form och dess ytegenskaper. Flygplan och helikoptrar är de mest använda plattformarna för att skaffa LIDAR-data över stora områden. LIDAR-system tillåter bland annat forskning och kartläggning med undersökning av både naturliga och konstgjorda miljöer med noggrannhet, precision och flexibilitet (National Oceanic and Atmospheric Administration, 2023).

LiDAR-teknologi är en avgörande komponent i moderna självkörande bilar. Den mäter avståndet till föremål i bilens omgivning genom att mäta flygtiden för en laserstråle som projiceras vertikalt mot marken. Denna data används sedan för att bestämma närvaron av ett föremål och dess avstånd från bilen, vilket gör det möjligt för bilen att lokalisera sig själv, undvika hinder och navigera. Därför är säkerheten för självkörande bilar starkt beroende av effektiviteten hos LiDAR-systemen (Volvo, 2020).

2.1.13 VANET (Vehicular Ad Hoc Network)

VANET är en förkortning för Vehicular Ad Hoc Network, vilket innebär ett trådlöst nätverk av fordon som kan kommunicera med varandra utan att behöva en central infrastruktur. VANETs kan användas för att förbättra trafiksäkerheten och informationsutbytet mellan fordon (Kugali, S., 2020). Fordonen eller andra enheter fungerar som noder och bildar ett litet nätverk. Varje nod delar den information den har, och efter att ha skickat sina egna data tar emot data som skickas av andra noder. V2V som nämnts tidigare i arbetet är den del av ett VANET nätverk (Techironed, 2022).

2.1.14 OTA (Over The Air)

Over-the-air-uppdateringar är snabba och bekväma programuppdateringar. Over-the-Air-teknik gör att vissa programuppdateringar för vissa fordonskomponenter kan laddas ner och installeras via en trådlös anslutning (Malik, S. & Sun, W., 2020).

2.2 Regulationer

2.2.1 Riktlinjer för personuppgifter

2020 kom riktlinjer om behandling av personuppgifter i samband med uppkopplade fordon och rörlighetsrelaterade applikationer. Riktlinjerna är utgivna av Europeiska dataskyddsstyrelsen (EDPB). Riktlinjerna syftar till att ge vägledning om hur dataskyddsreglerna ska tillämpas på behandling av personuppgifter i samband med uppkopplade fordon och rörlighetsrelaterade applikationer. Riktlinjerna omfattar behandling av personuppgifter som utbyts mellan fordonet och personliga enheter som är anslutna till det, till exempel smarttelefoner, samt uppgifter som samlas i fordonet och delas med tredje part, till exempel fordonsleverantörer, försäkringsbolag eller myndigheter.

Riktlinjerna betonar att behandlingen av personuppgifter i samband med uppkopplade fordon och rörlighetsrelaterade applikationer måste följa principerna om laglighet, ändamålsbegränsning, minimering, noggrannhet, lagringstidsbegränsning, integritet och konfidentialitet. Riktlinjerna ger också rekommendationer om hur man säkerställer att de registrerade rättigheterna respekteras. Till exempel rätten till information, åtkomst, rättelse, radering och invändning. Riktlinjerna innehåller även exempel på god praxis och riskbedömningar för olika typer av behandlingar (EDPB, 2023).

Dataskydd är viktigt av flera anledningar. För det första handlar det om att skydda den enskilde människans personliga integritet, som är en del av vår rätt till privatliv. För det andra hjälper dataskydd till att förebygga dataintrång, läckage och missbruk av personuppgifter, som kan leda till ekonomiska förluster, identitetsstöld eller andra skador. För det tredje bidrar dataskydd till att upprätthålla förtroendet mellan medborgare, kunder, anställda och organisationer som behandlar personuppgifter. För det fjärde kräver dataskyddslagstiftningen att organisationer som behandlar personuppgifter följer vissa principer och regler för att säkerställa en laglig, ändamålsenlig och transparent behandling (Svensk Handel, 2023).

2.2.2 WP.29 Cybersecurity Regulations

"WP.29 Cybersecurity Regulations" är en internationell standard som antogs i juni 2020 av FN:s ekonomiska kommission för Europa (UNECE) för att reglera cybersäkerhet i fordon. Denna standard ger fordonssektorn en ram att sätta upp processer för att identifiera och hantera cybersäkerhetsrisker i fordonets design, verifiera att riskerna hanteras, se till att riskbedömningar hålls aktuella och att övervaka attacker.

WP.29 Cybersecurity-bestämmelserna godkändes i juni 2020. De ger fordonssektorn ett ramverk för att införa processer för att:

• Identifiera och hantera cybersäkerhetsrisker i fordonsdesign

• Verifiera att risker hanteras

• Se till att riskbedömningar hålls aktuella

• Övervaka attacker och svara på dem

• Analysera lyckade eller försök till attacker

• Se över cybersäkerhetsåtgärder mot bakgrund av nya hot

• Säkerställa säkerhetslivscykelhantering (över utvecklings, produktions och efterproduktionsfaserna)

Det är uppenbart att WP.29-reglerna ger viktiga riktmärken för intressenter när det gäller cybersäkerhetsstandarder för fordon.

Cybersäkerhet för bilar börjar med 3 viktiga sårbara områden:

1. Fordonet
Det finns mängder med elektroniska styrenheter i en ansluten bil. Styrenheterna skickar data via luften eller till och med via fysiska medier (som fobs och USB-minnen). Alla sårbarheter här kan utnyttjas av angripare.

2. Kommunikationsskiktet
Fordonsdata under transport ger en annan möjlighet för hackare, vilket leder till distribuerade överbelastningsattacker (DDoS), spoofing och andra dataintrång.

3. Applikationsskiktet
Uppenbarligen har all denna fordonsdata en slutdestination, från stadsmyndigheter till underhållningsleverantörer och mer. Stark cybersäkerhet behövs för att säkerställa att endast auktoriserade enheter kan komma åt data, och att dessa intressenter skyddar sina egna system (Thales, 2023).

Denna standard är obligatorisk för alla nya fordonstyper i EU från juli 2022 och kommer att bli obligatorisk för alla nya fordon som produceras från juli 2024 (Kilian Marty, 2021).

2.3 Cybersäkerhetsaspekter

2.3.1 Blockchain

En blockchain är en distribuerad databas som lagras i många kopior. Det lagras en på varje nod i ett peer-to-peer-nätverk. De många kopiorna samt en sekvens av kryptografiska hashfunktioner gör det svårt eller omöjligt att i efterhand manipulera databasens historik. Tekniken används för att skapa en säker och transparent logg över transaktioner och andra händelser (kryptomagasin.se, 2021).

2.3.2 DO-ABE Blockchain

DO-ABE är en blockchain-baserad modell för fordonsdata, tillsammans med ett datadelningsschema, som använder blockchain-baserad dataägarbaserad

attributbaserad kryptering eller “data-owner-based attribute-based encryption” (DO-ABE).

Uppkopplade bilar är till för att skapa en tvåvägs-nätverkskommunikation mellan fordon och all infrastruktur. Det finns stort behov av att utveckla specifika processer för hantering för säker och effektiv datadelning, samt transaktioner mellan fordons nätverk. Speciellt nu när “black boxes” blir allt mer vanligt i fordon.

Ett förslag till att verkliggöra detta är en krypterad blockchain-baserad modell. Den föreslagna modellen uppnår de grundläggande kraven för konfidentialitet och integritet. Systemet hanterar på ett säkert och effektivt sätt en stor kapacitet med integritetskänslig black-box video data genom att lagra metadatan på blockchain (on-chain) och kryptera den råa datan externt (off-chain). Detta i ett “consortium blockchain”. Dessutom kan dataägarna av den föreslagna modellen kontrollera sin egen data genom att använda den Blockchain-baserade DO-ABE och ägardefinierade åtkomstkontrollistor.

Transaktioner som utförs på en blockchain kallas “on-chain” transaktioner och erbjuder större säkerhet och transparens eftersom de är verifierade och registrerade på en offentlig distribuerad reskontra som inte kan ändras. Men on-chain transaktioner kan inkludera höga avgifter och långsamma behandlingstider beroende på nätverkets verifieringsmetod. Off-chain-transaktioner bekräftas utanför blockchain-nätverket, vilket ofta resulterar i en billigare och snabbare process för användaren. Block som läggs till i en off-chain-kedja kan inte ändras, så att arbeta utanför blockkedjan gör ett nätverk mer sårbart för bedräglig aktivitet (Coindesk, 2022).

2.3.3 BLOCKCHAIN-KONSORTIUM

Ett blockchain-konsortium är en grupp organisationer som samarbetar för att driva ett blockchain-nätverk tillsammans. Dessa organisationer har vanligtvis ett gemensamt mål eller en uppsättning mål relaterade till användningen av blockchain-teknik, och de arbetar för att underhålla och styra nätverket. Konsortier kan användas för en mängd olika ändamål, som att skapa ett delat system för hantering av försörjningskedjan eller ett decentraliserat digitalt identitetssystem. Privata blockkedjor används vanligtvis av företag för specifika mjukvarulösningar och för att möta specifika affärsbehov. Offentliga blockkedjor är öppna för allmänheten och kan nås av alla med en internetuppkoppling. Ett blockchain-konsortium är en kombination av offentliga och privata egenskaper och används mest inom ett företag eller en grupp av organisationer (DATA CONOMY, 2023).

3 Metod

Som skrivet innan, målet med arbetet är att få till en klar relevant bild hur cybersäkerhetsmiljön ser ut idag gällande sårbarheterna i uppkopplade bilar. Metoden för detta arbete kommer ta form av en litteraturstudie då det finns mängder med ny intressant information kring ämnet. En annan anledning är att tillgång till egna experiment inte är möjligt, då det saknas tillgång till uppkopplade bilar eller verktyg som behövs för att kunna experimentera eller analysera dem. En intervjustudie kunde varit en legitim metod för forskningsfrågan, men används inte i detta arbete av två

anledningar. Först och främst fanns det inte någon kvalificerad och tillgänglig person att få tag i. Den andra anledningen att inte göra en intervju är att då får arbetet en mycket smalare syn på ämnet, vilket kräver en mer omfattande kropp av text. En intervju skulle dock kunna komplettera arbetet om det var tillgängligt, något som definitivt skulle kunna ge bra insikter till ett framtida arbete. Arbetet kommer att bygga på befintlig forskning kring uppkopplade fordon, med inriktning på sårbarheter och dess eventuella lösningar. Arbetet kommer att planeras med hjälp av tre steg där forskningsfrågor, sökord och databaser fastställs. Informationen sorteras sen i form av tematisk kodning med hjälp av en 6-stegs-process. Målet är att läsa och sålla ut viktig information om inriktningen från olika källor och knyta ihop en analyserad samlad bild hur miljön ser ut idag för sårbarheterna i uppkopplade bilar och dess möjliga skydd i cybersäkerheten. I slutet representeras alla teman i form av en rapport av sammanhängande struktur.

Litteraturstudien är inspirerad av hur (Kitchenham, 2004) beskriver konstruktionen av metoden. Det tre viktigaste stegen att följa är att först planera undersökningen, genomföra undersökningen och till slut rapportera resultaten. Litteraturstudier kan ge insikt om den utvärderade informationen stödjer befintliga eller nya hypoteser. Det kan också ge en bra grund för framtida arbeten och kommande ny forskning. Att kunna skapa nya hypoteser och se hur bakgrunden stämmer in på resultaten är en viktig del av detta arbete. Det viktigaste för detta arbete kan dock vara framtidsaspekten, att ge en grund för kommande arbeten som kan ta nytta av kartläggningen i litteraturstudien.

Metoden i arbetet kommer att underlätta processen genom att ta stöd av mindre akademiska källor som bygger på vad (Kitchenham, 2004) hävdar. Detta är för att lättare förstå och strukturera upp metoden i arbetet. Arbetet kommer följa en vägledning som (Paré & Kitsiou, 2017) föreslår, där arbetet ska byggas upp i följande ordning:
-Formulera en frågeställning eller ett syfte
-Utföra litteratursökningar
-Tillämpa inklusionskriterier
-Kvalitetsbedömning
-Extrahera data
-Analysera data

3.1 Datainsamling

I det tidiga stadiet av arbetet definieras forskningsfrågan och dess omfattning. Det är viktigt att tidigt ha en klar bild av vad som omfattar frågan och vilka avgränsningar som behövs.

1. **Formulering och avgränsning av forskningsfråga.** Det blir mer strukturerat och effektivt att göra sökningar efter en väl definierad och avgränsad forskningsfråga. I detta steg är det också viktigt att plocka ut huvudbegreppen i frågan, som sen kommer bra till hands i kommande steg. Det skrivs ner relevanta delfrågor för att bryta ner forskningsfrågan i mindre delar, vilket underlättar strukturen på arbetet.

2. **Hitta sökord och skapa sökblock.** Innan fastställda sökord och sökblock

sker det testsökningar där olika fraser körs för att hitta och fastställa passande nyckelord. Det görs genom att se tidigare forskning och relaterade artiklar, och vad för ord som används i rubrikerna och taggarna. Här byggs det upp olika sökfraser som täcker de viktiga huvudbegreppen i forskningsfrågan.

3. **Val av databaser.** För att hitta ett gäng av databaser att använda sker sökningarna i Google Scholar vilket är en sökmotor för akademiska databaser. Målet är att hitta minst två olika databaser med kvalitetskontroll och bra med artiklar kring ämnet.

De tre stegen är förberedelserna inför analysen och är inspirerade av en guide på systematisk litteraturöversikt (Universitetsbiblioteket, 2023). Dessa stegen speglar även mycket av vad (Wohlin, 2012) hävdar, vilket kommer att vara i åtanke under datainsamlingen och hela analysfasen till den systematiska litteraturanalysen för att få en så pålitlig process som möjligt. De mindre akademiska källorna är använda för att få en mer lätthanterlig bild av stegen.

3.2 Analys och kodning

För att ge arbetet en tydlig beskrivning av analysmetoden och därmed ge en högre nivå av reproducerbarhet följs en analysprocess som bygger på och är inspirerad av (Wolfswinkel et al., 2013). Den tematiska analysen följer en populär 6-stegs-process (Paperpile, 2023); (Scribbr, 2023). Processen används då det är en rimlig och effektiv lösning att presentera forskningsfrågan i en sammanhängande och logisk struktur.

6-stegs-process:

1. **Insamling av data.** Här skapas en bekantskap med datan som bygger upp hur inriktningen av arbetet kommer bygga på.

2. **Kodning av data.** Av den insamlade datan sållas ut delar som representerar relevant mening eller intresse som berör forskningsfrågan.

3. **Generera teman.** Koderna undersöks och den insamlade datan identifierar ett bredare mönster av mening för arbetet, detta då i form av teman och relevant data till varje tema.

4. **Granska teman.** Teman kontrolleras om det funkar i samband med de kodade utdragen och datan för att se om de fångar upp essensen av forskningen.

5. **Definiera teman (och namngivning).** Här utvecklas en detaljerad beskrivning av varje tema som beskriver dess huvudsakliga idé.

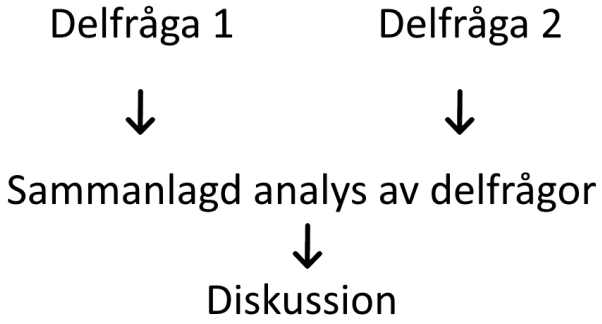
6. **Skriv upp rapporten.** Här presenteras alla teman i en sammanhängande struktur med stöd från datan som relaterar till forskningsfrågan och litteraturgranskningen.

I insamlingsprocessen av data har de relevanta styckena och delarna av varje artikel samlats i ett stort dokument. Vid detta stadie hålls delfrågorna i arbetet i åtanke för att lättare kunna sålla information. I varje stycke skrivs en sidokommentar som kort förklarar styckets innehåll för att snabbt kunna känna igen innehållet. När alla stycken är kommenterade börjar teman genereras genom att undersöka de mönster som finns i de olika delarna. Styckena delas upp i olika teman beroende på hur innehållet relaterar till vart annat. Efter att teman har genererats granskas de olika styckena för att slå fast att de kodade uttagen passar in och är nog för att svara på forskningsfrågan. Om det skulle vara kort om information eller bristande svar genomförs insamlingen av data på nytt med tanke på de saknade länkarna. När alla teman är granskade defineras de till olika punkter som namnges efter relevant område. Det skrivs en beskrivning av vad temat innebär och varför temat är viktigt för arbetet, samt vilken delfråga i arbetet den svarar på. Till sist presenteras datan i form av en rapport som knyter samman alla teman för att få ett strukturerat svar på forskningsfrågan.

Figur 1 presenterar en simpel modell på hur arbetet kommer gå till. Innan den här modellen implementeras sker allmän undersökning kring bakgrunden där varje delfråga blir definierad. (Se kapitel “analys”.) För varje delfråga appliceras modellen:

Figur1 - processmodell - Författarens egna

När varje delfråga är analyserad och redovisad implementeras den andra delen av modellen. Alla samlade kodade stycken knyts ihop för att sedan kombineras. Med hjälp av de sammanknutna delfrågorna byggs resultatet fram som ska ge en bild på hur cybermiljön i uppkopplade bilar ser ut idag gällande sårbarheterna och dess eventuella lösningar..



Figur2 - resultat modell - Författarens egna

Målet med metodiken är att svara på alla delmål med så relevant information som möjligt. Informationen kommer att presenteras på ett strukturerat sätt där varje punkt beskrivs och kopplas till forskningsfrågan. I slutet knyts säcken ihop och arbetet lägger upp en bredare vinkel på hur helheten ser ut i dagsläget.

3.3 Val av källor

För att uppnå en så relevant bild som möjligt prioriteras nyare artiklar med utgångsår 2020 och framåt. Valet av 2020 som ursprungsår beror på förutom att det inte är så många år bort, är att "WP.29 Cybersecurity Regulations" blev godkända av UNECE (United Nations Economic Commission for Europe). WP.29 innebär ett ramverk för att hantera cybersäkerhetsrisker inom fordonsdesign och operation (Thales, 2021). Denna reglering kommer att ha en betydande inverkan på cybersäkerhetsmarknaden för fordon (McKinsey & Company, 2020).

De valda primära källorna (IEEE & ACM), är rekommenderade av (Brereton et al., 2007), då databaserna passar in på informationsteknik och mjukvaruutveckling.

Databaser som används

IEEE (Institute of Electrical and Electronics Engineers)
IEEE är en sammanslutning av över 360 000 ingenjörer och vetenskapspersoner från cirka 175 länder. IEEE är en icke-vinstorienterad organisation som bildades 1963. IEEE är känd för att utveckla standarder för teknik och elektronik, samt ha en pålitlig databas med vetenskapliga artiklar.

ACM (Association for Computing Machinery)
ACM är en av världens största akademiska databaser gällande utbildning och vetenskap inom data. Det är en trovärdig sida med kopplingar mellan författare, verk och institutioner.

Extra källor

Utöver de två främsta databaserna använda i undersökningen så dök det upp några udda artiklar som skedde på Google Scholar innan urvalet av databaser. Anledningen

till att dessa källor fortfarande är med i arbetet är för att det har hittats en enstaka artikel som ger nyttig data till arbetet. Källorna placeras som "extrakällor" då arbetet inte krävde mer från databasen eller att det helt enkelt inte fanns nog med relevanta artiklar. Det har alltså skett ett val att fortfarande ha med dessa "udda" artiklar för att stärka arbetet.

JAREE (Journal on Advanced Research in Electrical Engineering)
På JAREE hittar man forskningsartiklar med ämnen som till exempel kraft- och energisystem, telekommunikation och signalbehandling, elektronik, teknik, styrsystemsteknik, informationsteknik etc. Journalen består av personer och institutioner som är relaterade till utbildning och forskning i Indonesien. Denna källan används då institutionen kan ge oss en bra bild för hur utmaningarna, samt eventuella lösningar ser ut inom cybersäkerhet inom uppkopplade fordon.

MDPI (Association for Computing Machinery)
MDPI är utgivare av kostnadsfria vetenskapliga tidskrifter med över 390 granskare.

3.4 Sökblock

Det är viktigt att tänka igenom söktermerna för att få ett framgångsrikt och giltigt resultat. Sökresultaten ger omfattningen och träffsäkerheten på en systematisk litteraturstudie. Det är viktigt att endast använda relevanta söktermer så inte sökningsfasen tappar fokus på fel områden. Det är alltså viktigt att vara medveten om relevanta nyckelord i forskningsfrågan. Synonymer av de främsta termerna är också värda att undersöka för att öka chansen till relevanta sökträffar (Jesson et al., 2011).

Sökningsfasen använder sig av totalt 9 stycken sökblock. Som skrivet innan är fraserna framtagna genom att testsöka efter relevanta resultat och se vilka nyckelord som passar bäst för att få fram de mest användbara artiklarna. Blocken är presenterade nedanför i två rader. De gröna texten är orden i början av båda blocken tillsammans med ett av det blåa fraserna. Det resulterar i totalt 9 olika sökblock.

Det är även viktigt att sålla ut träffar som hittas med irrelevant fakta trots de relevanta nyckelorden som finns i texten. Det är lätt att datainsamlingen blir överväldigande med alla sökresultat (Wohlin et al., 2012)

- Connected Cars + cybersecurity / vulnerabilities
- Connected Vehicles + cybersecurity / vulnerabilities / IoT / integrity / privacy / threats / data

3.5 Kriterier för artiklar

För att inte helt brett och öppet samla in artiklar med varierande relation till frågan är det viktigt att ha fördefinierade kriterier för vilka artiklar som ska inkluderas och exkluderas. Det underlättar arbetet då det snabbt sorterar ut irrelevanta artiklar som annars skulle göra allting mer brett och rörigt. Det är lätt att i datainsamlingen tappa bort den röda tråden i vad som ska undersökas, då är kriterierna en bra mall att följa Det är alltså viktigt att formulera kraven för inkluderingskriterierna innan själva undersäkningen börjar (Wohlin et al., 2012).

Inkludera	Exkludera
Publicerad tidigast år 2020	Möter inte inkluderingskriterier
Kvalitetskontroll i form av “Peer Reviews”	Artikeln kostar pengar utanför högskolans biblioteksportal
Skriven på antingen Svenska eller Engelska	Spekulativ data som inte har någon bevisad relevans i nutiden
Relaterar och är relevant till arbetets forskningsfråga	

Tabell 2 - Kriterier - Författarens egna

3.6 Sökstrategier

Sökblocken slogs fast med hjälp av att se vilka ord som förekommer i relevanta artiklar till arbetet. I början används breda termer som är kopplade till forskningsfrågan för att se precisionen av orden. Fler användbara termer uppkommer sedan med hjälp av att lösa nyckelord i titlar och abstrakter som uppkommer i de redan funna relevanta artiklarna. Informationen läggs ihop till olika sökblock där orden kombineras på olika sätt för att bygga upp en taktik för sökningen. Med användning av de sökblock som bestämts utfördes även ytterligare metoder för att få fram relevanta artiklar (Universitetsbiblioteket, 2023).

En av metoderna som används under sökningsfasen var “Backwards Snowballing”, vilket innebär att man går bakåt i tiden och tittar på referenslistor i de artiklar man redan har hittat för att hitta fler relevanta artiklar. På så sätt hittas ytterligare artiklar som inte dyker upp i databassökningarna (Jalali, S., & Wohlin, C., 2012).

3.7 Etik

När det kommer till forskningsetiken under arbetets gång så är en av de viktigaste delarna att respektera tidigare forskning och se till så att informationen kommer till rätt användning. Tidigare forskning ska genom arbetet få nytt liv i form av en rättvis och relevant syn på området. Det gäller att inte plocka fakta ur artiklarnas kontext då innehållet kan skifta i betydelse. En viss noggrannhet ligger alltid i åtanke när information, förslag och teorier tolkas av forskningsförfattare. Trots att arbetet lyser upp delar som är osäkra inom cybersäkerheten, och att det finns chans för till exempel eventuella hackare att dra nytta av arbetet så är möjligheten för positiva resultat mycket mera sannolikt. För att förhindra intrång i cybersäkerheten måste vi alla vara på samma sida när det kommer till den teknologiska utvecklingen. Då är det omöjligt att det inte finns en del få dåliga aktörer. Arbetets etik-tänk är inspirerat av Vetenskapsrådet (Vetenskapsrådet, 2022).

3.8 Validitet

Validitetshot är viktigt att tänka på eftersom det kan påverka arbetets resultat och trovärdighet. Validitet handlar om hur väl en undersökning mäter det den avser att mäta. Om en undersökning inte är valid kan det leda till felaktiga slutsatser och beslut. Det är därför viktigt att tänka på validitetshot och försöka minimera dem så mycket som möjligt (tankeredskap.se, n.d.).

Det finns två tillfällen då validiteten är extra viktig. Först när utformningen av undersökningen sker med alla olika moment som förekommer i utredningsprocessen. Sen bedömningen av arbetets egen utredning. Det gäller att konstruera trovärdighet genom att förmedla det som forskarna och författarna vill. En annan viktig sak att ha i åtanke är hur väl arbetet överensstämmer med verkligheten utanför litteratur och tolkningar. Det ska finnas en klar koppling mellan arbetets metod och hur den leder till ett rimligt svar på forskningsfrågan (Metoddoktorn, 2023). Validiteten måste genomsyra hela arbetet, inte bara analysfasen. Validiteten visar hur resultatet av arbetet är sant och korrekt, och därmed inte partiska av författarens subjektiva åsikter (Wohlin et al., 2012). För att hålla arbetet opartiskt och transparent redovisas varje steg i sina olika processer. Målet är att få en så träffsäker kartläggning som möjligt genom att låta den noggrant utvalda informationen av akademiska källor presentera resultatet. Genom att få synvinklar från flera betrodda källor och förmedla vad författarna menar utan förutsatta tankeställningar blir arbetet trovärdigt.

3.9 Analys

Delfrågorna besvaras i en analys som utgår från tematisk deduktiv kodning. Baserat på material som samlats in från inluderingskriterier katigoriseras datan till olika teman som baseras på delfrågorna. Genererande av teman utgår från intuition av vad de utplockade kodningarna pekar på. Det bygger på vad för intressanta mönster det finns i relation till forskningsfrågan. Efter det första skedet av kodning har skett och det finns en överblick på alla koder skapas relevanta teman i form av olika “högar” av sorteringen av koder. De största högarna blir då arbetets teman som i sin tur kommer svara på delfrågorna.

Delfrågor:

- Vart finns sårbarhetsytorna i uppkoplade bilars infrastruktur? - För att bygga upp kartläggningen så är detta grunden för arbetet, vilka komponenter, teknologier och områden i bilens infrastruktur är sårbara.
- Vad finns det för eventuella skyddsmetoder till sårbarheterna? - För att utveckla kartläggningen är det nyttigt att få insikt på vilka eventuella lösningar det finns för sårbarhetsutmaningarna, och vart fokuset borde ligga i framtiden.

Analysen kommer ske genom att använda Tematisk deduktiv kodning vilket är en metod där man använder befintliga utgångspunkter eller teorier för att identifiera och analysera teman i den insamlade datan. Detta gör det möjligt att lyfta datans analytiska nivå samtidigt som den sammanfattas på ett effektivt sätt (Frågor och Svar, 2022). Kodningsmetoden börjar med att plocka ut relevant text och kategorisera texten i olika “högar” som relaterar till forskningsfrågan. Datan från de olika kodningarna extraheras sen och bildar teman som svarar på forskningsfrågan (Braun & Clarke, 2006).

Vid varje tema kommer den insamlade datan redovisas på ett sätt som förklarar relevanta områden och på så sätt redovisar temat. Vid varje tema har sökningsprocessen genomförts. Frågeställningen om vad som ska vara med i arbetet går ut på att fråga om vad som är relevant och hjälper till att svara på frågorna. Det kommer ske en steg-för-steg metod då varje tema har sina små rubriker med tillhörande information som bygger upp faktan om temat. Analysen inleds med en sammanfattning av vad som är det tydligaste och mest uppenbara svaret på varje delfråga med den information som är tillgänglig från varje tema. Samma sak sker sen på lite större skala då hela arbetet summeras, för att sedan jämföras och kombineras i en kartläggning som är i form av den ursprungliga forskningsfrågan.

4 Resultat (och analys)

Träffar i databasen

IEEE
connected vehicles cybersecurity **143**
connected cars cybersecurity **21**
connected vehicles vulnerabilities **133**
connected cars vulnerabilities **30**

connected vehicles IoT **611**
connected vehicles integrity **87**
connected vehicles privacy **358**
connected vehicles threats **242**
connected vehicles data **3635**

ACM
connected vehicles cybersecurity **78,564**
connected cars cybersecurity **77,833**
connected vehicles vulnerabilities **82,014**
connected cars vulnerabilities **81,315**

connected vehicles IoT **79,660**
connected vehicles integrity **80,152**
connected vehicles privacy **85,353**
connected vehicles threats **82,775**
connected vehicles data **122,728**

Databas	Totala träffar	Valda för abstract-läsning	Valda för hel-läsning	Använda till teman
IEEE	5 260	42	32	27
ACM	770 394	10	6	3
JAREE	-	1	1	1

MDPI	-	1	1	1

Tabell 3 - Databasurval - Författarens egna

Sökningsfasen gjordes med en okonventionell metod där endast de första 10 sidorna i varje sökblock granskades och därefter valdes med efter relevans. Anledningen till detta är att efter cirka 10 sidor börjar resultaten visa mer och mer av irrelevanta artiklar som bara snuddar vid ämnet. En mer sofistikerad sökningsmetod skulle dock vara bra att ha i åtanke i framtida arbeten för att hitta ännu mer information kring området. Sökninngsmetoden skulle kunnas ses som ett hot mot validiteten av arbetet då varje artikelträff är inte granskat. Det gjordes ett beslut att de källor som dök upp under proccessen är nog för arbetet då arbetet fick mer än nog med information för att besvara forskningsfrågorna, då flera olika källor pekar på samma sak i arbetets inom arbetets område. Det är dock ett steg som framtida arbete borde definitivt ha i åtanke.

Teman

Under arbetets gång kom det fram fler och fler liknande påståenden om återkommande områden. Många artiklar kunde beröra både sårbarheter men även lösningsförslag så vissa källor kommer upp i svaren till båda delfrågorna. Detta blev första steget i kodningsprocessen då styckena delades upp i grupper relaterade till ett specifikt sårbarhetsområde. Till exempel kunde dessa kodningar vara: “ECU”, “LIDAR” och “OTA”. För att inte överbelasta arbetet med för många teman togs beslutet att ha ett samlat tema för första delen av forskningsfrågan, vilket resulterade i “Sårbarhetsområden”, eller som det presenteras i analysen “Främsta sårbarhetsytorna är ingångarna till mängden personlig fordonsdata” vilket beskriver områdena. När det gäller den andra delfrågan om relevanta skydd fanns det en stor gemensam nämnare i form av “kryptering och blockchains” som fick bli arbetets andra tema vilket presenteras i texten som “Kryptering i blockchains, främsta skyddet för dataintrång”. Anledningen till att ett tredje tema finns är att förutom blockchains fanns det många andra övriga förslag på skydd som inte riktigt berörde det återkommande ämnet om kryptering. Därför heter det temat “Övriga skydd”, eller “Forma framtidens cybersäkerhet i fordon med ramverk, standarder och redundans” som det presenteras i texten. Det är mer inriktat på breda lösningar i form av standarder och ramverk istället för mer specifika tekniska lösningar som uppkommer i föregående tema.

Kodningsprocessen av datan för att besvara på den första delfrågan “Vart finns sårbarhetsytorna i uppkopplade bilars infrastruktur?”

Det uppkom en bra hög med olika komponenter och områden som visade sig vara sårbarheter och mål av angripare. Kodningen av sårbarheterna började i form av olika högar med områdena. Första tanken var att ha de områden som relaterade mest till vart annat i olika teman, till exempel: ECU/CAN BUS, V2V/V2I/V2X, WiFi/Bluetooth/5g, USB/OBD etc. Det blev till slut dock avsevärt rörigt att ha så många teman, speciellt när områdena kan passa in på flera kodningar. Dessutom är tanken med arbetet att inte rikta in sig för mycket på en specifik del och faktiskt göra en kartläggning i ett så sammankopplat system. Till slut så valdes det första temat att vara en bred samling av sårbarhetsytorna i fordons uppkopplade systenm. - Sårbarhetsområden.

Kodningsprocessen till den andra delfrågan "Vad finns det för eventuella skyddsmetoder till sårbarheterna?"

Likt det första temat så uppkom det många olika typer av relevanta områden. Dock så var det oftast en röd tråd genom alla utvalda artiklar, kryptering och blockchains. Det blev naturligt att ha ett gemensamt tema då kryptering och blockchains är ofta väldigt ihopknutna i hur de funkar. Det blev naturligt att ha ett eget tema dedikerat till de området.

Till sist fanns det artiklar som tog upp förslag som inte alls passande in på kryptering och blockchains, vilket då gjorde att dessa artiklar hamnade i en separat hög jämte det andra temat. Det fick till sist bli det tredje temat med lite övriga tankar och förslag kring skydden som inte riktigt hörde hemma i ett detaljerat tema, men som ändå hade lite gemensam röd tråd i form av redundans, regleringar mm.

Temaindelning

Antal relevanta stycken	**Passande tema**
37	Sårbarhetsområden
11	Kryptering & Blockchains
13	Övriga skydd

Tabell 4 - Temaindelning- Författarens egna

De tre slutgiltiga teman som ska presentera resultatet gavs till slut mer övergripande och passande namn för att tydligare förklara innehållet.

- Främsta sårbarhetsytorna är ingångarna till mängden personlig fordonsdata
- Kryptering i blockchains, främsta skyddet för dataintrång
- Forma framtidens cybersäkerhet i fordon med ramverk, standarder och redundans

I tabellen nedanför redovisas vilka artiklar som bidrar till varje tema. Notera att en artikel kan uppkomma flera gånger under samma tema, och även i flera olika teman. Det är viktigt att ha i åtanke att det existerar samspel mellan områdena, där av kan samma artikel ge insikt i flera områden.

Främsta sårbarhetsytorna är ingångarna till mängden personlig fordonsdata.	• (Kumar, S., et al., 2021). • (Bajpa, P., et al., 2020). • (Changalvala, R., & Malik, H., 2020). • (Yadav, N., et al., 2022). • (Masood et al., 2023). • (Malik, S. & Sun, W., 2020). • (Rashed, F., et al., 2020). • (Wang, Y., et al., 2023). • (Cali, U., et al., 2023).

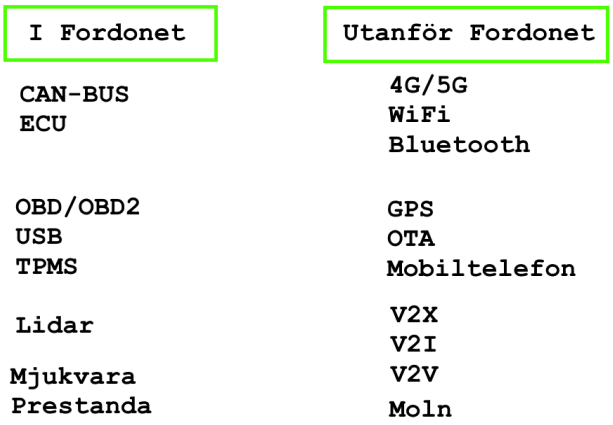
	• (Salek M., et al., 2022). • (Rasheed, R., et al., 2023). • (Huang, J., et al., 2021). • (Masood, A. et al., 2020). • (Cui, Y. et al., 2021). • (Kexun, H., et al., 2020). • (Wu, Z., et al., 2021) • (Reyes, G., et al., 2023).
Kryptering i blockchains, främsta skyddet för dataintrång.	• (Yadav, N., et al., 2022). • (Noh, J., et al., 2020). • (Li, W. et al., 2020). • (Na, D. & Park, S., 2021). • (Salek M., et al., 2022). • (Wang, Y., et al., 2023). • (Cali, U., et al., 2023). • (Salek M., et al., 2022). • (Tyagi, A & Goyal, D. 2020).
Forma framtidens cybersäkerhet i fordon med ramverk, standarder och redundans.	• (Masood, A. et al., 2020). • (Kumar, S., et al., 2021). • (Rashed, F., et al., 2020). • (Changalvala, r., & Malik, H., 2020). • (Wu, Z., et al., 2021). • (Cui, Y. et al., 2021). • (Reyes, G., et al., 2023). • (Huang, J., et al., 2021). • (Sasank, V., et al., 2022).

Tabell 5 - Artiklar kopplade till teman - Författarens egna

4.1 Främsta sårbarhetsytorna är ingångarna till mängden personlig fordonsdata.

Den mest värdefulla variabeln för hackare är förarens personliga information. Som vilket nätverk som helst mellan olika parter så kommuniceras det konstant stora mängder med precis information. De punkterna som kan vara sårbara för attacker kan utnyttjas via både fysiska medium och kommunikationsmetoder med omvärlden.

De olika komponenterna och kommunikationsteknologierna är ofta väldigt involverade och beroende av varandra. Det kan göra det svårt ibland att kategorisera exakt vart i ett område en sårbarhet hör in. I figur 3 är de olika sårbarhetsområdena uppdelade i två led beroende på om sårbarheten är lokalt i fordonet eller i en extern uppkoppling till omvärlden.



Figur 3 - Sårbarhetsområden två led - Författarens egna

CAN/ECU

CAN-Bussen tillsammans med alla ECU-enheter är själva ryggraden i fordonets interna system. Detta system är sårbart för alla möjliga typer av attacker och ingångar för angripare.

Fordonets många sensorer är sammankopplade via CAN-bussen för att alla ECU enheter ska kunna agera baserat på värdena. Angripare kan koppla in en slutenhet till den anslutna plattformen för att få tillgång till CAN-bussen, vilket skulle göra det möjligt för dem att få tillgång till fordonets interna system för att injicera falska sensorvärden och tvinga fordonet att vidta oönskade åtgärder. Inkräktare kan få tillgång till denna CAN-bussen via:

- Trådbundet medium som OBD-portens USB-port.
- Trådlöst via till exempel Global System for Mobile Communications (GSM) eller över Wi-Fi.
- Genom API:er som Short Message Service (SMS), webbgränssnitts-API:er och mobila API:er.

När inkräktaren får tillgång till dessa kanaler kan de göra riktade attacker över anslutna enheter som motorsystem, drivlina, transmissionssystem, säkerhetssystem och bromssystem (Kumar, S., et al., 2021).

Den interna arkitekturen i bilar var inte designad för säkerhet. Till exempel tillhandahåller vanligtvis inte CAN-bussen grundläggande säkerhetsfunktioner som autentisering eller kryptering av data. Dessutom saknar CAN förmågan att logga eller filtrera kommunikation, vilket gör intrångsdetektering och kriminalteknisk analys utmanande (Bajpa, P., et al., 2020).

Kopplingen mellan ECU-enheter, ställdon och interna sensorer är speciellt sårbara för cyberattacker där angripare tar trådlös kontroll. Sensorsystemen i autonoma fordon är anslutna över flera nätverk, gateways och gränssnitt till databehandlingsenheterna. Överföringen av sensordata är sårbara för olika interna attacker som kan kränka integriteten (Changalvala, R., & Malik, H., 2020).

ECU-datalagring är sårbar för ddos attacker (Yadav, N., et al., 2022).

Baserat på insamlad data från olika ECU:er, som gör beslut åt fordonet. I falska förhållanden, till exempel dålig eller korrupt sensordata, kan ECU starta nödbromsar. Det finns ytterst lite litteratur om åtgärdsstrategier i ett sådant scenario (Masood et al., 2023).

OBD/OBD2/USB
De mer direkta lokala komponenterna på fordonet blir en sårbarhet om angripare kan komma åt portarna fysiskt.

Angripare måste ha direkt tillgång till OBD-porten. Utnyttjning av OBD kan ge angriparen tillgång att skapa driftstörningar, kontroll av fordonet och informationsstöld (Yadav, N., et al., 2022).

Att missbruka detta hjälpmedel och utnyttja alla möjliga sårbarheter kan resultera i allvarliga konsekvenser. Mobilapplikationer kan utnyttjas för att tvinga den hemliga PIN-koden att gå offline och ansluta till dongeln via Bluetooth. Forskare från Argus Research Team hittade ett sätt att hacka sig in i Bosch Drivelog ODB-II-dongeln och injicera alla typer av skadliga paket i CAN-bussen. Detta gjorde det möjligt för dem att stoppa motorn på ett fordon i rörelse genom att ansluta till dongeln via Bluetooth. ODB-II-dongel kan användas för att injicera alla typer av skadliga paket i CAN-bussen (Malik, S. & Sun, W., 2020).

V2X/V2V/V2X
En stor del av sårbarhetsytan finns i kommunikationen mellan fordon och enheter i omgivningen. I ett så uppkopplat nätverk med konstant kommunikation mellan olika fordon och infrastruktur kan det räcka med en ingång för att komma åt flera delar av systemen.

De stora antal sensorer, nätverksanslutningar och trådlös kommunikation i V2V eller V2X ger sårbarheter i form av oavsiktliga bakdörrar som angripare kan utnyttja. Skadliga attacker kan vara spoofing, jamming och avlyssning. Dessa skadliga aktiviteter påverkar uppkopplade bilars säkerhetstjänster som konfidentialitet, autentisering, integritet och tillgänglighet (Rashed, F., et al., 2020).

WiFi/5G/Bluetooth
De trådlösa kommunikationsteknologierna är också en sårbarhetsyta för uppkopplade fordon.

För fjärrattacker kan den skadliga enheten penetrera vilket som helst av de externa kommunikationssystemen i fordonet, till exempel wifi eller mobilnätet (Reyes, G., et al., 2023). Enligt Upstreams säkerhetsrapport var 79,6 % av alla cyberattacker som upptäcktes 2020 fjärrattacker (Wang, Y., et al., 2023).

Ytan som är sårbar för attacker gällande trådlös kommunikation i uppkopplade fordon har sårbarheter som anslutningen till smartphones, andra fordon eller laddstationer. Det kan ske till exempel över Bluetooth eller Wi-Fi. Det finns även sårbarheter i

kommunikationen mellan fordon och infrastruktur, eller till molnet över till exempel LTE (Cali, U., et al., 2023).

5G har sina egna sårbarheter, av vilka några har ärvts från 4G. Till exempel hot från cellsitesimulatorer ävem kallade "Stingrays". Några är unika problem som massnätverksfel på grund av delad infrastruktur. Varje fel i det underliggande nätverket mellan fordonet och molnet kan potentiellt äventyra applikationer involverade i molnet. Det krävs mer forskning om cybersäkerheten i 5G (Salek M., et al., 2022).

Navigering, radar, plats & timing

GPS-enheten kan utsättas för manipulation som kan ge förfalskade destinationskoordinater. Det kan leda till att fordonet avviker från den ursprungliga färdvägen.
Angripare kan påverka systemet med hjälp av en bakdörr vid till exempel en bristande mjukvaruuppdatering. Det kan leda till manipulering av bilens instrumentkamera och få bilder i realtid på till exempel vart den är parkerad. LIDAR system kan också läcka högupplöst inblick i omgivningen (Kumar, S., et al., 2021).

På grund av långdistansöverföringen tar användarsegmentet i GPS emot signaler med mycket låg effekt, vilket är den största sårbarheten i det globala satellitnavigeringssystemet. Eftersom GPS sänder en högfrekvent bärvåg är en annan viktig fråga därför siktlinjen. De flesta av hoten på GPS-mottagaren är förknippade med dessa två problem, siktlinje och lågeffektsignal. Dessa två sårbarheter spelar en avgörande roll vid jamming och spoofing attacker (Rasheed, R., et al., 2023).

Radar är avkänningsenheten som sänder den elektromagnetiska radiosignalen och tar emot ekot från objekt för att bestämma position och hastighet. Sårbarheter och utmaningar förknippade med radar är relaterade till utmaningar av elektromagnetiska radiovågor och objektets fysiska utseende i ett detekteringsutrymme. Det finns sårbarheter i cyberfysiska system som kan leda till potentiella faror och risker (Rasheed, R., et al., 2023).

LTE-positioneringssystem är en platsbaserad tjänst som använder LTE-nätverket för att fastställa platsen för en enhet. Liksom alla andra positioneringssystem har även LTE-positioneringssystemet vissa sårbarheter på grund av radiovågorna som kan störas på olika sätt av till exempel en angripare. Det kan ske avlyssning, jamming, spoofing etc (Rasheed, R., et al., 2023).

Interna navigeringsenheter är mycket känsliga och deras resultat kan påverkas av interna elektromagnetiska störningar och omgivande temperatur (Rasheed, R., et al., 2023).

Posittionering med hjälp av LIDAR har även vissa sårbarheter som liknar radars sårbarheter då arbetsprincipen för radar är identisk med lidar. Några av lidars sårbarheter är ogynnsamma väderförhållanden, siktlinje, begränsad räckvidd, spoofing och störningar (Rasheed, R., et al., 2023).

Molnet
Ett integritetsbevarande schema för platsbaserade tjänster är att önska med uppkopplade fordon. Konceptet med konventionella ad hoc-nätverk omvandlas gradvis till ett nätverk av fordon. Samtidigt skapas allt fler platsbaserade tjänster för att ge förare bekvämlighet. Men den frekvent uppdaterade platsinformationen som skickas till platstjänst-servern sätter också användarens integritet på spel (Huang, J., et al., 2021).

Molntjänster för fordon tillåter fordon att skapa anslutningar baserat på V2V- eller V2I-kommunikation.På grund av fordonens anslutning via ett delat trådlöst medium, kan en angripare hota säkerheten och integriteten för de meddelanden som vidarebefordras genom det. En angripare kan placera ut sin avlyssningsstation längs det område den vill övervaka och avlyssna den trådlösa kommunikationskanalen för att samla in privat information om fordonet. Dessutom kan angripare gissa identiteten på ett eller flera legitima fordon och använda dessa identiteter för att injicera skadliga meddelanden i nätverket på beteendet hos legitima fordon. Angriparna kan också förneka sin inblandning i att injicera de påstådda meddelandena (Masood, A. et al., 2020).

Med utvecklingen av uppkopplade fordon blir “Cloud Control Platform” en viktig del för att beräkna körstrategier. När strategierna läggs ut på molnet måste dock viss privat data från fordonstillverkare skickas till molnet, vilket blir en sårbarhet i sig. Till exempel “Engine Map”, som är kärndata för fordonstillverkare. Hur man skyddar denna data har varit ett av det största hindrena för uppkopplade fordon (Cui, Y. et al., 2021).

Molnet utför en viktig roll för snabb beslutstattning, beräkning och hantering av en enorm mängd data. Det är ett arkiv med användardata. Det är också en tillgångscentral för kommunikation till en pool av andra anslutna fordon. Om ett fordons cybersäkerhet kan bli kompromissat kan det öppna porten till denna molninfrastruktur. Cyberattacker över molntjänster har potential att rikta in sig på en massa samtidigt. Läckage av användardata kan vara ett allvarligt integritetsproblem (Kumar, S., et al., 2021).

För molnstödda applikationer till uppkopplade bilar är cybersäkerheten extremt viktig. Säkerhetsfel kan störa det molnsanpassande transportsystemet för ett helt område genom att exponera känslig information, öka trafikanternas sårbarheter och till och med orsaka dödsolyckor. Dessa effekter kan förstärkas då varje intrång i cybersäkerheten som sker i moln-applikationer kan påverka andra IoT-applikationer och vice versa på grund av liknande resursdelning i en IoT-miljö (Salek M., et al., 2022).

OTA/Mjukvara
Mjukvaran i ett system, precis som i vanliga datorer, har stor funktion i cybersäkerheten. Ibland kan det dock även vara en sårbarhetsyta, speciellt om överföringen av uppdateringar blir äventyrad.

När tillverkaren väl hittar säkerhetshot släpper de uppdateringar med hjälp av OTA. De har lika många förmåner som säkerhetsproblem. Till att källan till uppdateringarna har verifierats representerar de också hot och risker (Kumar, S., et al., 2021).

Under OTA-uppgraderingsprocessen är överföringsrisker och manipulationsrisker för uppgraderingspaket de främsta cybersäkerhetshoten som OTA-systemets sårbarheter står inför. Det finns cybersäkerhetsrisker från tjänsteplattformen till meddelandet, dataöverföringskanalen till fordonet. Först och främst har det kryphål i systemet på tjänsteplattformssidan, utvecklingsporten och de olika subplattformssystemen och databaserna. Kryphålen kan bli ingången till hackare. Under dataöverföringsprocessen kan meddelanden som serviceplattformen och fordonet interagerar med kapas och förfalskas. I överföringsprocessen för att ladda ner uppgraderingspaketet på fordonssidan kan angriparen använda nmetoder för att skicka det förfalskade uppgraderingspaketet till fordonssidan (Kexun, H., et al., 2020).

Vissa OTA-uppdateringar avsedda att undvika kritiska bilsystem har gjort mer skada än nytta. En OTA-uppdatering som skickades ut till 2017 och 2018 Jeep och Dodge Durango-modeller visade sig för vissa att innehålla en bugg för systemet. Instrumentbrädan hamnade i en ond cirkel av oändliga omstarter, vilket effektivt inaktiverade underhållningssystemet och vissa nödtjänster (Malik, S. & Sun, W., 2020).

OTA-uppgraderingar är avgörande för cybersäkerheten. Med den ständiga förbättringen av attacktekniken måste tillverkare kontinuerligt optimera och förbättra säkerheten för OTA. OTA-funktionen ett mycket attraktivt mål för hackare. Kapning, manipulering och andra metoder används för att attackera OTA-uppgraderingslänken för fordon (Wu, Z., et al., 2021)

Zero-Day sårbarheter är kritiska brister i ett program eller ett OS som är okänt av tillverkarna då programvaran är nysläppt. Det kan resultera i förödande attacker tills sårbarheten är fixad. Hackare kan utnyttja en "noll dagars sårbarhet" för att negativt påverka uppkopplade bilprogram, data, ytterligare smarta bilar eller ett nätverk av uppkopplade fordon, för att leverera skadlig programvara (Malik, S. & Sun, W., 2020).

Det senaste inom mjukvaruutveckling kan i stort sett ännu inte uppfylla strikta säkerhetsstandarder för all programvara. Även om mjukvarusäkerheten i bilsystem förbättras på grund av pågående ansträngningar inom säkerheten, finns det fortfarande sårbarheter och kommer att fortsätta att existera. Det är viktigt att ha i åtanke att även om säkerhetsstandarder finns på plats, finns sårbarheter fortfarande (Bajpa, P., et al., 2020).

Det finns en del medvetna buggar hittade av hackare i den inbyggda programvaran för elbilar vilket oftast är på grund av osäkra mjukvaruuppdateringar. Svaga tilldelade lösenord som ska skydda systemen är en av sårbarheterna. Osäker, ineffektiv datadelning av resurser mellan fordonet och internet är en annan. Överflöd av data i en buffert som skadliga enheter kan identifiera för att attackera CAN-bussen (Reyes, G., et al., 2023).

Övriga Sårbarheter
Det finns andra sårbara ytor som lätt kan gå under radarn när man tänker sig cybersäkerheten i bilar. Till exempel mobiltelefoner som är kopplade till bilsystemet, trådlösa bilnycklar, laddstationer för elbilar, däcktrycksövervakningssystem och till och med bilens datorprestanda.

Mobiltelefon
Appar i mobilen blir en sårbarhet då hackare kan få tillgång till bilsystemet, till exempel radion. Det kan leda till att hackare spelar upp skadliga multimediafiler som modifierar systemets kod. Det finns möjlighet att missbruka systemet och potentiellt spionera på uppkopplade bilkomponenter (Yadav, N., et al., 2022).

Mobiltelefoner kan injiceras med skadlig programvara som gör att en hackare får tillgång till privat information som lösenord och inställningskontroller. Tekniska experter förklarar att användning av mobiltelefoner i bilar kan vara ett recept på katastrof eftersom det aldrig utformades för att skydda säkerhetskritiska system. Moderna fordon använder Wi-Fi och Bluetooth för att dra fördel av fjärrfunktioner. Bilsystemen använder trådlösa funktioner för att överföra filer, acceptera fjärrkommandon och skicka systemstatusmeddelanden som till exempel motorstatus. Mobilapplikationer kan också använda de trådlösa faciliteterna för att interagera med bilsystemen. En angripare kan utnyttja kända säkerhetsluckor i trådlösa medier. Utnyttjande av sårbarheter på Wi-Fi eller Bluetooth kan leda till att en angripare kommer åt systemet med administrativa rättigheter. Angripare kan också utföra attacker på Wi-Fi-lösenord. På liknande sätt kan förarkomponenterna i Bluetooth eller Wi-Fi också utgöra utnyttjandemöjligheter för hackare, få tillgång till att utföra fjärrkommandon på systemet och gå så långt som att stoppa bilmotorn mitt på motorvägen eller en korsning eller en blind kurva. Denna mobilappattack kan också användas för att kontrollera grundläggande funktioner i bilarna (Malik, S. & Sun, W., 2020).

Bilnyckel
Den trådlösa nyckelinmatningsfunktionen används för att hålla reda på hur du slår på eller av bilen på distans. Det hjälper ägaren att låsa bilen från en avlägsen plats, istället för att manuellt låsa bildörrarna. Forskare har testat det trådlösa nyckelsystemet och kommit fram till att bilen ger kontroll genom att bygga en proxybrygga mellan nyckeln och bilsystemet. En trådlös förstärkare kan utnyttja det trådlösa nyckelsystemet genom att skapa en proxybrygga mellan nyckeln och bilen som använder en signal för att låsa upp bildörrarna automatiskt (Malik, S. & Sun, W., 2020).

Man kan komma in i fordonet med hjälp av nyckelbrickan eller nyckelfritt. När föraren försöker låsa sin bil kan angripare försöka förhindra det genom att använda en mängd olika tekniker. Till exempel garagedörröppnare, hemljuskontroller eller dimmers. Sändningarna från nyckelbrickan kommer att blockeras i områden som parkeringsplatser eller gator när dessa enheter är undangömda i buskar och slås på under längre perioder. Signaleringen för en bil med fjärrstart kan även blockeras. Det är möjligt att spela in och kopiera denna konstanta signal för att få tillträde till en bil. Dessutom är det möjligt att stänga av larmet och startspärren så att kriminella kan starta och sno bilar. Det har till exempel hävdats att angripare kan skapa en billig,

kompakt elektronisk pryl som kan döljas på eller bredvid en säker bil. En nyckelfri kod kan spelas in av den här enheten och användas för att öppna bilen vid ett senare tillfälle. Den sänder en störningssignal för att förhindra att bilen tar emot kodsignaler från ägarens nyckelbricka samtidigt som den fångar upp signalerna från båda upplåsningsförsöken. Dessutom är vissa startspärrar och larm beroende av relativt tunna hemliga nycklar. De går lätt sönder med en bärbar dator på några minuter (Yadav, N., et al., 2022).

Laddstationer
Att ladda en elbil med en allmän laddstation är något av de mest sårbara scenarierna. Detta beror på att medan batteriet laddas, upprättas ett kommunikationsprotokoll där ett informationsutbyte mellan batteri-hanteringssystemet och laddstationen äger rum. Hackare kan utnyttja dessa kommunikations och beräkningskomponenter för att äventyra tillgängligheten, integriteten och konfidentialiteten hos ett nätverk av laddningsstationer eller till och med elnätet (Reyes, G., et al., 2023).

När det gäller att rikta in sig för en elbil så är lokala attacker den mest direkta metoden på grunda av de fysiska anslutningspunkterna som radiofrekvenssensorer, CAN-porten och laddningsstationer (Reyes, G., et al., 2023).

Prestanda
Den begränsade prestandan i anslutna fordon kan utnyttjas av hackare genom som kan till exempel överflöda systemen med förfrågningar för att neka användaren till resurser (Kumar, S., et al., 2021).

Däcktrycksövervakningssystem
I och med att Däcktrycksövervakningssystem (TPMS) använder väldigt enkla protokoll kan TPMS-kommunikation göras omvänd eftersom den inte är beroende av krypteringsteknik. Dessutom kan TPMS-problem uppstå på grund av strömslöseri och spoofing. Detta innebär att angriparen kan lyssna på eller förfalska kommunikation som kommer från en närliggande bil (Yadav, N., et al., 2022).

4.2 Kryptering i blockchains, främsta skyddet för dataintrång.

En gemensam nämnare bland de flesta förslag på säkerhetssystem i dagens uppkopplade bilar är kryptering i blockchains. För att uppkopplade fordon snabbt ska kunna kommunicera med mängder av precis information mellan vart annat och till molnet krävs det att informationen är säker och solid.

Försvaret mot cyberattacker på fordons sårbarheter kan stärkas med hjälp av blockchain-teknik. Tekniken ger funktioner till viktig information som gör den: oföränderlig, transparent, säker, enhällig och decentraliserad. Blockchain kan användas för att erbjuda realtidsinformation och genomföra transaktioner mellan olika parter som är involverade i bilsektorn, inklusive producenter, köpare, fordonsfinansieringsföretag, tjänsteleverantörer och försäkringar. Lagrad data samlas in från olika sensorenheter eller fordon till fordon, och kommunikation mellan fordon och infrastruktur på blockkedjan i form av block som använder konsensusprotokoll. Konsensusprotokoll är en mekanism som genom noderna i nätverket når en gemensam

överenskommelse. De bildade blocken används för att fatta beslut i realtid för olika tillämpningar av fordonsnätverk. Olika användningsfall av Blockchain i fordonsnätverket är förtroendehantering och meddelandenätverk i VANETs, meddelandehantering och ECU-datalagring (Yadav, N., et al., 2022).

En blockchain-baserad autentiseringsmetod för uppkopplade fordon är ofta del av lösningsförslaget. De flesta konventionella metoder använder en centraliserad arkitektur och tar inte hänsyn till attacker från insidan. Några studier har antagit blockchain-teknik för fordon. Det flesta av dem har dock inte tagit hänsyn till rörlighetsproblemet i fordonnätverk. I en föreslagen metod antas blockchain-teknik för att säkerställa integritet och effektiv autentisering. Från blockchain-arkitekturen kan man skapa ett decentraliserat nätverk och fordonen kan autentisera meddelanden genom att använda information på ett distribuerat sätt utan stöd från RTA (RTA står för "Registrar Transfer Agent" och är en plattform som används för att överföra tillgångar på sekundärmarknaden). Genom formell verifiering och implementation visar det att den föreslagna metoden kan uppnå flera säkerhetsmål och diskuterar överhuvudtaget om overhead som orsakas av procedurerna för blockchain. Det finns flera utmanande frågor i blockchain-baserade fordonsnätverk (Noh, J., et al., 2020).

Ett förslag på säker trafikhanteringssystem är ett decentraliserat och platsmedvetet system för att skydda integritet med flera blockchain-baserade uppkopplade fordonsnätverk. Systemet inkluderar "Zero-Knowledge Range Proof" (ZKRP) i en gateway-mekanism för att verifiera uppkopplade fordon som passerar mellan angränsande blockchain-nätverk utan att avslöja någon känslig information. Blockchain-nätverket mäter benchmarking inklusive transaktionslatens, genomströmning och framgångsgrad. För ZKRP-schemat mäter författarna tidsåtgången för bevisgenerering och verifiering under olika inställningar. Resultaten visar att det föreslagna systemet är effektivt och genomförbart för decentraliserad trafikhantering (Li, W. et al., 2020).

En "lightweight blockchain" föreslås för att lösa förfalskning och ändring av en black-box imagedata och integritet. Efter att ha laddat upp en video till IPFS (InterPlanetary File System) reduceras videostorleken till 46 byte, vilket är IPFS-hash-storleken, och sparas i blockkedjan. Detta bekräftar att fördröjningstiden för uppladdning och nedladdning inte nämnvärt påverkar prestandan, och ökningen av fördröjningstiden enligt kapaciteten är också linjär. En ny konsensusalgoritm reducerar även nätverkstrafiken för att minska latensen. IPFS-hashvärdet lagras i blockkedjan med användarens publika nyckel. Endast användare med en privat nyckel kommer åt videodatan, vilket säkerställer integriteten (Na, D. & Park, S., 2021).

Blockchain-teknologi är en av de utvecklade cybersäkerhetsteknologierna som visar potential för att säkerställa cybersäkerheten för moln-applikationer. Blockchain-tekniken fungerar baserat på identifiering av och förtroende mellan två transaktioner. Blockchain cybersäkerhet är baserad på peer-to-peer (P2P) nätverksgrunder. För att skapa förtroende mellan ett stort antal uppkoplade fordon hjälper blockchain-teknik varje fordon att autentisera inkommande data. Blockchains

kan användas för att lita på de anslutna enheterna och tillåta åtkomst till en molnenhet (Salek M., et al., 2022).

Blockchain är en decentraliserad och säker plattform för informationsdelning, och den kan förbättra säkerheten för V2V-kommunikation. Det kan ge olika fördelar såsom säker autentisering av användare, upptäckt av obehörig åtkomst till fordon, pålitlig informationsdelning mellan fordon för lång och kortdistanskommunikation. Ett förslag är "2-SAP" som kan validera användaren och upptäcka obehöriga användare på ett säkert sätt. Således kan fordon dela information utan att kompromissa med lagrad data i sina enheter.
(Wang, Y., et al., 2023).

Risker för sårbarheter ökar när det gäller elfordon, eftersom de är starkt beroende av kommunikation och uppkoppling, är anslutna till laddstationer och har mer avancerade funktioner som fjärrkontroll och övervakning. För att hantera dessa sårbarheter har flera åtgärder föreslagits. Användningen av kryptering och säkra kommunikationsprotokoll för att skydda data, samt föreskrifter och standarder för att styra insamling och användning av data. Dessutom kan tillverkare och tjänsteleverantörer också erbjuda funktioner som radering av data och att välja bort datadelning för att ge konsumenterna mer kontroll över sin data. För att förhindra att bilen och dess system hackas bör programvaran uppdateras regelbundet, säker nätverkskommunikation och starka autentiseringsmetoder bör användas (Cali, U., et al., 2023).

Vi behöver kryptering, autentisering och auktorisering säkerställer dataöverföring och lagring i V2X. Det skulle även vara bra med mer avancerade säkerhetsprotokoll, inklusive blockchain och AI för att identifiera och förhindra cyberattacker i realtid (Cali, U., et al., 2023).

Det krävs mycket mer forskning kring hur utvecklare skulle kunna utrusta blockchain-teknologin med AI i den molnbaserade miljön (Salek M., et al., 2022).

Genom att förändra den fysiska miljön kring analoga sensorer, som låsningsfria bromssystem, kan vi förebygga livshotande situationer (Yadav, N., et al., 2022).

Försäkringsbolag installerar IoT-appar i bilar för att samla in kundens säkerhetsdata och körinformation och möjliggöra beslut om försäkringsanspråk. För att förhindra att säkerhetsinformation och kördata hamnar i fel händer bör data krypteras på nätverksnivå. Principen för Blockchain används ofta för att slutföra denna uppgift (Tyagi, A & Goyal, D. 2020).

4.3 Forma framtidens cybersäkerhet i fordon med ramverk, standarder och redundans.

För att få en jämn och pålitlig miljö av uppkopplade bilar så krävs det att det finns befintliga prövade och bevisade riktlinjer som tillverkare ska följa. Redundans bör också implementeras så fordon har ytterligare mekanismer som skyddar systemet från sårbara punkter. Det är en bit kvar tills vi har nog med forskning i samtliga säkerhetsområden.

Eftersom befintliga säkerhetslösningar med decentralisering kanske inte är tillräckliga för att möta säkerhets- och integritetsutmaningarna är det nödvändigt att anta kompletterande åtgärder. För närvarande är AI och maskininlärning lovande tekniker för att utveckla säkerhetslösningar för olika dynamiska nätverksmiljöer (Masood, A. et al., 2020).

Inom cybersäkerhet är redundans idén om att koppla kritiska delsystem till mer än ett delsystem och därmed eliminera att systemet kan gå sönder vid en enda punkt (ett så kallat "single point of failure"). Det är ett kostsamt arrangemang med tanke på den extra vikten och kostnaden för de extra delarna. Om ett ramverk beslagtas av en inkräktare kan olika ramverk fortfarande stödja den funktion som det beslagtagna systemet ansvarade för (Kumar, S., et al., 2021).

Att introducera grundläggande analog kontroll i en ständigt framåtskridande digital miljö är ett annat säkerhetsarrangemang. En roll kan till exempel stödjas av tre repetitiva elektroniska styrramverk och ett mekaniskt. Denna icke-hackbara strategi för sista återhämtning börjar presenteras i fordon för säkerhetskritiska ramverk (Kumar, S., et al., 2021).

Inom flygindustrin separeras underhållningsramverket från de resterande systemen för att få en säker arkitektur. Att anpassa det samma i fordons ekosystem kan gynnas genom att skydda och isolera de säkerhetskritiska delsystemen i ett fordon (Kumar, S., et al., 2021).

Det finns många olika förslag på frameworks som ska säkerställa anslutningen mellan förare och fordon (Rashed, F., et al., 2020).

Ett ramverk för att hitta onormala datamönster kan användas för att övervaka data som tas emot över kommunikationskanalen. Detta anomalidetekteringssystem är implementerat för säkerhetskritiska delsystem i ett fordon. Det kommer att kunna förutsäga en enhets onormala aktiviteter och förhindra den från att ytterligare styra andra ECU:er (Kumar, S., et al., 2021).

Ett förslag till skydd för sårbarheter gällande sensorerna finns i form av ett ramverk kallat "Spead Dither 3D QIM" som ska kunna verifiera integriteten för en av de kritiska sensorerna som används i autonom körning (Changalvala, r., & Malik, H., 2020).

Förslag till förbättring av säkerheten kring OTA är ett säkert OTA-uppgraderingsschema genom att analysera olika ECU-hårdvaru och mjukvaruarkitekturer kombinerade med olika algoritmegenskaper (Wu, Z., et al., 2021).

Ett förslag för ramverk till molnet är "Fully Homomorphic Encryption" och Blockchain-teknik kombinerat för att beräkna och spåra krypteringsdata i molnet. I denna ram kan privat data skyddas, omfattningen av dataanvändning kommer att begränsas och samtidigt kommer utförandet av en specifik typ av beräkningar med krypteringsdata i molnet att uppfyllas (Cui, Y. et al., 2021).

Tillverkare och forskare måste samarbeta för att bygga försvar mot cyberattacker och inga bilmodeller är 100 % säkra. Nätverket och enheterna måste säkras från både interna och externa hot. Periodisk kontroll av sårbarheter i olika nivåer av gränssnitt måste analyseras och eventuella risker måste åtgärdas. Mjukvara måste hållas uppdaterad med jämna mellanrum. När systemen uppdateras med patchar från tillverkaren kan det vara en extra fördel att verifiera källan före uppdatering. Isolering av fordonsbuss och säkerhetskritiska system från externt nätverk kan betraktas som en lösning som använder intrångsdetekteringssystem. Att involvera algoritmer för artificiell intelligens för att övervaka nätverket för onormal datatrafik kan resultera i ett bättre attackförsvarssystem (Kumar, S., et al., 2021).

Konfiguration av en laddstation och programuppdateringar måste enkelt tillämpas utan att behöva starta om systemet.
Sensorer och laddningspunkter kan användas för att injicera en attack (Reyes, G., et al., 2023).

Ett nytt platsintegritetsbevarande schema tillåter fordon att skicka exakt realtidsplatsinformation till platstjänst-servern samtidigt som de förhindrar att spåras av angripare. I det föreslagna schemat använder ett fordon platsinformationen från utvalda skuggfordon, vars rutt avviker från begäran, för att generera flera virtuella banor till servern för att vilseleda angripare. Simuleringsresultaten visar att detta föreslagna schema uppnår en hög nivå av integritetsbevarande och överträffar andra moderna scheman när det gäller plats-entropi och spårningsframgångsgrad (Huang, J., et al., 2021).

Säker och privat kommunikation är målet i uppkopplade fordon med VANET. Det första steget för att göra VANET så säkert som möjligt innan implementering och användning är att genomföra säkerhet och integritet på ett sätt som säkerställer tilliten. För att anslutna sammankopplade transportsystem ska kunna fungera inom VANET måste både säkerhetskrav och integritetskrav identifieras och uppfyllas. För att kommunikationsnätverket ska anses vara säkert måste säkerhetsimperativen konfidentialitet, autentisering, icke-förnekande och integritet vara uppfyllda. Ett förslag för säkerhet med VANET är användning av “Elliptic Curve Integrated Encryption Scheme” (ECIES) på grund av dess mindre nyckelstorlek och överlägsen säkerhet. AES-256-GCM är krypteringsalgoritmen som ger bäst balans mellan hastighet och säkerhet, på grund av dess parallellism och inbyggda integritetskontroll som krävs för VANET. Ytterligare forskning och utveckling krävs för att matcha de framsteg i teknik som utan tvekan kommer att komma i den tid då anslutna helt autonoma bilar blir verklighet (Sasank, V., et al., 2022).

5 Diskussion

Det blir ganska uppenbart att det inte finns tillräckligt med forskning kring cybersäkerheten i uppkopplade bilars komponenter, men det finns en bra kartläggning på vart sårbarheterna uppstår. Det är en bra början för att i framtiden kunna skapa nya ramar och standarder för säkerhetsprotokoll etc. Det här arbetets styrka är att redan från början ha ett fågelperspektiv på de professionella arbeten som utförts tidigare och

samla datan till en sammanlagd grund för kartläggningen. Svagheten är att arbetet inte har någon direkt koppling till ämnet via experiment eller individer i branschen. Detta kan leda till mindre precisa förklaringar, samt inte lika djupa diskussioner. Tid är en annan faktor som spelar in till en potentiell svaghet inom arbetet. Att få med all relevant information i sitt fulla esse är helt enkelt inte rimligt under det tidsfönster som arbetet skrivs inom. Arbetet kunde utföras mer fullt om andra delar inom uppkopplade bilar kunde bidra till den fulla bilden och ge andra inputs till ämnet, till exempel mer ingående beskrivningar av hur systemen och skydden fungerar, samt hur attackerna utförs. Det är ingen nyhet att teknikens utveckling springer vidare snabbare än någonsin och uppkopplade bilar är verkligen inget undantag. Trots de säkerhetsstandarder som har satts för uppkopplade bilar 2020 så har själva implementationen en bit kvar. Det finns många bevisade lösningar till olika integrationsproblem, det är bara en tidsfråga att se vilka som blir normen och vilka som försvinner. Olika märken kanske använder olika typer av skydd för sina sårbarheter i systemet. Det råder heller inget tvivel om integriteten när det kommer till förarens privata data. Det är något som absolut är av högsta vikt och måste hanteras på ett så ansvarsfullt och pålitligt sätt som möjligt.

6 Samhällspåverkan

När bilden av hur många sårbara ytor som finns i fordons cybersäkerhet, tillsammans med bakgrunden av alla miljoner cyberattacker som utförs dagligen, finns det etiska tankeställningar som kommer fram. En diskussionsfråga skulle kunna vara om det verkligen är rimligt att fortsätta den teknologiska utvecklingen med huvudet först, speciellt när det kommer till självkörande bilar. Förutom integritetshoten med personlig värdefull information, så handlar det om människors liv. Är det en bra sak att lägga så mycket ansvar på automatiserade och komplexa system som vi vet kan bli (och aktivt blir) kompromissade av angripare, terrorister eller andra makter. Man skulle kunna debattera att självkörande bilar fortfarande minskar trafikolyckor och är för övrigt ett mer säkert sätt att köra fordon, även fast systemen alltid kommer ha brister. Det är en komplicerad fråga som är värd att diskutera.

Som skrivet i introduktionen och bakgrunden finns det oändliga utvecklingsmöjligheter och forskningsområden inom fordons cybersäkerhet att utforska. Det råder inget tvivel på att cybersäkerhetsområdet inom fordon är extremt viktigt för framtiden. Arbetet är nyttigt för att peka ut och lysa ljus på de områden framtidens forskare och utvecklare måste rikta in sig på. Det understryker även hur mycket mer arbetet som krävs för att ha en konsekvent miljö av säkerhet i fordonssystem. Det är viktigt att inte glömma bort de viktiga säkerhetsaspekterna i en konstant rusning av ny teknologi. En hållbar utveckling kräver arbeten som redovisar sårbarheter och sätter dom på kartan för framtiden. Det här arbetet bidrar med att ta ett steg tillbaka och observera hur mycket som fortfarande inte är självklart gällande cybersäkerheten. Arbetet pekar ut listan på områden som behöver mer forskning och fokus så framtiden kan gå i en bättre, säkrare riktning. Arbetet understryker också vad det är som faktiskt fungerar bäst just nu när det kommer till lagring av personlig data, samt kommunikation av data. Kryptering och blockchains är det främsta verktyget vi har i nutid för att säkerställa integriteten och riktigheten i fordonsdatan. Arbetet ger även förslag på eventuella framtida ramverk, metoder och standarder som kan i sig förbättra cybersäkerheten. Arbetet är ett viktigt steg på vägen för att komma närmare målet med säkra uppkopplade bilar.

7 Etiska Aspekter

Att lysa ljus på sårbarheter i cybersäkerheten kan även ha sina negativa konsekvenser. Det finns helt klart chans att arbetet kan bidra till olagliga handlingar som hackarförsök eller dataintrång med hjälp av kartläggningen. Det är något som helt enkelt bör förväntas när informationen är tillgänglig. Det skulle dock kunna argumenteras att en angripare skulle fått tag på informationen förr eller senare ändå, och att det är bättre att vetskapen om sårbarheterna hamnar i allas händer så tillverkare, utvecklare och användare är på samma nivå gällande hur cybersäkerhetsmiljön ser ut. Det väger troligen mer åt en positiv inverkan på samhället att dokumentera sårbarheter så att inte bara det mest insatta är de enda som har tillgång till informationen.

8 Sammanfattning

Detta arbete ställer frågan om vad det finns för sårbara ytor i uppkopplade bilar, och hur man eventuellt kan skydda systemen. Med hjälp av en litteraturstudie och tematisk deduktiv kodning har det skapats en kartläggning av sårbarheter i moderna bilsystem, uppföljt av relevanta lösningsförslag. Arbetet resulterade i tre teman som tillsammans besvarar forskningsfrågan. Cybersäkerhets-sårbarheterna sträcker sig från det fysiska till det trådlösa och har olika typer av potentiella hot, från hackare och angripare till felaktig programvara. Kartläggningen består av flera sårbara nyckelkomponenter som ECU och CAN-bussen som ger tillgång till bland annat fordonets många sensorer. Trådlös kommunikation som WiFi, 5G och bluetooth kan bli kompromissad med till exempel avlyssning och störningar. Kommunikationen fordon förlitar sig på mellan fordonet och omgivningen i V2X, V2V eller V2I är också något som kan bli utnyttjade av angripare. Mängden personlig data i sig kan bli en sårbarhet då den ofta delas med molnet från tillverkaren, mobiltelefonen, företag etc. Sårbarheter i cybersäkerheten kan även uppkomma i oväntade medel som laddstationer för elbilar, eller OBD-porten. I kartläggningen ser vi att det finns många sårbarhetsytor i ett samspel av nätverk i och mellan fordon, andra fordon, infrastruktur m.m. Enligt flera forskningsartiklar visar det sig att det främsta skyddet som ofta kommer upp i lösningsförslag är att kryptera datan med blockchainteknik på olika sätt. Det är för nuläget den mest pålitliga metoden att säkerställa tilliten och integriteten på dataflöden. Förutom implementering av olika versioner av blockchainteknik så finns det flera förslag på grundläggande tillvägagångssätt som standarder och ramverk och att implementera redundans i systemen.

9 Framtida arbeten

I framtiden kan arbetet utvecklas i form av djupare analyser av nutidens och framtidens eventuella cybermijlö. Tekniken går framåt med språngande fart så ett kompletterande arbete som ser vilka vägar som valts inom cybersäkerhets-standarder och protokoll skulle klara upp en klarare bild utan de många förslag som getts under arbetet. Att blanda den befintliga faktan och studierna med inputs från hjärnor inne i branschen skulle vara en bra uppgradering på kartläggningen. Det återstår också mycket forskning och tid för att se hur förslagen ser ut i verkligheten på större skala. Det finns alltid utvecklingsrum inom forskningsfrågan.

Referenser

Ahlberg, J. (2023) Hur fungerar självkörande fordon – och vilka fördelar och utmaningar finns?
https://se.ramboll.com/press/artiklar/hur-fungerar-sjalvkorande-fordon--och-vilka-fordelar-och-utmaningar-finns

Aries, K. (2021) What Is V2V Technology?: V2V vs V2I vs V2X Technology Systems
https://www.verizonconnect.com/resources/article/connected-vehicle-technology-v2v-v2i-v2x/

Aptiv (2020) What Is an Electronic Control Unit?
https://www.aptiv.com/en/insights/article/what-is-an-electronic-control-unit

Almehrezi, F., Yeun, C., Yoo, P., Damiani, E., Hammadi, Y., Yeun, H. (2020) An Emerging Security Framework for Connected Autonomous Vehicles
https://ieeexplore-ieee-org.libraryproxy.his.se/document/9348317

Bajpa, P., Enbody, R. (2020) Towards Effective Identification and Rating of Automotive Vulnerabilities
https://dl-acm-org.libraryproxy.his.se/doi/epdf/10.1145/3375706.3380556

Braun, Virginia, Clarke, Victoria (2006) Using thematic analysis in psychology, Qualitative research in psychology

Brereton, Pearl, Kitchenham, Barbara A., Budgen, David, Turner, Mark, Khalil, Mohamed (2007) Lessons from applying the systematic literature review process within the software engineering domain, Journal of Systems and Software

Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., Das, R. (2020). Attacks on Self-Driving Cars and Their Countermeasures: A Survey
https://ieeexplore.ieee.org/document/9257492

Cichy, P., Salge, T., Kohli, R. (2021) PRIVACY CONCERNS AND DATA SHARING IN THE INTERNET OF
THINGS: MIXED METHODS EVIDENCE FROM CONNECTED CARS
https://eds-s-ebscohost-com.libraryproxy.his.se/eds/pdfviewer/pdfviewer?vid=0&sid=3aab6da7-6fa8-42a3-80f4-95a7f5588efd%40redis

Coindesk (2022) On-Chain vs. Off-Chain Transactions: What's the Difference?
https://www.coindesk.com/learn/on-chain-vs-off-chain-transactions-whats-the-difference/

Cui, Y., Li, S., Wang, Y., Gao, B. (2021) The Data Protection of Intelligent Connected Vehicles Cloud Control Framework Using Fully Homomorphic Encryption https://ieeexplore-ieee-org.libraryproxy.his.se/document/9338620/authors#authors

Cui, Y., Li, S., Wang, Y., Gao, B. (2021) The Data Protection of Intelligent Connected Vehicles Cloud Control Framework Using Fully Homomorphic Encryption https://ieeexplore-ieee-org.libraryproxy.his.se/document/9338620

Chah, B., Lombard, A., Bkakria, A., Yaich, R., Galland, A. (2021) Privacy Threat Analysis for connected and autonomous vehicles https://www-sciencedirect-com.libraryproxy.his.se/science/article/pii/S1877050922015733

Changalvala, R., Malik, H. (2020) Sensor Data Integrity Verification for Autonomous Vehicles Using Spread 3D Dither QIM https://ieeexplore-ieee-org.libraryproxy.his.se/document/9348492

Cali, U., Kuzlu, M., Elma, O., Gucluturk, O., Kilic, A., Catak, A. (2023) Cybersecurity and Digital Privacy Aspects of V2X in the EV Charging Structure https://dl-acm-org.libraryproxy.his.se/doi/fullHtml/10.1145/3590777.3591406

DATA CONOMY (2023) Sharing the benefits with consortium blockchains https://dataconomy.com/2023/01/blockchain-consortium-advantages/

Euceda, G., Akundi, A., Luna, S. (2023) Cybersecurity Challenges in Electric Vehicles: An initial literature review and research agenda https://ieeexplore-ieee-org.libraryproxy.his.se/document/10131069

EDPB https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_sv

Elliott, D., Keen, W., Miao, L. (2019) Recent advances in connected and automated vehicles https://www.sciencedirect.com/science/article/pii/S2095756418302289

EY Germany Switzerland Austria (2020). Cybersecurity for connected vehicles - World Intelligent Connected Vehicles Conference https://www.youtube.com/watch?v=vcOq8l0_Ctw

Ferrovial (2023) What Are Connected Autonomous Vehicles? https://www.ferrovial.com/en/innovation/technologies/connected-autonomous-vehicl

es/

Fragor och svar (2022) Hur gör man en tematisk analys ? https://www.fragorochsvar.com/hur-gor-man-en-tematisk-analys/#Hur_gor_man_en_tematisering

Gossett, S. (2022) Automotive IoT: A Brief Overview of the Connected Car

https://builtin.com/internet-things/iot-in-vehicles

IoT Sverige (2023) IoT – så funkar det https://iotsverige.se/om-oss/iot-sa-funkar-det

Jesson, Jill, Matheson, Lydia, Lacey, Fiona M. (2011) Doing your literature review: Traditional and systematic techniques

Joy, J. & Gerla, M. (2017). Internet of Vehicles and Autonomous Connected Car - Privacy and Security Issues https://ieeexplore-ieee-org.libraryproxy.his.se/document/8038391

Jalali, S., Wohlin, C. (2012) Systematic literature studies: Database searches vs. backward snowballing https://ieeexplore.ieee.org/document/6475394

Jiaqi Huang, Yi Qian, Rose Qingyang Hu (2021) A Privacy-Preserving Scheme for Location-Based Services in the Internet of Vehicles https://ieeexplore-ieee-org.libraryproxy.his.se/document/9663103

Javier, F. (2022) Cybersecurity in electric car's operational technology (OT) https://upcommons.upc.edu/handle/2117/375182

Kaspersky (2017) Appar för uppkopplade bilar saknar skydd mot intrång

https://www.kaspersky.com/about/press-releases

kryptomagasin.se (2021) Vad är blockchain? – Enkel och begriplig förklaring

https://kryptomagasin.se/vad-ar-blockchain/

Kugali, S., Kadadevar, S. (2020) Vehicular ADHOC Network (VANET):-A Brief Knowledge

https://www.ijert.org/vehicular-adhoc-network-vanet-a-brief-knowledge

Kumar, S., Mary, G., Suresh, P., Uthirasamy, R. (2021) Investigation On Cyber-Attacks Against In-Vehicle Network

https://ieeexplore-ieee-org.libraryproxy.his.se/document/9383720

Kexun, H., Changyuan, W., Yanyan, H., Xiyu, F. (2020) Research on cyber security Technology and Test Method of OTA for Intelligent Connected Vehicle https://ieeexplore-ieee-org.libraryproxy.his.se/document/9196445

Kim, K., Kim, J., Jrong, S., Park, J., Kim, H. (2021) Cybersecurity for autonomous vehicles: Review of attacks and defense https://www.sciencedirect.com/science/article/abs/pii/S0167404820304235

Khan, S., Shiwakoti, N., Stasinopoulos, P., Warren, M. (2021) Security assessment in Vehicle-to-Everything communications with the integration of 5G and 6G networks https://ieeexplore-ieee-org.libraryproxy.his.se/document/9644368/authors#authors

Khan, H., Hanif, A., Ahmed, Q. (2023) Threat Analysis of Position, Navigation, and Timing for Highly Automated Vehicles https://ieeexplore-ieee-org.libraryproxy.his.se/document/10140072

Kitchenham, B. (2004). Procedures for performing systematic reviews https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

Luo, F., Zhang, X., Hou, S. (2021) Research on Cybersecurity Testing for In-vehicle Network https://ieeexplore-ieee-org.libraryproxy.his.se/document/9637070

Li, W., Guo, H., Nejad, M., Chen, C. (2020) Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach https://ieeexplore.ieee.org/abstract/document/9210529/authors#authors

Masood, M., Saeed, Z. & Khan, U. M. (2023). A Review: Cybersecurity Challenges and their Solutions in Connected and Autonomous Vehicles (CAVs) http://jaree.its.ac.id/index.php/jaree/article/view/322

Marty, K. (2021) How cybersecurity will impact the automotive market https://certx.com/automotive/unece-wp-29-r155-how-cyber-security-will-impact-the-automotiva-market-as-of-june-2022/

Malik, S., Sun, W. (2020) Analysis and Simulation of Cyber Attacks Against Connected and Autonomous Vehicles https://ieeexplore-ieee-org.libraryproxy.his.se/document/9138643

Metoddoktorn (2023) vägledning för uppsatser och PM i företagsekonomi
https://libguides.mdu.se/c.php?g=678062&p=4832296

Moukahal, L., Zulkernine, M. (2019) Security Vulnerability Metrics for Connected Vehicles
https://ieeexplore-ieee-org.libraryproxy.his.se/document/8859489/authors#authors

Moukahal, L., Zulkernine, M., Soukup, M. (2021) Vulnerability-Oriented Fuzz Testing for Connected Autonomous Vehicle Systems
https://ieeexplore-ieee-org.libraryproxy.his.se/document/9557794/authors#authors

MyCarly.com (2023) OBD-port – Vad är en OBD-port och hur används den?
https://www.mycarly.com/sv/blog/obd-sv/obd-port-vad-ar-en-obd-port-och-hur-anvands-den/

Masood, A., Lakew, D., Cho, S. (2020) Security and Privacy Challenges in Connected Vehicular Cloud Computing
https://ieeexplore-ieee-org.libraryproxy.his.se/document/9152970/authors#authors

McKinsey & Company (2020) With the software content of cars increasing, what do automotive players need to know about cybersecurity?
https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge

Noh, J., Jeon, S., Cho, S. (2020) Distributed Blockchain-Based Message Authentication Scheme for Connected Vehicles https://www.mdpi.com/2079-9292/9/1/74

Nawrath, T., Fischer, D., Markscheffel, B. (2017) Privacy-sensitive data in connected cars https://ieeexplore.ieee.org/document/7856736/authors#authors

NHTSA. (2022) Vehicle-to-Vehicle
https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication

NHTSA (2022) Cybersecurity Best Practices for the Safety of Modern Vehicles
https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-pre-final-tag_0_0.pdf

Na, D., Park, S. (2021) Lightweight blockchain to solve forgery and privacy issues of vehicle image data.

https://ieeexplore-ieee-org.libraryproxy.his.se/document/9562586/authors#authors

National Oceanic and Atmospheric Administration (2023) What is Lidar and what is it used for?
https://www.americangeosciences.org/critical-issues/faq/what-lidar-and-what-it-used

Paré, Guy, Kitsiou, Spyros (2017) Methods for Literature Reviews, Handbook of eHealth Evaluation: An Evidence-based Approach, University of Victoria.

Placek, M. (2021) Connected cars worldwide - statistics & facts
https://www.statista.com/topics/1918/connected-cars/#topicOverview

Powers, J. (2022) Automotive IoT: A Brief Overview of the Connected Car
https://builtin.com/internet-things/iot-in-vehicles

Parling, A. (2011) INSTALLERA BLACKBOX
http://www.twostrokerider.se/installera-blackbox-

Patrick Lin (2015) TED-Ed: The ethical dilemma of self-driving cars
https://www.youtube.com/watch?v=ixIoDYVfKA0

Paperpile (2023) How to do a thematic analysis.
https://paperpile.com/g/thematic-analysis/

Rebiger, S., Moraes, T., Vergara, X. (2019) TechDispatch #3: Connected Cars
https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-3-connected-cars_en

Scribbr (2023) How to do thematic analysis | Step-by-step guide & examples.
https://www.scribbr.com/methodology/thematic-analysis/

Sun, X., Yu, F. & Zhang, P. (2021). A Survey on Cyber-Security of Connected and Autonomous Vehicles.
https://ieeexplore-ieee-org.libraryproxy.his.se/document/9447840

Svensk Handel (2023) Viktigt om dataskydd
https://www.svenskhandel.se/radgivning/dataskydd-och-integritet/viktigt-om-dataskydd

Sasank, V., Lokesh, B., Mahesh, J., Kumar, I., Kumar, T., Prasad, C. (2022) Security and Privacy in Associated Self Controlled Cars

https://ieeexplore-ieee-org.libraryproxy.his.se/document/9716404

Smith, L. (2021) en Senior Policy Counsel vid Future of Privacy Forum (FPF) och en ledande FPF Connected Cars Working Group sa om datasekretess inom bilar
https://www.financialexpress.com/auto/car-news/internet-connected-cars-what-data-is-collected-access-hyundai-venue-kia-sonet-seltos-mg-hector/2305516/

Singh, A. (2021) Internet-connected cars: What data is collected, who has the access and more
https://www.financialexpress.com/auto/car-news/internet-connected-cars-what-data-is-collected-access-hyundai-venue-kia-sonet-seltos-mg-hector/2305516/

Salek, M., Khan, S., Rahman, M., Deng, H., Islam, M., Khan, Z., Chowdhury, M., Shue, M. (2022) A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications
https://ieeexplore-ieee-org.libraryproxy.his.se/document/9716070

Thales (2023) A single automotive cyber security standard is coming at last

https://www.thalesgroup.com/en/worldwide-digital-identity-and-security/iot/magazine/single-automotive-cyber-security-standard

Tankeredskap (n.d.) Validitet och reliabilitet
(https://www.tankeredskap.se/tankeredskap/vetenskapsteori/hur-finner-vi-sanningen/vi-anvander-vetenskapen/metoder/neutral-forskning/validitet-och-reliabilitet/

Trafikvärket (2021) Uppkopplade fordon
https://bransch.trafikverket.se/for-dig-i-branschen/forskning-och-innovation/aktuell-forskning/transport-pa-vag/uppkopplade-fordon/

Tyagi, A. & Goyal, D. (2020) A Survey of Privacy Leakage and Security Vulnerabilities in the Internet of Things
https://ieeexplore-ieee-org.libraryproxy.his.se/document/9137886/authors#authors

Techironed (2022) How (Vehicular ad hoc network) VANET works in Networking?
https://techironed.com/how-vehicular-ad-hoc-network-vanet-works-in-networking/

Universitetsbiblioteket (2023) Systematisk litteraturöversikt som examensarbete
https://kib.ki.se/soka-vardera/systematiska-oversikter/systematisk-litteraturoversikt-som-examensarbete

Vetenskapsrådet (2022) Etik i forskningen och god forskningssed

https://www.vr.se/uppdrag/etik/etik-i-forskningen.html

Vipin Kumar Kukkala, Sooryaa Vignesh Thiruloga, Sudeep Pasricha (2022). Roadmap for Cybersecurity in Autonomous Vehicles
https://ieeexplore-ieee-org.libraryproxy.his.se/document/9721088

Volkswagen (2023) Vad är uppkopplade bilar?
https://www.volkswagen.se/sv/innovation-och-teknik/uppkopplade-bilar.html

Volvo (2020) LiDAR-teknik för säker självkörning i nästa generations Volvobilar.

https://www.media.volvocars.com/se/sv-se/media/pressreleases/268323/lidar-teknik-for-saker-sjalvkorning-i-nasta-generations-volvobilar

Vurpillat, J. (2021) What is connected car data
https://otonomo.io/blog/connected-car-data/#:~:text=Connected%20cars%20generate%20car%20data%20attributes%20that%20specify,Controller%20Access%20Networks%20%28CANs%29%2C%20and%20even%20infotainment%20systems.

Wikipedia (2023) Styrenhet (fordon)
https://sv.wikipedia.org/wiki/Styrenhet_%28fordon%29

Wang, Y., Yu, B., Yu, H., Xiao, L., Ji, H., Zhao, Y. (2023) Automotive Cybersecurity Vulnerability Assessment Using the Common Vulnerability Scoring System and Bayesian Network Model
https://ieeexplore-ieee-org.libraryproxy.his.se/document/10002327

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). Experimentation in software engineering. Heidelberg: Springer

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. European journal of information systems

Wu, Z., Liu T., Jia, X., Sun, C. (2021) Security design of OTA upgrade for intelligent connected vehicle
https://dl-acm-org.libraryproxy.his.se/doi/10.1145/3473714.3473851

Yadav, N., Ansar, S., Chaurasia, P. (2022) Review of Attacks on Connected and Autonomous Vehicles (CAV) and their Existing Solutions
https://ieeexplore-ieee-org.libraryproxy.his.se/document/9965024