Samverkande IoT-system och databearbetning

Ronnie Johansson (red.), Maria Andersson,
Pontus Hörling, Farzad Kamrani

FOI-R--4884--SE

December 2019

FOI

Ronnie Johansson (red.), Maria Andersson, Pontus Hörling, Farzad Kamrani

Samverkande IoT-system och databearbetning

Titel	**Samverkande IoT-system och databearbetning**
Title	IoT systems collaboration and data processing
Rapportnr/Report no	FOI-R--4884--SE
Månad/Month	December
Utgivningsår/Year	2019
Antal sidor/Pages	63
ISSN	1650-1942
Kund/Customer	FMV
Forskningsområde	Ledningsteknologi
FoT-område	Ledning och MSI
Projektnr/Project no	E64153
Godkänd av/Approved by	Cecilia Dahlgren
Ansvarig avdelning	Försvars- och säkerhetssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Bild/Cover: Shutterstock

Sammanfattning

Den tekniska utvecklingen, bland annat i form av telekommunikation med hög bandbredd och miniatyriserad energisnål elektronik, stimulerar investeringar i IoT-system och framväxten av fenomen som ”smarta städer.” Målet är att ökad tillgång på (relevant) data skall möjliggöra uppföljning och effektivisering av existerande verksamhet eller skapandet av helt nya tjänster. Samtidigt finns det en potential i att IoT-system som tjänar ett visst syfte kan komma till användning i en annan verksamhet, exempelvis för samverkan vid samhällskriser. Särskilt myndigheter kan tänkas vara benägna av att samverka kring IoT-system. Försvarsmakten skulle kunna vara intresserat att förstärka sin lägesbild i ett insatsområde med hjälp av offentliga IoT-system.

I den här rapporten undersöker vi dels hur stor beredskapen för IoT-samverkan är idag (år 2019) hos svenska offentliga organisationer, vilken visar sig vara begränsad, dels exempel på IoT-samverkan utanför Sverige och hur utvecklingen skulle kunna se ut i den närmaste framtiden.

Rapporten har dessutom två självständiga och mer tekniska delar: hantering av strömmande data och informationsbearbetningsmetoder. Data som genereras av IoT-system utgörs ofta av en ström av data och vi beskriver ett tekniskt stöd för att hantera sådana dataflöden. Vi presenterar också en litteraturstudie över metoder (främst från AI-området) som kan användas för att bearbeta den strömmande IoT-information samt förbättra hanteringen av IoT-system.

Vi avslutar med några rekommendationer för vidare arbete.

Nyckelord: IoT, Internet of things, sakernas internet, samverkan

Summary

Technological developments, including in the form of high bandwidth telecommunications and miniaturized energy-efficient electronics, stimulate investment in IoT systems and the emergence of phenomena such as “smart cities”. The goal is to increase access to (relevant) data to enable monitoring and stream-lining of existing operations or the creation of entirely new services. At the same time, there is a potential that IoT systems that are intended to serve a specific purpose can support other activities. Especially government agencies may be interested in collaborating on IoT systems and data. The Swedish Armed Forces could be interested in strengthening its situation picture in an intervention area with the help of public IoT systems.

In this report, we investigate, on the one hand, the readiness today (in 2019) for IoT collaboration among Swedish public organizations, which turns out to be limited, and, on the other hand, examples of IoT collaboration outside Sweden and what the development may look like in the near future.

In addition, the report has two more independent and technical parts: streaming data management and information processing methods. Data generated by IoT systems consists of a stream of data and we describe a technical support for managing such data flows. We also present a literature study of methods (mainly from the AI area) that can be used to process streaming IoT information and improve the management of IoT systems.

We conclude with some recommendations for further work.

Keywords: IoT, Internet of things, cooperation

Innehållsförteckning

1 Inledning

FOI fick i juni 2019 i uppdrag av Försvarets materielverk (FMV) att dels undersöka civila myndigheters nyttjande av IoT-system[1] och förmåga att dela IoT-data mellan myndigheter, samt dels att undersöka vissa tekniska aspekter på IoT-system. Finns förmågan hos myndigheter att samverka om IoT-system så finns även den tekniska möjligheten för Försvarsmakten (FM) att ta del av den informationen, för att exempelvis förstärka sin lägesbild. Vi förtydligar vad vi menar med IoT-samverkan i avsnitt 1.1.

Arbetet är en fortsättning på tidigare projekt. (Johansson, 2018)

1.1 Bakgrund

Sakernas internet (eng. *Internet of things, IoT*) är ett samlingsnamn för teknik som kortfattat handlar om att med modern telekomteknik, strömsnåla och miniatyriserade sensorer och processorer, och internetteknik göra information från sensorer tillgängliga för delning och därmed skapa nya tjänster baserat på den informationen (definitionen av IoT och relaterade begrepp hanteras i Bilaga 1). I och med den planerade 5G-teknikens introduktion under början av 2020-talet förväntas IoT-tekniken få sitt stora genombrott. 5G-nätet möjliggör större dataflöden och fler uppkopplade sensorer. Nya IoT-tjänster kommer att utvecklas som bland annat kommer att användas av civila organisationer och myndigheter för att automatisera och effektivisera sin verksamhet.

FM kan tänkas komma i kontakt med IoT-system[2] 1) genom att externa civila system tas i bruk och blir en del av samhällets teknologiska infrastruktur; 2) interna tekniska system som FM upphandlar (exempelvis system för underhåll av fordon) kommer att levereras med IoT-system; och 3) omvärldens militära organisationer (fientliga, neutrala, samarbetspartners) skaffar sig IoT-system som därmed måste beaktas i försvarsplaneringen.

I den här rapporten fokuserar vi på den förstnämnda formen, nämligen de möjligheter som förekomsten och framväxten av civila IoT-system erbjuder FM:s verksamhet och hur förutsättningarna ser ut idag. En stor

[1] IoT är en förkortning av *Internet of things* eller *Sakernas internet* på svenska.

[2] Med IoT-system menar vi en samling IoT-noder som kan samla in och förmedla data samt den teknologi som krävs för att skapa en viss tillämpning.

utmaning är dock att det för att nyttja andra IoT-system är dels är känt vilken data som finns tillgänglig (inklusive dess mening och kvalitet) samt att den kan (rent tekniskt) och får (rent juridisk) delas. Därför är förmodligen de IoT-system som först och främst kan komma till användning av FM de som används i offentlig verksamhet (dvs. resurser som används av myndigheter, kommuner och landsting). I vår föregående rapport (Johansson, 2018, s. 6) nämnde vi några typiska användningsområden med offentlig IoT: stöd till samhällsfunktioner, datainsamling för verksamhetsutveckling, stadsplanering, och krishantering.

En del data samlas in för real-tids bevakning och styrning av någon process (exempelvis för styrning av tillverkningslinor och trafikflöden), medan andra data samlas in under lång tid för att erbjuda statistiskt underlag (exempelvis för mätningar av luftföroreningar eller för planering av gågator). I många fall kommer datainsamlingen (vilken typ av data, hur ofta den samlas in etc.) och datalagringen (hur data representeras och lagras) vara skräddarsydd för en bestämd tillämpning och dess värde för en utomstående användare kan vara begränsat.

I viss utsträckning har vi redan idag ett samhälle där data samlas in för att användas för olika syften, i real-tid eller för långsiktig lagring och analys. Med 5G-tekniken och annan infrastruktur blir det mer och snabbare datatrafik. Alla dessa data kommer inte bli tillgängliga för samhällelig nytta, men det kan förväntas att åtminstone offentliga organisationer kommer vilja dela sina data.

Det kräver dock att myndigheterna vet vilka data som finns tillgänglig samt att de kan (rent tekniskt) och får (rent juridisk) delas.

Vi ser framför oss en digitaliserad värld där IoT-system ständigt installeras, anpassas, och uppgraderas på ett organiskt sätt (efter behov) mer eller mindre oberoende av varandra av skilda ägare. Vi introducerar begreppet *IoT-samverkan* i den här rapporten och använder det flitigt. *Samverkan* definieras som följer i (MSB, 2014, s. 20), d.v.s.

> *Samverkan är den funktion som, genom att aktörer kommer överens, åstadkommer inriktning och samordning av tillgängliga resurser.*

Samordning i definitionen ovan betyder vidare ”[…] anpassning av aktiviteter och delmål så att tillgängliga resurser kommer till största möjliga nytta.” och att ” Samordning handlar om att aktörer inte ska vara i vägen för varandra, och hjälpa varandra där det går.”

Med IoT-samverkan menar vi då att IoT-system har förmågan att dela med sig av sina insamlade data till godtyckliga (men behöriga) användare

(mänskliga individer eller andra tekniska system). Ett samverkande IoT-system kan eventuellt även erbjuda ett gränssnitt för styrning av dess datainsamling och ställdon.

Några färdigheter som krävs för att dra nytta av teknikutvecklingen är dels 1) infrastrukturen som krävs för att hantera data som "strömmar" från IoT-system samt 2) smart informationsbearbetning och styrning av dataströmmen (exempelvis genom AI-metoder). Vi behandlar även dessa två områden separat i vår rapport.

1.2 Syfte

Uppdragsgivaren FMV har ett intresse för FM:s möjlighet att ta del av IoT-data för informationsutbyte av IoT-data mellan olika organisationer.

Som ett steg på vägen för att nå ovanstående mål skall projektet dels erbjuda insikt i hur det ser ut på myndigheterna idag (nyttjas IoT-system och delas data?) och dels undersöka existerande samverkan samt möjligheten till samverkan.

Projektet rymmer också en teknisk del som beskriver teknik för att hantera strömmande data samt informationsbearbetningsmetoder för att nyttja IoT-data.

1.3 Avgränsningar

I avsnitt 1.1 listar vi tre skilda sammanhang där FM kan tänkas behöva ta hänsyn till IoT-system. Arbetet som redovisas i den här rapporten rör främst den första typen, dvs. FM:s förhållande till externa civila system, och då främst IoT-system för offentlig verksamhet.

Vi tittar i det här arbetet inte på FM:s egen förmåga att begära extern IoT-data och nyttja den (det är inte nåbart inom ramen för det rådande projektet) utan vi begränsar oss till myndigheternas samarbetsförmåga vad gäller IoT-data.

Samtidigt som IoT-system erbjuder en förhoppning om tillgång till intressant data och ett förbättrat beslutsstöd, så ökar användarens sårbarhet eftersom IoT-systemet kan infiltreras och dess information stjälas eller manipuleras. Om IoT-systemet dessutom är ett *cyber physical system*, och därmed förutom datainsamling även har ställdon med förmåga att styra viss verksamhet (exempelvis trafikljus och –flöde) så riskeras att Totalförsvaret direkt motverkas av de egna IoT-systemen. Cybersäkerhet, som förhindrar att IoT-system manipuleras eller tas över, är därmed en kritisk förmåga. Det är dock ett omfattande område som

förtjänar att behandlas separat. Vi hänvisar t.ex. till FOI:s rapport (Kamrani, Wedlin, & Rodhe, 2016) för mer information.

1.4 Metod

Projektet är uppdelat i tre delar av olika karaktär:

i) myndighetssamverkan,

ii) strömmande data,

iii) informationsbearbetningsmetoder och styrning.

Del i) utfördes primärt genom att dels se över den kunskap som FOI redan har om myndighetssamverkan, men även genom direkta kontakter med företrädare för svenska myndigheter och organisationer som bland andra MSB,[3] DIGG,[4] forskningsinstitutet RISE,[5] och det Vinnova-sponsrade strategiska innovationsprogrammet IoT Sverige.[6] Kontakterna har typiskt inletts med en öppen fråga om respektive organisations IoT-bruk: ”Nyttjas IoT-system i er organisation idag?”

Under arbetets gång har vi även deltagit i en del nationella möten och konferenser med koppling till IoT. Den 10:e oktober 2019 deltog vi i IoT Sveriges årskonferens i Uppsala, den 5:e och 6:e november i ECS 2019[7] på Kistamässan, och den 19:e november i konferensen Mötesplats Samhällssäkerhet[8] på Kistamässan.

Del ii) om strömmande data presenterar exempel på hur sådan kan hanteras och omfattar främst webbaserad dokumentation av ämnet och datatekniska verktyg för ändamålet.

Del iii) gör ett ostrukturerat urval ur den tillgängliga litteraturen (främst från IEEE Internet of Things Journal) om informationsbearbetnings-

[3] Myndigheten för samhällsskydd och beredskap, https://www.msb.se/

[4] Myndigheten för digital förvaltning, https://www.digg.se/

[5] Research institutes of Sweden, https://www.ri.se/

[6] IoT Sverige (https://iotsverige.se/) startade 2014 och är ett av ett tiotal så kallade strategiska innovationsprogram gemensamt finansierade av Vinnova, Energimyndigheten och Formas. ” IoT Sverige finansierar innovationsprojekt som sker i samverkan mellan offentlig sektor, som är programmets huvudsakliga behovsägare, och företag, akademi/institut och civilsamhället.”

[7] Embedded conference Scandinavia, http://embeddedconference.se

[8] https://www.samhallssakerhet.se/

metoder för IoT-system för att ge exempel på existerande metoder och resultat.

1.5 Läsanvisningar

I kapitel 2 beskriver vi vad vi kommit fram till om svenska offentliga aktörers engagemang rörande IoT-system, och erbjuder några tankar om framtiden. Vi diskuterar även forskningen om IoT-interoperabilitet och några olika internationella initiativ. I kapitel 3 beskriver vi hur strömmande IoT-data kan hanteras. I kapitel 4 gör vi ett nedslag i litteraturen om olika datalogiska metoder (framför allt AI-metoder) för att bearbeta IoT-data och styra IoT-system. Slutligen i kapitel 5 bidrar vi med en sammanfattning och tentativa förslag på vidare arbete.

Notera att vi använder fotnötter flitigt i den här rapporten för att erbjuda förtydliganden och vidarebefordra den intresserade läsaren till fördjupad läsning.

2 Myndighetssamverkan med IoT

Myndighetssamverkan sker exempelvis inom ramen för det civila försvaret. I det här kapitlet diskuterar vi behovet av IoT-samverkan mellan myndigheter, hur det ser ut idag med sensordatautbyte, och vilken teknik och vilka system som finns tillgängliga för samverkan.

Vi blickar också utåt för att se hur samverkan mellan IoT-system har behandlats av andra organisationer och i forskningen.

2.1 Drivkrafter för IoT-samverkan

Samarbete i Totalförsvaret är kanske för FM både den mest intressanta drivkraften för samverkande IoT-system och också den mest tydliga samverkansuppgiften som offentliga organisationer kan samlas kring.

MSB som har en central roll i samordningen av den civila delen av Totalförsvaret har ett särskilt intresse för samordning mellan myndigheter. Bland annat betonas teknisk samordning för att kunna dela information vid samhällsstörningar och slutsatsen kan dras att en ”standardiserad miljö som gör det möjligt att dela information” behövs. (MSB, 2014)

En sådan miljö skall ha ”standardiserade och väl kända gränsytor och informationsformat som stödjer informationsutbyte på ett effektivt och säkert sätt.” Det noteras också att den svenska förvaltningsmodellen ställer till problem då den uppmuntrar myndigheterna att skapa individuella lösningar som enbart inriktar sig på myndighetens egna uppdrag och inte stimulerar stöd för samverkan.

Ett antal komponenter som stöder bildandet av individuella och samlade lägesbilder har också identifierats.[9] Flera av dessa komponenter är i grunden icke-tekniska men kan i varierande utsträckning understödjas av tekniska hjälpmedel. Det handlar bland annat om att dela rätt information, anpassa delad information efter mottagaren, och visa vilka resurser som finns tillgängliga hos samarbetspartners.

En allvarlig samhällskris kan beskrivas med tre faser där behovet av informationssamverkan skiljer sig åt. (Lindgren, o.a., 2018) Dessa är:

- Fas 1 - *Nuläge*: Detta är krisens omedelbara uppkomst och existens.

[9] Begreppet *lägesbild* diskuteras vidare på djupet i (Landgren & Borglund, 2016).

- Fas 2 - *Efter några dagar*: Den mest akuta krisen har gått över, men många störningar kvarstår. Exempel på sådana störningar är hos transporter och kollektivtrafik.
- Fas 3 - *Efter några veckor*: Nu fungerar samhället i stort sett normalt, men det kvarstår vissa störningar som behöver åtgärdas.

Vid den akuta krisen (Fas 1) finns en stor efterfrågan på information som kan ge en god överblick över krisområdet. Myndigheter samverkar för att skapa en så god lägesbild som möjligt. En efterfrågad typ av sensor i denna fas är kameran, antingen en fast monterad kamera eller en mobil kamera placerad exempelvis på en UAS (Unmanned Aerial System). Ingen direkt uttalad samverkan verkar finnas för de tidsperioder som följer på den akuta krisen (Fas 2 och Fas 3). En tolkning är att samverkan kan vara mycket begränsad eller rentav sällsynt i dessa faser (Lindgren, o.a., 2018).

I övrigt så kan det finnas behov av att samla in och dela lokal information, exempelvis om luftkvalitet vilket kommunerna är ålagda att göra.[10] Offentliga aktörer kan också vara intresserade av att dela information för att stödja näringslivet (exempelvis för utveckling av nya tjänster).

2.2 Offentlig IoT-samverkan – idag och framöver

Vi väljer att lite grovt dela upp den offentliga verksamheten i två grupper: myndigheter och kommuner då IoT-verksamheten inom dessa grupper förefaller ha olika drivkrafter och aktiviteter. Vad det gäller kommuner är det exempelvis naturligt att fokusera på tillämpningsområdet ”smarta städer”, medan myndigheterna har ett fokus som är frikopplat från en viss geografisk plats. För båda grupperna gäller att i den mån IoT-system är relevant för respektive verksamhet så är verksamheten i bara startgroparna. Det är varken så att man har IoT-utrustning eller beredskap att samverka, men inte heller (ännu) så att man har byggt fast sig i någon myndighetsspecifik teknik som försvårar eller omöjliggör IoT-samverkan. Nackdelen med nuvarande situationen är alltså att effektivt utnyttjande av IoT-data över myndighetsgränserna fortfarande är en framtidsvision. Fördelen är att det fortfarande finns en möjlighet att utforma framtidens IoT-samverkan.

[10] Naturvårdsverket, http://www.naturvardsverket.se/Stod-i-miljoarbetet/Vagledningar/Luft-och-klimat/Miljokvalitetsnormer-for-utomhusluft/Rapportera-luftkvalitetsdata/, besökt 2019-12-08

2.2.1 Myndigheter

I dag sker ingen formaliserad samverkan med sensorer eller sensordata hos bevakningsansvariga myndigheter. Detta är en av slutsatserna från MSB-projektet BEViS. (Lindgren, o.a., 2018) BEViS leds av Polisen och flera svenska myndigheter deltar. Några av de mest engagerade myndigheterna är Trafikverket, FM, FOI och FMV. Slutsatsen relaterar först och främst till de bevakningsansvariga myndigheter som deltar i BEViS.

Samverkan inom bevakningsområdet kan idag beskrivas som en ad hoc-samverkan som kommer till stånd vid akuta situationer. Räddningstjänsten, Trafikverket och Polisen kan samverka exempelvis via kamerabilder för att snabbare få information om omfattningen av en allvarlig händelse (Andersson, Lindgren, Nilsson, Berglund, & Svenonius, 2019). Samverkan inom bevakningsområdet kan även ske kring utbildning och övningar, samt till viss del vid inköp och anskaffning (Nilsson, Lindgren, Andersson, & Nordlöf, 2018).

BEViS undersöker hur samverkan om sensordata mellan myndigheter ska kunna formaliseras i organisationerna på ett effektivt sätt. Projektet tar även upp frågor kring juridik och informationssäkerhet, vilket är viktiga frågor vid samverkan med sensorer och sensorinformation.

Samverkan är ofta baserad på personliga kontakter mellan enskilda tjänstemän. Detta gör att samverkan idag kan påverkas bland annat av personalförändringar. Någon slutar sin anställning och byter till ett nytt jobb, och risken finns då finns att samverkansmöjligheten minskar under en period.

På 2019 års konferens ”Mötesplats Samhällssäkerhet” nämndes samverkan som en viktig faktor i flera presentationer. Samverkan mellan samhällsaktörer har ökat under senare år, och ses som en nödvändighet för ett säkert samhälle. Det är mer samverkan idag inom eller mellan kommuner och länsstyrelser jämfört med fyra år sedan. Övningar och utbildningar mer besökta idag än tidigare. Frivilligorganisationer samverkar vid kriser i större utsträckning i dag. (Samhällssäkerhet, 2019) Ett exempel på ett sådant tillfälle är skogsbränderna i Sverige 2018. (SOU, 2019) Ett önskemål från andra samhällsaktörer är att Frivilligorganisationerna ska kunna delta i samverkan i ännu större utsträckning. (Samhällssäkerhet, 2019) Totalförsvarsövningen 2020 (TFÖ 2020) är en aktivitet som initierar ökad samverkan mellan det militära och civila försvaret. TFÖ 2020 kommer att öva hur samhällsaktörer ska samverka för att kritiska funktioner ska fortsätta att fungera trots svåra påfrestningar. TFÖ 2020 kommer också att öva hur samhället ska prioritera resurser och fördela förnödenheter. (MSB, 2019) En viktig

förutsättning för att kunna ta rätt beslut är en samlad lägesbild. IoT-lösningar skulle kunna bidra med ytterligare information till den samlade lägesbilden.

Vi har under projektet även försökt att skapa oss en bild av i vilken utsträckning IoT-system används inom övriga svenska myndigheter. Vi har hört med MSB om deras uppfattning men även haft direkt kontakt med några myndigheter, bland andra Tullverket och Polisen. Vårt första intryck, även om en noggrannare undersökning skulle kunna ge en annan bild, är att användningen än så länge är begränsad. Vi valde därför att denna gång fokusera på MSB och deras stödsystem (se mer i avsnitt 2.2.3). Vår bild verkar överensstämma med en MSB-finansierad rapport där 13 myndigheter ingick. (Lindman & Saarikko, 2018, ss. 32-33) Värt att nämna är att Polisen är involverad i ett pågående projekt som bland annat omfattar logistik av bevismaterial.[11]

2.2.2 Kommuner

Hos kommuner och landsting finns det ett stort intresse av att göra data tillgängliga, inte minst för att sådana krav ställs från staten. Flera dataportaler har skapats för att dela PSI-information (public sector information).[12] Informationen är dock, så vitt vi kan förstå, statisk och åtkomsten saknar flera av de egenskaper som kan önskas vid IoT-samverkan nämligen realtidsåtkomst och möjlighet att styra IoT-systemen.

Andra exempel på pågående IoT-verksamheter är mellan kommuner, företag och organisationer. I ett samarbete mellan Karlshamn Energi, Affärsverken, Olofströms Kabel-TV och Ronneby miljöteknik provas IoT i syfte att hitta besparing för verksamheter samt ge invånarna utökad service. (Sydöstran, 2019) Kalmar Energi och Linnéuniversitetet låter invånare i Kalmar testa idéer inom IoT och på så sätt få prova på både möjligheter och utmaningar med tekniken. (Linnéuniversitetet, 2019) Härryda kommun driver fem pilotprojekt som handlar om att med IoT kontrollera bland annat vägtemperaturer och nivåmätning av spill- och dagvatten samt övervaka nätstationer och kabelskåp. (Industrinyheter, 2019)

[11] https://nfc.polisen.se/om-nfc/nyhetsarkiv/2018/december/nationellt-centrum-for-iot-internet-of-things/ , besökt 2019-12-08

[12] Den nationella dataportalen: https://oppnadata.se/
Stockholms stads dataportal: https://dataportalen.stockholm.se/ , besökta 2019-12-08

Det finns en risk att kommunerna för sin lokala verksamhet utvecklar och upphandlar sina egna IoT-system och utvecklar egna datamodeller och åtkomstmetoder utan att ta in samverkansnytta i beräkningen. Det finns dock för närvarande ett försök att råda bot på den risken. Forskningsinstitutet RISE driver nämligen ett projekt, ”City as a platform”,[13] som omfattar 18 svenska kommuner (inklusive de folkrikaste) och primärt syftar till att dra gemensamma lärdomar och effektivisera skapandet av smarta städer. Även om projektets mål inte direkt är IoT-samverkan så kan exempelvis gemensamma datamodeller bli ett nyttigt resultat.

2.2.3 Framtiden

För den framtida utvecklingen finns idag inte några permanenta offentliga aktörer med uttalat ansvar för IoT-samverkan. Det finns däremot två aktörer som skulle kunna få det ansvaret: DIGG och MSB. Den blott dryga året gamla[14] Myndigheten för digital förvaltning (DIGG) har ett regeringsuppdrag att öka tillgängligheten i öppen data och stödja ”datadriven innovation.” Men fokus på uppdraget är spridandet av öppen information (till allmänhet och näringsliv) och inte specifikt att skapa myndighetsinteroperabilitet för data.

MSB kommer förmodligen vara en viktig aktör för framtida IoT-samverkan, dels för att MSB som företrädare för det civila försvaret har ett operativt ansvar, dels för att myndigheten redan idag utvecklar och förvaltar en rad system för samverkan mellan myndigheter. Några exempel är Rakel, SGSI och WIS, system som är under ständig utveckling och direkt kan bidra till att möjliggöra IoT-samverkan. För gemensam lägesbild till sjöss finns Sjöbasis där Kustbevakningen har lett utvecklingen. Verktygen och systemen beskrivs kortfattat i avsnitten 2.3 till 2.6.

För att myndigheter skall kunna utbyta IoT information på ett flexibelt och säkert sätt behövs en lämplig infrastruktur som garanterar dessa egenskaper. En flexibel lösning skulle möjliggöra att myndigheter vid behov inhämtar IoT-information från någon annan myndighet utan att först behöva införskaffa särskild utrustning och begära tillstånd. En gemensam molntjänst skulle kunna vara en sådan lösning.

[13] https://www.ri.se/sv/vad-vi-gor/projekt/city-platform, pågår 2018-2021

[14] Myndigheten startade sitt arbete den 1:a september 2018.

En hel del krav ställs dock på en sådan eventuell molntjänst då viss information endast bör nyttjas internt eller är känslig på annat vis (exempelvis omfattas av GDPR).

I slutet av september 2019 meddelade svenska Regeringen att den avser att utreda förutsättningarna för en statlig molntjänst. Resultatet väntas i maj 2021. Under tiden har Försäkringskassan en särskild uppgift, som sträcker sig fram till 2023, att underhålla molntjänster för vissa myndigheter. (Ekot, 2019; NyTeknik, 2019) Det är mycket troligt att SGSI kommer att ligga till grund för den molntjänsten och att Rakel möjliggör trådlös koppling mellan IoT-sensorer och det framtida myndighetsmolnet.

I december 2019 följde regeringen upp med ett besked om att även arbetet med att möjliggöra datautbyte mellan myndigheter skall utföras under DIGG:s ledning. (Sveriges Radio, 2019)

2.3 Rakel

Rakel[15] är ett verktyg för radiokommunikation mellan personer inom samhällsviktiga verksamheter. (MSB, 2018) Med Rakel kan användare ringa och ta emot samtal, sända och ta emot data samt komma åt vissa databaser. Det går även att sköta vissa tekniska funktioner såsom övervakning av tekniska system. Det kan exempelvis vara övervakning av el-, vatten och värmeförsörjningssystem. Planen är att framöver förstärka Rakel med ökad datakapacitet, samt även tjänster för sekretess.

MSB och Trafikverket har samarbetat i ett projekt där Rakel kompletteras med en lösning för mobila tjänster som bild- och dataöverföring. Tjänsten kallas MVNO (Mobile Virtual Network Operator) och innebär att det skapas en mobiloperatör utan ett eget radionät men där det är möjligt att överföra data via kommersiella nät. I detta fall är det Trafikverket som är den virtuella mobiloperatören. Andra myndigheter som använder Rakel kan också använda MVNO-tjänsten. (Trafikverket, 2019) Anledningen till MVNO-tjänsten är att Trafikverket vill modernisera sin hantering av sina mobilt uppkopplade utrustningar såsom trafiksäkerhetskameror, vägväderinformation och skyltar. Antalet uppkopplade utrustningar är stort, närmare 10 000 stycken. (Trafikverket, 2019)

[15] https://www.msb.se/sv/verktyg--tjanster/rakel/, besökt 2019-12-08

2.4 SGSI

SGSI[16] (Swedish Government Secure Intranet) är en krypterad kommunikationstjänst för samverkan mellan myndigheter dels i Sverige, dels i Europa via EU-nätet TESTA. SGSI utgörs av ett intranät. Det är därmed skiljt från internet och påverkas därför inte av störningar såsom överbelastningsattacker. SGSI är avgiftsfinansierad. (MSB, 2019)

Med SGSI är det möjligt att ta del av andra anslutna myndigheters databaser, skicka skyddad e-post samt ha videokonferenser. (MSB, 2018)

Det finns idag en koppling mellan SGSI och Rakel, vilket ökar möjligheterna till kommunikation med data, även ute i fält.

2.5 WIS

WIS[17] (webbaserat informationssystem) är ett internetbaserat informationssystem för delning av information. Med WIS är det möjligt att bygga upp en gemensam lägesbild. Aktörer som kan delta i WIS är myndigheter, kommuner, landsting, frivilligorganisationer och privata aktörer med ansvar under en kris. (MSB, 2019) Den typ av information som kan delas är anteckningar, lägesrapporter, dokument eller enkla kartnoteringar. Informationen kan sedan kategoriseras, delas, sökas och filtreras baserat de egna behoven. (MSB, 2019)

WIS hanterar öppen information, men kommunikationen över internet är krypterad. (MSB, 2019) Under 2019 ska en ny tjänst lanseras som möjliggör att WIS även finns på SGSI. WIS kan då användas även om internet inte fungerar.

2.6 Sjöbasis

Sjöbasis[18] är ett myndighetsgemensamt system för sjöbaserad informationssamordning. (Kustbevakningen, 2019) Systemet möjliggör ett informationsutbyte mellan Försvarsmakten och civila myndigheter.

[16] https://www.msb.se/sv/verktyg--tjanster/sgsi, besökt 2019-12-08

[17] https://www.msb.se/sv/verktyg--tjanster/wis , besökt 2019-12-08

[18] https://www.kustbevakningen.se/granslos-samverkan/sjoovervakningsuppdraget/samverkan-sjoinformation/ , besökt 2019-12-08

Sjöbasis samlar och bearbetar sjölägesinformation och sjöinformation. Informationen görs tillgänglig för de myndigheter som behöver den.

Sjölägesinformation är uppgifter om fartyg som rör sig på sjön. Sjöinformation är tilläggsinformation såsom fartygets ägare, besättning, last, kartor och väderinformation. Sjöinformation kan också vara misstankar om brott. (Kustbevakningen, 2019)

Exempel på myndigheter, förutom Kustbevakningen, som använder Sjöbasis är Försvarsmakten, Rikspolisstyrelsen, Tullverket, Transportstyrelsen, Sjöfartsverket, MSB, Havs- och vattenmyndigheten, SMHI, Naturvårdsverket och Sveriges Geologiska Undersökning. (Kustbevakningen, 2019)

En ny version av Sjöbasis sattes i drift 2017. (Kustbevakningen, 2019) Den nya versionen innehåller bland annat en AI-modul för anomalidetektion. AI-modulen varnar när fartygets beteende avviker från det normala. (HiQ, 2019)

En europeisk version av ett myndighetsgemensamt system för sjöbaserad informationssamordning är MARSUR (Maritime Surveillance Networking). (EDA, 2019) Syftet med MARSUR är att förbättra den gemensamma sjölägesbilden i Europa. Systemet gör det lättare att utbyta information mellan medlemsländer. Exempel på information som utbyts är fartygens positioner, målspår, identifikationsdata, chat och bilder.

2.7 Kommersiella verktyg

Förutom verktyg såsom Rakel, SGSI, WIS och Sjöbasis så använder myndigheterna även kommersiella verktyg för samverkan. Det kan röra sig om verktyg för videohantering vid övervakning, där kameror integreras i ett kameranätverk och informationen från kamerorna samlas in för att bidra till en lägesbild. Ett problem med kommersiella verktyg kan vara att garantera att informationen som hanteras behandlas på ett informationssäkert sätt. (MSB, 2018)

2.8 Interoperabilitet inom IoT

Interoperabilitet är enligt flera aktörer[19] den faktor som mest skulle påskynda fördelarna med IoT-interoperabilitet. Avsaknaden av

[19] https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-internet-of-things-five-critical-questions , besökt 2019-12-08

interoperabilitet (samverkan) har dessutom pekats ut som ett väsentligt hot mot de potentiella fördelarna med IoT och det förutsagda ekonomiska vinsterna. (Manyika, o.a., 2015) Många stora företag, bland andra Amazon[20] (AWS IoT), Cisco[21] (Jasper), IBM[22] (Watson), Apple[23] (HomeKit), Google[24] (Android Things), och Microsoft[25] (Azure IoT) har profilerat sig inom IoT marknaden och varje IoT-plattform främjar sin egen IoT-infrastruktur, protokoll, gränssnitt, format och semantik. IoT-interoperabilitet är en grundläggande förutsättning för att alla dessa lösningar tillsammans kan arbeta sömlöst och visionen om ett globalt IoT-ekosystem förverkligas. (Noura, Atiquzzaman, & Gaedke, 2019)

Interoperabilitet inom IoT är inte något nytt problem och interoperabilitet mellan olika informationssystem har en lång historia. Det finns flera definitioner av interoperabilitet i litteraturen men enkelt uttryckt betyder interoperabilitet *förmågan att fungera tillsammans*. Detta innebär att två interoperabla IoT-system ska kunna förstå varandra och använda varandras funktionalitet.

IEEE[26] definierar interoperabilitet som förmågan hos två eller flera system eller komponenter att utbyta information och förmågan att använda den information som har utbyts. Enligt denna definition realiseras interoperabilitet genom att utforma standarder. Inom IoT kan interoperabilitet definieras som två systems förmåga att kommunicera och dela tjänster med varandra.

Förmågan hos två system att interoperera kan presenteras på olika sätt. Man brukar använda sig av en modell som delas i olika nivåer, där den lägsta nivån inte kräver någon interoperabilitet och högre nivåer representerar en mer omfattande interoperabilitet. Tolk (2004) föreslår en flernivåmodell för interoperabilitet mellan två system (se Figur 1) som brukar kallas *LCIM* (eng. *Levels of Conceptual Interoperability Model*). Denna modell har reviderats flera gånger och finns i olika versioner som beroende på sammanhang varierar i detaljer och antal nivåer men för

[20] https://aws.amazon.com/iot/

[21] https://www.jasper.com/

[22] https://www.ibm.com/watson

[23] https://www.apple.com/lae/ios/home/

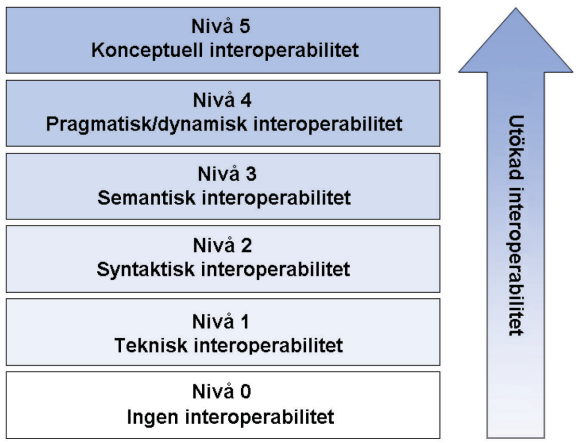
[24] https://developers.google.com/iot

[25] https://azure.microsoft.com

[26] https://www.ieee.org

enkelhetens skull håller vi oss till den ursprungliga modellen. I denna modell representerar nivåerna följande grad av interoperabilitet:

0) Två **isolerade** system med ingen anslutning alls.
1) En **teknisk** anslutning där **bitar** kan skickas mellan två system.
2) En **syntaxnivå** som tillåter att **data** i standardiserade format skickas mellan två system, dvs. de stödjer samma protokoll och format.
3) Den **semantiska** nivån, inte bara data utan även dess sammanhang, dvs. **information** kan skickas mellan två system. Den entydiga betydelsen av data som skickas är definierad av gemensamma referensramar.
4) Den **pragmatiska/dynamiska** nivån, information och dess användning och tillämpbarhet, dvs. **kunskap**, kan skickas mellan två system.
5) Den **konceptuella** nivån, dvs. två system kan etablera en gemensam lägesbild av världen.



Figur 1. Modell för interoperabilitet mellan två system, där nivå 0 är två isolerade system och nivå 5 representerar interoperabilitet på konceptuell nivå. (Tolk, 2004)

Det är tänkbart att det för IoT finns det ytterligare en högre nivå av interoperabilitet över nivå 5 av LCIM-modellen där två system inte bara delar en gemensam lägesbild utan använder och styr varandras sensorer och ställdon och gemensamt påverkar omgivningen.

Heterogenitet är förstås en försvårande omständighet för interoperabilitet inom IoT. Men heterogenitet är inte ett koncept begränsat bara till IoT.

Även i den fysiska världen finns det många typer av heterogeniteter, t.ex. att människor talar olika språk. De kan fortfarande kommunicera med varandra genom en översättare (människa/verktyg) eller genom att använda ett gemensamt språk. (Noura, Atiquzzaman, & Gaedke, 2019)

På samma sätt bör de olika elementen inom IoT (enheter, tjänster, applikationer etc.) kunna samarbeta och kommunicera med varandra för att IoT-ekosystemet ska förverkligas. Noura, Atiquzzaman, & Gaedke (2019) föreslår en taxonomi för IoT- interoperabilitet:

1) interoperabilitet mellan enheter,
2) interoperabilitet i nätverket,
3) syntaxnivå interoperabilitet,
4) semantisk interoperabilitet,
5) interoperabilitet mellan plattformar.

För en detaljerad tolkning av dessa nivåer och den tekniska innebörden av varje nivå hänvisar vi den intresserade läsaren till (Noura, Atiquzzaman, & Gaedke, 2019).

Den *Europeiska ekonomiska och sociala kommittén*[27] (EESK) har tydligt yttrat sig och på flera områden förespråkat vikten av interoperabilitet. Inom hälso- och sjukvården, som tycks vara ett område där interoperabilitet gör stor skillnad, förutspår EESK att digitalisering kommer att möjliggöra en allmän användning av hälsodata och sociala data. Här kommer troligen digitaliseringen att främja integreringen av system och enheter med maskininlärningstjänster och behovet av interoperabilitet och kapacitet för samverkan (maskin-till-maskin) där hänsyn tas till användares olika behov och preferenser. EESK har också angett flera andra yttranden om interoperabilitet mellan informationssystem av medlemsstaternas polis och rättsväsende, flyktingar och migration samt tull och gränskontroll.

2.9 Utblick mot övriga världen

Nedan beskrivs kortfattat igenom några olika intressanta utvecklingar som sker på den internationella arenan som kan ha bäring på IoT-samverkan.

[27] https://www.eesc.europa.eu/

Så vitt vi kan se så finns det idag inga färdiga COTS-lösningar[28] för samverkan mellan IoT-system. En aktör på marknaden är dock Thales som utvecklar ett ”integrationsramverk” för IoT-data, DPIF,[29] som FOI har arbetat med i ett EDA-projekt.[30]

Stora IT-företag som Ericsson[31] och Microsoft[32] vilka vill hitta nya affärsmöjligheter med IoT gör det de kan för att förenkla för sina kunder att investera i IoT-lösningar.

EU-kommissionen har en satsning sedan 2016 som kallas NGI (Next Generation Internet) initiative[33] som syftar till att se till att framtidens internet försvarar ”europeiska värden” som öppenhet, transparens, integritet och datasäkerhet. NGI omfattar bland annat byggande av ett europiskt ekosystem för IoT.

Nato har sedan en tid tillbaka en satsning som är av stor relevans för FM och dess förhållande till offentliga IoT-system. Den aktuella Nato-gruppen kallas IST-147 ”Military applications of the Internet of things”. (Johnsen, o.a., 2018) Gruppen har arbetat med ett scenario där en militär organisation drar nytta av den existerande infrastrukturen i en smart stad, och under 2017 genomfördes ett experiment i Helsingfors där verkliga smart-city sensorer nyttjades av simulerade militära enheter.

[28] Commerical-off-the-shelf, alltså färdigutvecklat och i sälj- och levererbart skick

[29] https://www.thalesgroup.com/en/dpif , besökt 2019-12-08

[30] FOI deltog under 2014-2016 i EDA-projektet IN-4-STARS2.0 som handlade om militär IoT i internationella insatser.

[31] https://computersweden.idg.se/2.2683/1.723983/5g-ericsson-smarta-saker-koppla-upp, besökt 2019-09-26

[32] https://computersweden.idg.se/2.2683/1.725646/iot-microsoft-prylar-verktyg, besökt 2019-10-30

[33] https://www.ngiot.eu/community/ngi-iot-initiatives/, besökt 2019-12.12

3 Strömmande data

IoT-system samlar vanligtvis in data och förmedlar dessa upprepade gånger under sin livstid och beroende på sin utformning ger de därmed ofta upphov till en (eller flera) tidsordnade strömmar av data i den takt data samlas in. Detta att jämföra med en mer traditionell hantering av data som exempelvis ett långsamt föränderligt medlemsregister i en relationsdatabas. För data som redan är lagrad, där datavolymen är känd, kan ingående data beroende på format läsas från början till slut i den ordning den är lagrad på datamediet (sekventiellt) eller i valfri ordning (direktaccess). Sekventiella filer kan vid läsning och skrivning betraktas som en sorts dataströmmar från eller till datamediet. Direktaccess innebär att mindre poster på valfri plats i filen kan läsas eller skrivas oberoende av position, jmf med en typisk databas.

Data som kontinuerligt genereras från IoT som ”läser av” sin omgivning (sensorer) går dock inte ”greppa” på samma sätt eftersom den till sin natur inte är lagrad utan genereras kontinuerligt med tiden.

På engelska talar man i det första fallet ofta om ”batch processing” och i det senare fallet om ”stream processing”. I det här kapitlet beskrivs närmare hur man praktiskt kan arbeta med det senare: strömmar av data som måste läsas av och analyseras i realtid. Beskrivningen bygger i viss utsträckning på erfarenheter som vunnits i tidigare projekt kring strömmande data (mera specifikt AIS-data från stora mängder fartyg[34]), referenser (Johnsen, Bloebaum, Brannsten, & Lund, 2018), (Johnsen, o.a., 2018) samt studium av webbaserad dokumentation för mjukvaror för ”Stream processing”, främst angiven i fotnötter.

3.1 Kort om produktion av strömmande data

En generalisering ger vid handen att strömmande data är sådan som på ett visst format kontinuerlig, i något transmissionsmedium (”etern”, akustik, kabel, fiber, m.m.) skickas ut till de som vill läsa av strömmen, eller till en viss/vissa mottagare som ”prenumererar” på dessa data. Typiskt är (först analogt, senare digitalt) TV och radio. Militären har länge nyttjat elektroniskt strömmande data för situationsuppfattning och uppdragsstyrning såsom radar, bildöverföring och olika former av

[34] https://cordis.europa.eu/project/rcn/94732/factsheet/en, besökt december 2019

datalänkar. Dessa har ofta arbetat med proprietära protokoll, nationellt eller beroende på leverantör. Standardiseringsarbete har dock pågått länge, i synnerhet inom Nato för vilket det tidigt var nödvändigt att kunna utbyta information inom hela koalitionen.

Den ursprungliga IoT-tanken var att olika fysiska IoT-noder (omnämns nedan ”enheter”), såsom sensorer (eng. *sensors*) och ställdon (eng. *actuators*) ute i den fysiska miljön (”at the Edge”) skulle göra sig tillgängliga över Internet via en URL.[35] Sedan skulle intern statusdata och mätt sensordata kunna efterfrågas från dem via denna URL, eller ge kontrollkommandon till dem så att de utifrån dessa kunde justera sig själva eller påverka sin omgivning (i fallet ställdon). Detta innebär då en ren ”stuprörsarkitektur”. Analysen av insamlad rådata avsågs ske högre upp, potentiellt i ”molnet” (”Cloud processing”), vilket i praktiken kan vara någon server/klusterhall var som helst i världen, eller åtminstone i utpekade servrar på större avstånd från enheterna, och kontrollkommandon kan skickas tillbaks.

Med mer intelligenta enheter som idag förekommer kan mer av styrning och sensordatabehandling ske i dem själva, eller i närbelägna gateways[36] och även beslut om vad som skall göras med analysresultatet. Enheter kan även samverka med varandra direkt, såsom att en enhet med en sensor direkt visar in en annan mot något intressant fenomen att observera. Dataanalysen i sig kan helt eller delvis ske i eller åtminstone närmare enheterna och ”marken” där de befinner sig (”Fog processing” (Johnsen, o.a., 2018), jmf. ”Edge Computing”), vilket kraftigt kan snabba upp IoT systemets sammantagna ”perception” av sin omgivning. Detta är speciellt viktigt om enheterna producerar strömmande data i hög takt vilken annars obehandlad, ev. efter viss ensning av dataformat, i en stuprörsanalogi skickas vidare upp för analys till centrala noder som riskerar att bli överbelastade. Även om kraftfulla servrar eller kluster skulle kunna hantera denna datatakt är risken ännu större att ofördelaktiga, ofta trådlösa, kommunikationslänkar nära enheterna har alltför låg bandbredd eller batterikapacitet för rådataströmmar eller ibland helt fallerar med oacceptabla dataförluster och fördröjningar som resultat.

[35] Uniform Resource Locator - den teckensträng som identifierar en viss resurs på nätet. Se https://sv.wikipedia.org/wiki/Uniform_Resource_Locator, besökt 2019-12-08

[36] ”Mellannoder” som är uppkopplade mot en eller flera enheter och som kan vara en protokollsport mot Internet för dessa. I kommunikationen med gateway:en kan enheterna vid behov nyttja andra specialanpassade protokoll än de som förekommer på Internet. I gateway:en kan även viss ytterligare ”Fog processing” göras, i synnerhet om den kan ha bättre energiförsörjning än enheterna själva.

Teknologier finns för mera avancerade enheter att ha viss Artificiell Intelligens såsom bild- (t.ex. Deep Learning) och ljudigenkänning och endast behöva sända någon form av identitetsbeteckning på det observerade fenomenet som sin utström. Här tillkommer även möjligheten att en enhet / samling av enheter endast skickar data då en viss händelse iakttagits, se resonemanget kring CEP nedan. Enheterna kan även publicera sina data på flera strömmar med olika ämnen, ”topics”, beroende på vad för fenomen de tror sig ha observerat, och sedan prenumererar mottagarna endast på vissa utvalda ämnen för att få den för dem mest relevanta informationen. Att reducera utströmmen till förädlad data av mindre volym är även fördelaktigt ur ett energiperspektiv; batteriresurser sätter hårda gränser på energiåtgång. Å andra sidan kräver avancerad lokal dataanalys också energi, så här måste en avvägning göras.

Ju mer avancerade sådana här enheter är ju mer tillkommer dock en växande säkerhetsproblematik såsom att en fiende kanske lätt kan tillgripa en enhet och genom ”reverse engineering” försöka finna ut hur igenkänningsfunktionen i den fungerar, vilka algoritmer som används etc och använda denna kunskap mot oss.

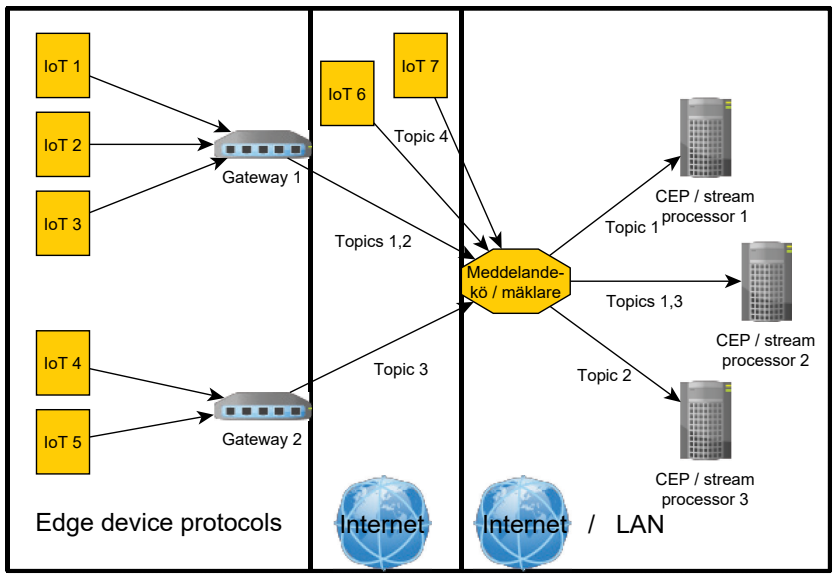
Militära tillämpningar av sådana här systemkoncept är förstås mångfaldiga: Soldatmonitorering, logistikhantering, IoT i fordon (autonoma, fjärrstyrda, förarstyrda), IoT som placeras ut på fasta platser för övervakning, eventuellt i kluster i ett område, etc. Det går potentiellt även att nyttja redan befintlig IoT infrastruktur på platsen för insatsen (mer och mer militär verksamhet är urbant orienterad, och där finns även flest IoT-system). Bästa sättet att erhålla information från dessa, och skicka till dem, varierar dock. Ofta kan ett prenumerationsförfarande på utvalda dataströmmar vara det bästa.

Vi tänker oss nu att vi har en generisk arkitektur som, med ursprung i ett potentiellt stort antal enheter (t.ex. sensorer), i en viss topologi via nödvändiga gateways, gör sina data såsom RGB[37]bilder (byteström), JSON[38]meddelanden (textström) etc. tillgängliga som strömmar enligt

[37] Rött-Grönt-Blått; varje bildpixel kodar sina nyanser av rött, grönt och blått i varsin databyte. En bild på 256x256 pixlar ger då en ström på 256*256*3 = 196608 bytes. I praktiken används dock någon form av bildkompressionsalgoritm för att minska datavolymen. Hos mottagaren måste då data packas upp igen.

[38] JavaScript Object Notation – en vanligt förekommande komprimerad textnotation för att beskriva ”Properties” och Property Values” vilket kan nyttjas för att utbyta data, exempelvis sensormätresultat och styrkommandon. Se https://sv.wikipedia.org/wiki/JSON.

lämpligt protokoll på Internet. Teknologier finns, såsom Apache Camel[39], för att routa strömmande data, eventuellt konverterat till lämpligt format, till berörda mottagare. Väl genomförda analyser som nyligen gjorts, med för- och nackdelar hos olika arkitekturer finns i (Johnsen, Bloebaum, Brannsten, & Lund, 2018). En användare vill nu få hjälp att nyttja dessa strömmar, matchat mot sina behov. Typiskt sker det genom ett ”push” (subscribe / publish), eller genom ett ”pull” (request / response) förfarande på olika ämnen som strömmarna logiskt gör sig tillgängliga via någon form av ”meddelandemäklare” såsom exempelvis Apache Kafka.[40] Om källor begär ”pull” för att lämna från sig data kan en prenumerationsliknande ström ändå upprättas genom att en process med viss frekvens gör pull och då får svar som sänds vidare till användaren, vilken då kan uppfatta sekvensen av svar som en meddelandeström. En generisk arkitektur visas i Figur 2.



Figur 2. En generisk arkitektur för strömmande data fördelade på olika Topics. Gränserna ovan kan flyttas beroende på arkitektur och valda protokoll, de olika streamprocessorerna kan ligga i samma fysiska server, separerade på Internet eller i ett LAN eller samsas i ett kluster. Routningen av IoT-data kan även gå direkt från vissa Gateways till utsedda mottagarnoder / streamprocessorer utan att gå via mäklare.

[39] Se https://camel.apache.org/

[40] Se https://kafka.apache.org/

3.2 Hantering av strömmande data – Händelsestyrd dataanalys

Complex Event Processing (CEP) (Wikipedia, 2019) är en idag tämligen mogen analysmetodik som handlar om att utifrån ett antal enkla, ”atomära” händelser som iakttagits, i viss temporal sekvens, konstatera att ett visst händelsemönster (complex event) uppfyllts efter en viss tid, och då aviserar förekomsten av denna *komplexa händelse* för vidare analys och eventuell åtgärd. Wikipedia (2019) listar även åtskilliga produkter som är mer eller mindre anpassade åt olika tillämpningsområden för strömmande data. Dessa varierar starkt och kan exempelvis utgöras av:

- Att detektera vibrationer i maskiner för att ge reglerande feedback om vissa skadliga vibrationsmönster framträder
- Att följa varierande börskurser för att snabbt ta ett investeringsbeslut
- Att följa trafiken från ett antal vägkameror på en eller flera vägar, räkna fordon av olika typer i olika vägsegment och förutsäga när och var trafikstockningar kan komma att ske

I de två första fallen ovan handlar det ofta om CEP på millisekund till sekundupplösning, medan i det tredje fallet, samt troligen i de flesta militära fall med IoT, är de meningsfulla tidsspannen ofta betydligt längre såsom minuter eller mer.

Välutvecklade API:er finns för att koppla samman strömmande källor, via meddelandemäklare, CEP system (såsom Esper, Spark och Flink bland många andra[41]), och databassystem för analysresultat och visualiseringsgränssnitt. Den ännu något snåriga förekomsten av IoT arkitekturer och dataformat kan göra vissa trösklar högre vad gäller val av systemlösning nära datakällorna.

En mer trivial strömanalys, i detta fall nära enheten, skulle kunna utgöras av att sampla en termometer en gång per sekund och skicka ut data på strömmen endast då temperaturen överskrider 40 °C. Om detta skett väntar enheten en minut med att sampla igen för att undvika att ”ropa” för mycket. Efter denna minut, om temperaturen sjunkit under 40 °C återgår den till sekundsampling, annars ropar den igen och väntar en minut till etc. Redan på denna nivå går alltså en ”logik” att formulera för hur mätdata skall behandlas och rapporteras på utströmmen.

[41] Se www.espertech.com, spark.apache.org, flink.apache.org.

En grundläggande idé med mer icke-trivial analys över strömmande data för att reducera datamängden som skall analyseras, samt även resultatmängden, till hanterbara nivåer är annars att ha ett tidsfönster med fixt tidsspann bakåt från och med en specifik starttid inom vilket analysen försiggår. Data som ligger bakom fönstret glöms, de är ”out of date”, vare sig de tidigare resulterat i att skapa komplexa händelser eller inte. Flera varianter finns, såsom:

- ”Micro Batch Streaming” eller ”Tumbling window”, där fönstret flyttas fram stegvis med samma tidsintervall som fönstrets vidd och då processar de data (en micro batch) som finns i fönstret.

- ”Sliding window” som innebär att flytta fram fönstret med andra steg än dess vidd:

    - Kortare steg än dess vidd varvid överlapp fås, och de nya data som eventuellt kommit in i fönstrets ”front” processas tillsammans med de gamla data som finns kvar i fönstret före dessa.

    - Längre steg än dess vidd och så att säga ta periodvisa ”samplingar” med viss vidd av dataströmmen, men efterföljande analys missar då förstås de data som hamnar mellan fönsterlägena.

- ”Session window”, där fönstrets tidsvidd inte är konstant utan definieras av grupper, ”sessions”, av data som kommer in och där varje grupp åtskiljs med minst ett visst ”tysthetsintervall” då ingen data inkommit.

- ”Continuous Streaming”, där fönstret flyttas fram för varje datum som kommit in vilket ger steglängd motsvarande den momentana tidsluckan mellan två data, som kan variera beroende på datakälla. Detta är den form av tidsupplösning som snabbast reagerar på upptäckta mönster, men också den som kräver störst datorkraft vid hög datatakt.

Exempel på olika fönstervarianter visas i Figur 3.

Figur 3. Tre olika varianter av tidsintervallsfönster inom vilket data samprocessas för att hitta mönster. *Överst:* ”Tumbling window” som flyttas fram med fönstrets vidd. Varje datum med samma färg tillhör samma fönster. *Mitten*: ”Sliding window”; här varianten där fönstret flyttas fram med kortare intervall än fönstrets vidd vilket ger överlapp. De första blå data hamnar i fönster 1, de röda i 1, 2, de gula i 2, de ljusgröna i 2,3 osv. *Nederst:* ”Session window” där inkomna data grupperas inom fönster med vidder som bestäms av tidsomfånget hos datagrupper mellan vilka ”tysta intervall” är längre än ett visst intervall. Första och sista datat i en grupp bestämmer dess fönsters vidd. För ”Topic 1” är tidsskillnaden mellan data i de två brandgula paren precis inom acceptabel vidd för att inte tvinga fram en ny session. För ”Topic 2” överskrider dock tidsskillnaden mellan det gröna paret data gränsen, så de delas mellan slut och start på två konsekutiva sessionsfönster.

En speciell frågeställning här är hanteringen av ”negativ information”, dvs. en frågeställning där en komplex händelse skall genereras då något specifikt eller förväntat mönster *inte* upptäckts. Två händelser av en viss typ kan t.ex. inträffa mindre än ett visst tidsintervall från varandra, utan att följas av en, förväntad eller oförväntad, tredje händelse, av samma eller annan typ, högst en viss tid efter den andra händelsen. En komplex ”icke-händelse” skall då typiskt genereras då den tredje hypotetiska händelsen senast skulle ha kunnat uppfylla mönstret (men inte gjorde det). Detta innebär att CEP-mjukvaran inte kan ligga latent mellan händelser och endast analysera läget i fönstret då en ny händelse inträffar,

utan kan även avvakta ”timeout” för en potentiell kommande ickehändelse.

Olika CEP-mjukvaror tillhandahåller olika avancerade regler till att skapa tidsfönster och att flytta dem framåt. Den kan även ha flera fönster aktiva samtidigt på samma dataström för att hantera olika typer, eller ämnen, av data från en heterogen ström (om denna inte enklast kan hanteras som flera homogena strömmar efter ämne med var sina tidsfönster).

Begreppet ”data” är förstås mycket varierat beroende på hur avancerad förbehandling som finns i kedjan av enheter, gateways eller andra mellanprocessningssteg innan CEP-analysen. Det kan handla om en monofrekvent ström av temperaturmätningar (flyttal) från en enkel temperatursensor till identifierade personer eller objekt i en videoström (eller en akustisk ström), där endast person/objektID samt inmätt position/riktning skickas vidare till CEP från en avancerad videokamera med bildigenkänningsfunktionalitet eller en akustisk sensor med röst/ljudprofilsigenkänning. I CEP-funktionen kan då exempelvis finnas förmåga att leta efter ett visst beteendemönster, eventuellt genom matchad data från ett flertal närbelägna videokameror / akustiska sensorer över ett längre tidsintervall.

Ytterligare en viktig komponent i CEP är förmågan att skapa nya strömmar bestående av de redan identifierade komplexa händelserna. Dessa kan analyseras på högre abstraktionsnivå för att hitta mer komplexa mönster, såsom att flera personer eller objekt parallellt eller efter varandra följer vissa beteenden. Detta är ett viktigt sätt för att effektivt kunna nyttja datorkraft för att sammanställa stora volymer från åtskilliga strömmande datakällor till en lägescentral som prenumererar på olika komplexa mönster för att då de sker ta ställning kring åtgärd.

Det är även viktigt att ursprungsdata från IoT stämplas med den tidpunkt då de mättes, ”Event Time”, snarare än när datat tas emot vid olika steg i meddelandekedjan, och till slut når någon plats där bearbetning sker, ”Processing Time”. Det kan ta tid innan mätt data når CEP-mjukvaran, och data kan även komma i fel tidsordning. Detta gäller i synnerhet om strömmar från flera källor nyttjas där fördröjningen är av varierande storlek och kanske kraftigt varierande i tid p.g.a. ofördelaktiga transmissionsförhållanden och bandbredd. CEP-mjukvaror brukar ha funktionalitet för att hantera out-of-order data förekomst i strömmar, även om man förstås inte kan vänta hur länge som helst på en potentiellt viktig, men saknad mätning som kan ha kommit för sent, och att data har rätt tidsstämpel är då förstås avgörande för att kunna hitta mönster som baseras på temporal ordning.

Att formulera dessa eftersökta mönster görs ofta i något specifikt språk, specifikt för varje CEP-mjukvara. Dessa språk, Event Query Languages (EQL), brukar vara snarlika Structured Query Language (SQL), med databasliknande frågor på de data som finns i tidsfönster, utökat med omfattande temporala operatorer på datas tidsordning och –stämpel. En sådan ”fråga” utförs på data i omnämnda tidsfönstret varje gång det flyttats framåt, enligt någon av de varianter som nämndes ovan, på de data det överlappar.

En analogi mellan enkla och multipla dataströmmar och CEP på dessa kan slutligen göras gentemot s.k. informationsfusion, vilket handlar om sammanställning av information från olika källor baserat på vissa mönster, ofta temporala, spatiala och/eller kategoriska (dvs typinformation), i informationen (se även avsnitt 4.5). Det kan exempelvis handla om att ha identifierat ett visst rörligt objekt i en videosekvens från en videokamera och därför förvänta sig att se samma objekt i en närliggande kamera inom en viss tid.

Informationsfusion bygger mycket på sannolikhetsteori och innefattar antaganden om att osäkerheter finns hos de datakällor som används. Detta innebär att resulterande osäkerheter i det fusionerade resultatet måste kunna kvantifieras. CEP är dock mera ”strikt”, dvs. antingen har en händelse hänt eller inte vilket kan bli avgörande för om en komplex händelse, där den ingående händelsen är av avgörande betydelse för den komplexa händelsens mönsteruppfyllande, har hänt eller inte. Detta kan hanteras genom att, parallellt med att leta efter huvudmönstret, även leta efter snarlika mönster. En sådan metodik motsvarar så kallat multihypotesresonemang i informationsfusion. Det kan dock leda till att ett snabbt växande antal hypoteser om komplexa händelser som kan vara under utveckling måste hanteras vilket kräver stor datorkraft och förmåga att snabbt ”rensa” CEP-processens minne från hypoteser som inte verkar uppfyllas. Detta måste även ställas i relation till CEP-mjukvarans förmåga att hantera ovan nämnda out-of-order data.

3.3 Slutsatser

Analys av strömmande data (eng. *stream processing*) förutsätter delvis helt andra analysmetoder än analys av förlagrad data. Tidsaspekten är ofta mycket viktig och förmågan att i realtid upptäcka eftersökta temporala mönster i dataströmmarna undan för undan som mönstren utkristalliseras kan vara det viktigaste i analysen, för att snabbt kunna vidta lämplig åtgärd vid upptäckten. Det kan handla om stora datavolymer per tidsenhet, och även om viss dataanalys och –reduktion kan göras tidigare

i insamlingskedjan, eventuellt redan i IoT-sensorerna, så krävs speciell mjukvara för realtidsigenkänning av dessa mönster.

4 Informationsbearbetnings-metoder

I kapitel 3 behandlade vi specifikt fenomenet strömmande data. I det här kapitlet tittar vi dels vidare på olika metoder för att bearbeta innehållet i dataströmmarna,[42] men även metoder för att hantera IoT-systemen.

4.1 Översikt

De uppkopplade IoT-enheterna kommer framöver att samla en enorm mängd data via sina sensorer och användarnas interaktioner. Detta kommer att påverka internet, berika dess innehåll och skapa helt nya tjänster. Med fler anslutna enheter kommer mer användbar data men detta utgör också en ny utmaning för hur all data ska analyseras. Det är här *artificiell intelligens*[43] (AI) kommer in; att utnyttja den enorma tillgången till data för att skapa en tillförlitlig lägesbild och tillhandahålla nya tjänster som kommer till andra IoT-enheters användning.

Det är helt enkelt omöjligt för människor att granska och förstå all denna information med traditionella metoder. Även om samplingsstorleken minskas finns inte tillräcklig tid för beräkningar. Det stora problemet är att hitta sätt att analysera flödet av data och information som alla dessa IoT-enheter skapar. Att hitta insikter i terabyte av data är en verklig utmaning. För att vi ska skörda de fulla fördelarna med IoT måste vi förbättra både hastigheten och noggrannheten på analys av *big data.*[44] Det bästa sättet att ta itu med denna IoT-genererade information är att använda AI som den yttersta möjliggöraren för IoT. (Banafa, 2016)

Detta kapitel presenterar en överblick av hur AI är relaterat till och används inom IoT. De flesta tekniker, metoder och applikationer som diskuteras i detta kapitel är hämtade från vetenskapliga artiklar inom IoT och finns redan åtminstone på experiment- eller prototypsnivå. Som nämnts tidigare är IoT inte bara uppkopplingen av olika saker till internet, utan snarare sammankopplingen av alla saker via internet. Om detta (även

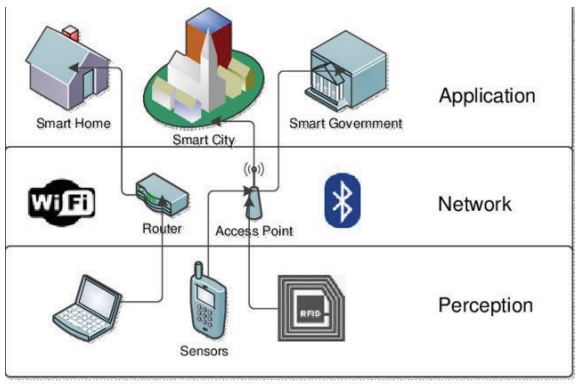
[42] Utöver CEP som vi diskuterar i avsnitt 3.2.

[43] Vi använder genomgående den övergripande termen AI även om i många fall kan den ersättas med de mer specifika begreppen maskininlärning och djupinlärning. Med AI menar vi här ett systems förmåga att lära sig av data som kommer från externa system eller är producerade genom interaktion med omgivningen och att använda inlärningen för att uppnå något mål.

[44] https://sv.wikipedia.org/wiki/Big_data

endast delvis) förverkligas, kommer det att finnas en enorm mängd data från olika resurser tillgängliga, vilket öppnar för en intensiv användning av AI på olika områden som inte går att föreställa sig idag. Då kommer antagligen IoT-nätverket att nå en grad av lägesbild som gör att många nya applikationer och enheter som nu inte är tänkbara kan förverkligas.

IoT-system kan delas in i tre konceptuella nivåer: i) perceptionsnivå, ii) nätverksnivå, och iii) applikationsnivå (se Figur 4).



Figur 4: Konceptuella nivåer i IoT-system

Vi delar också in AI i tre kategorier beroende på den nivå som metoden mest kommer att bidra till trots att indelningen inte helt stämmer överens med de tre olika nivåerna[45]: i) AI som stöd för hantering av IoT-sensorer och enheter, dvs. resursallokering och optimering av enheter, ii) AI som stödjer datatransport, kryptering, säkerhet och personlig integritet, och iii) AI-metoder för att behandla IoT data. Även om det sistnämnda inte är till synes specifikt för IoT och IoT kan använda sig av allmänna AI-metoder inom andra områden, finns det ändå vissa egenskaper hos IoT-enheter som skiljer de från andra system. Deras begränsade beräkningskraft och batteriresurser gör det intressant att studera AI i ett IoT-sammanhang.

Dessa tre kategorier diskuteras mer i detalj i följande avsnitt.

[45] Trots att det kan finnas AI-metoder som stödjer säkerhet på alla tre nivåer har vi samlat AI till stöd för säkerhet på nivå 2.

4.2 AI för hantering av IoT-enheter

AI kan användas för att organisera och optimera IoT-sensorer och enheter. Dessa uppgifter inkluderar men är inte begränsade till resursallokering, energihantering och schemaläggning. Nedan ges en beskrivning av varje tillämpning.

4.2.1 Ström och batterihantering

Inbäddade IoT-enheter har olika parametrar som kan justeras i realtid för att öka deras effektivitet och minska energiförbrukningen. AI-metoder kan användas för att bestämma effektiv parametersättning av sensorer, processorer och kommunikationsenheter.

Trådlösa sensornätverk för övervakning består av sensornoder som rapporterar temperatur, relativ fuktighet och andra miljöparametrar. Tiden mellan två på varandra följande mätningar är en kritisk parameter som kan påverka livslängden på sensornätverket och kvaliteten på de rapporterade data. Eftersom det finns en stor variation mellan olika scenarier är det utmanande att identifiera ett samplingsintervall som lämpar sig för alla möjliga fall. Dias, Nurchis, & Bellalt (2016) föreslår en AI-metod (*förstärkt inlärning*[46]) för att dynamiskt ställa in sensorernas samplingsintervall till ett optimalt värde så att varken relevant data förloras eller för många datapunkter samplas. Användningen av metoden innebär att den genomsnittliga kvaliteten av information som levereras behålls samtidigt som energi sparas.

Energisnåla *systems-on-chip* (SoC), dvs. integrerade systemkretsar har blivit huvudkomponenten i många framväxande tekniker särskilt inom IoT-domänen. För SoC:ar varierar den optimala arbetspunkten för maximal energieffektivitet beroende på temperatur, arbetsbelastning och andra parametrar för olika SoC-komponenter vid drift. Golanbari & Tahoori (2018) presenterar en AI-metod för att förutsäga och ställa in SoC till den mest energieffektiva inmatningsspänningen under körning, med tanke på effekterna av temperaturvariation av SoC-komponenter samtidigt som prestanda och tillförlitlighetskraven uppfylls.

I ett liknande arbete använder Golanbari o.a. (2017) en AI-metod för att hitta den optimala strömförsörjningsspänningen för chips för att förbättra energieffektiviteten för IoT-enheter med låg effekt vid körning.

[46] Förstärkt inlärning är en AI-metod där en agent lär sig genom interaktion med omgivningen och utifrån belöning som den får för sina handlingar.

Narrowband Internet of Things[47] (NB-IoT) är en radioteknologi-standard för låg energiförbrukning och bred täckning för ett brett utbud av mobila enheter och tjänster. Att öka antalet upprepningar av överföring anses som en lovande metod för att förbättra täckningen i NB-IoT. Ett stort antal repetitioner minskar dock systemets genomströmning och ökar energiförbrukningen för IoT-enheterna, vilket minskar enheternas batterilivslängd och ökar deras underhållskostnader. Chafiio o.a. (2018) föreslår en ny AI-metod för att förbättra NB-IoT-täckningen. I stället för att slumpmässigt välja tillgängliga kanaler för att upprätta anslutning till en nod, föreslår de i detta arbete en metod för att dynamiskt lära sig att välja bland de kanaler som är mest sannolikt tillgängliga och har gynnsamma täckningsförhållanden, vilket förlänger batterilivslängden på enheterna.

Solenergi är en viktig komponent i många IoT-scenarier där vissa resursbegränsade enheter är beroende av solenergi för att fungera utan försämrad prestanda. Att förutsäga solenergin är då nödvändigt för en effektiv hantering och utnyttjande av resurser. I likhet med AI-metoder som används för att förutsäga solenergin för större kraftverk, undersöker Kraemer o.a. (2017) möjligheten att använda AI för resursbegränsade sensorer baserad på lättillgänglig offentliga väderdata. Den genomförda utvärderingen tillämpad på kommersiell IoT-hårdvara i ett verkligt scenario visar genomförbarheten av lösningen och att det är möjligt att även med en begränsad tillgång till data förbättra systemet gradvis under körning.

4.2.2 Resursallokering/schemaläggning

Resurshantering och allokeringsproblem formuleras lämpligast som optimeringsproblem. I många fall är det inte möjligt att lösa dessa problem inom rimliga tidsgränser. Däremot finns det oftast approximativa AI-metoder som är skalbara och kan hitta en nära optimal lösning även om de inte kan garantera den exakta och optimala lösningen. Ett exempel på användningen av AI för resursallokering inom IoT-system är att avgöra om data ska bearbetas lokalt eller skickas till en molnserver. (Samie, Bauer, & Henkel, 2019)

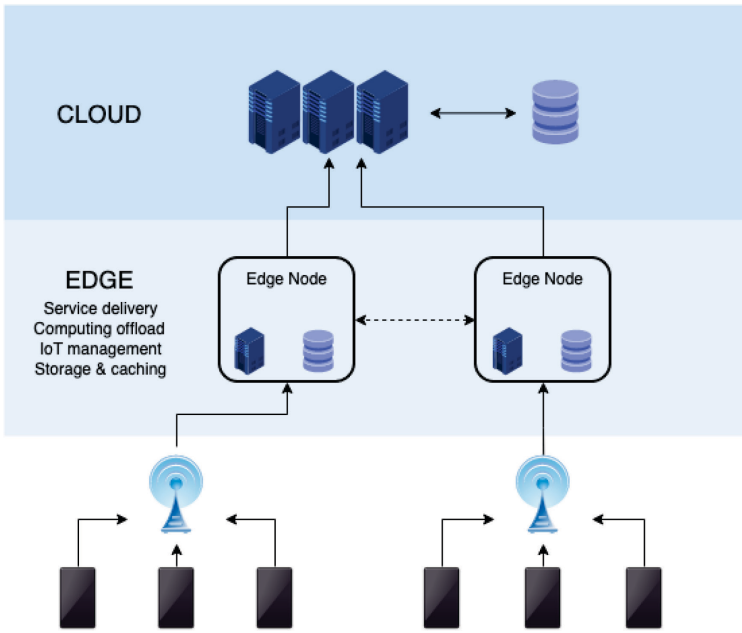
Prestanda av sådana system bestäms huvudsakligen av de ingående fysiska maskinernas sammansättning, deras konfiguration,

[47] NB-IoT används för kommunikation inom *low-power wide-area network* (LPWAN) som är en typ av trådlöst nätverk utformat för att tillåta kommunikation med lång räckvidd och låg överföringskapacitet bland anslutna objekt, t.ex. batteridrivna sensorer.

resursallokering och schemaläggning av jobb och uppgifter. Orhean, Pop, & Raicu (2018) föreslår en AI- metod (förstärkt inlärning) för att lösa schemaläggningsproblemet i distribuerade system. Metoden tar hänsyn till nodernas heterogenitet, deras placering i nätet och uppställningen av uppgifter och slutligen bestämmer en schemaläggningspolicy med en bättre exekveringstid. Författarna föreslår också ett ramverk för implementering av metoden som erbjuder schemaläggning som en tjänst till distribuerade system.

IoT-enheter samlar som sagt in en stor mängd data från omgivningen för att möjliggöra extraktion av användbar information, men det är inte självklart hur de olika IoT-enheterna och det heterogena IoT-systemet ska utföra databehandlingen. Cui, Kim, & Rosing (2017) föreslår ett ramverk som använder olika AI-metoder för big data och tar hänsyn till energi- och prestandakrav för databehandlingen över heterogena enheter. Modellerna även tar hänsyn till kommunikationskostnader och ökad efterfrågan på databearbetning. Det föreslagna ramverket avgör om databearbetningen ska utföras på *edge-enheten*[48] eller på molnservern. Edge-enheter löser ett grundläggande problem förknippat med molnarkitektur. Medan molnen är kraftfulla för lagring och bearbetning av data skapar de förseningar för IoT-enheter som skickar data fram och tillbaka. Genom att flytta beräkningsfunktionerna från molnen till lokala edge-enheter minskas kommunikationsfördröjningar och förseningar undviks (Figur 5).

[48] Edge-enheter är de enheter som sammankopplar IoT-enheterna till molntjänster. Flera leverantörer erbjuder IoT edge-teknologier och -enheter som varierar i tjänster och kapacitet.



Figur 5: IoT-enheter är kopplade via edge-enheter till molnet.[49]

DARPA[50] har organiserad en tävling SC2[51] med målet att använda AI för att hitta den bästa lösningen för en kollaborativ spektrumtilldelning till olika tjänster.

Den rådande metoden att tilldela radiospektrumet till olika intressenter, genom att dela upp det i ömsesidigt exklusiva områden, är inte det mest effektiva sättet. Visserligen garanterar denna process att tjänsterna inte stör varandra, men det är sällan alla tilldelade frekvenser används hela tiden och på sätt är resursen underutnyttjad. Detta tillvägagångssätt blir ohållbart då efterfrågan på spektrum ständigt växer.

För att ta itu med denna utmaning utlyste DARPA en tävling för att utforma en ny typ av kommunikationsenhet som inte sänder helt tiden på

[49] NoMore201, (https://commons.wikimedia.org/wiki/File:Edge_computing_infrastructure.png), https://creativecommons.org/licenses/by-sa/4.0/legalcode

[50] Defense Advanced Research Projects Agency (DARPA) är en amerikansk federal myndighet (under USA:s försvarsdepartement) som finansierar och bedriver forskning och tillämpad forskning för militära ändamål (https://www.darpa.mil/).

[51] Spectrum Collaboration Challenge (SC2) är en tävling som påbörjades 2016 och hade sin final den 23 oktober 2019 (https://www.spectrumcollaborationchallenge.com/).

samma frekvens, utan ett radiosystem där enheterna skickar på de frekvenser som är omedelbart tillgängliga. Idén var att ett AI används för att spektrumet utnyttjas optimalt, dvs. istället för att det distribueras permanent mellan enskilda, exklusiva ägare, tilldelas dynamiskt och automatiskt i realtid mellan olika enheter.

Över 30 lag deltog i utmaningen och tävlade under tre år med allt svårare utmaningar. Den slutliga uppgiften var att integrera AI så att radiosystemen som delar information med varandra och är samarbetsvilliga automatiskt kan styra tilldelningen av spektrumet dynamiskt och i realtid samtidigt som de är kapabla att ta hänsyn till prioritering av olika typer av trådlös trafik, tillförlighet av tjänster och överbelastade situationer. De 10 finalisterna som deltog i den sista avgörande tävlingen lyckades alla utklassa den existerande radiofrekvenstilldelningen. I slutet av tävlingen tog ett team från *University of Florida*[52] hem det stora priset på 2 miljoner dollar.[53]

Trots de lovande resultaten på en simulator är tillverkningen av antenner för IoT-enheter som har tillräckligt bra effekt vid flera olika frekvenser inte en trivial uppgift.[54] Det är viktigt att förstå att resultaten av DARPA:s stora utmaningar inte kan överföras direkt till industrin. Snarare är utmaningarna utformade för att avgöra om en grundläggande förändring är möjlig. Utifrån DARPA:s Grand Challenge för autonoma fordon 2004[55] tog det ytterligare ett decennium innan den autonoma tekniken började användas, dock på en mycket begränsad nivå, i kommersiella bilar.[56]

[52] http://innovate.research.ufl.edu/2019/10/24/gatorwings-wins-darpa-spectrum-collaboration-challenge/, besökt 2019-12-12

[53] https://www.technologyreview.com/s/614627/5g-ai-darpa-next-generation-of-wireless-devices/, besökt 2019-12-12

[54] Hamed Jahja, RF Filter Engineer, ACE Technologies Corp., intervju den 29 oktober 2019

[55] https://en.wikipedia.org/wiki/DARPA_Grand_Challenge#2004_Grand_Challenge

[56] https://spectrum.ieee.org/telecom/wireless/if-darpa-has-its-way-ai-will-rule-the-wireless-spectrum, besökt 2019-12-12

4.3 AI som stödjer säkerhet och personlig integritet

Trots likheter med andra informationssystem är säkerhets- och integritetsutmaningarna hos IoT-system mer omfattande, komplexa, och utmanande, på grund av följande skäl:

1. IoT-enheter finns överallt och en angripare kan använda den ökade fysiska tillgängligheten till enheter för att hitta fler sårbarheter i IoT-system.
2. IoT-enheter är vanligtvis batteridrivna, har i allmänhet lägre beräkningskraft och minne, och brukar inte vara kapabla att genomföra lämpliga säkerhet- och anonymiseringstjänster vilka kräver beräkningskraft och minnesresurser.
3. Antalet anslutna enheter ökar och därmed ökar mängden insamlad och ackumulerad information om oss individer i olika databaser kontinuerligt (även om känslig information kan tas bort eller skyddas av anonymisering när informationen sprids). En oförutsägbar kombination av till synes okänsliga data från olika källor kan skapa en unik identifierare som resulterar i sekretessbrott.
4. IoT-nätverket har en dynamisk struktur, enheterna kan ansluta sig och lämna nätet närsomhelst. I samband med mångfald av system och kommunikationsprotokoll gör detta de traditionella informationssäkerhetsåtgärderna otillräckliga. (Kamrani, Wedlin, & Rodhe, 2016)

På grund av den potentiellt genomträngande närvaron av IoT-enheter i människors liv är säkerhet och personlig integritet en av konsumenternas stora angelägenheter. För att förbättra användarnas integritet och säkerställa säkerheten kan AI-tekniker spela en viktig roll. Insatserna kan delas in i två kategorier: i) upptäcka och ii) förhindra. (Samie, Bauer, & Henkel, 2019)

Lee o.a. (2017) bygger en AI-baserad modell för *avvikande beteende profilering* (eng. *abnormal behavior profiling*) för IoT-enheter. Det föreslagna systemet integrerar olika typer av avvikelsedetektering i smarta byggnader som är utrustade med sensorer med hög beräkningskraft. Det föreslagna systemet föreslås för att hantera scenarier där en angripare ändrar en aspekt av data från hela datauppsättningen (t.ex. temperaturen) för specifika sensorer för att vilseleda ställdon, t.ex. kyl- eller värmesystem och brandsläckningssystem för att orsaka skada.

För att skydda IoT-enheter mot intrång, attacker och skadliga aktiviteter och bevara datasäkerhet och användarnas personliga integritet utvecklar Zhao o.a. (2017) ett AI-baserat intrångsdetekteringssystem som är anpassat till egenskaperna hos IoT-system som kräver övervakning i realtid. De experiment som författarna utför visar att systemet lämpar sig för att upptäcka intrång i IoT-system med avseende på beräkningskomplexitet och tidsprestanda.

Tillämpning av IoT förbättrar effektivt kvaliteten på bevakning och kontroll av smarta elnät. Beroende av tekniken ökar dock också sårbarhet för skadliga attacker, t.ex. *false data injection attacks*.[57] Wei & Mendis (2016) föreslår ett protokoll för att identifiera och mildra problemet för övervakningssystem inom smarta elnät genom att i realtid använda korrelationen mellan olika mätdata och utvärdera tillförlitligheten hos kritisk data.

Många leverantörer av IoT-moln integrerar både smartphones och industriella IoT-nätverk. Integration av mobila enheter med IIoT-nätverk[58] utsätter emellertid IoT-enheterna för betydande hot mot skadlig kod. Mobil skadlig kod är det största hotet mot säkerheten för IoT-data, användarnas personliga information och företagens finansiella information. Sharmeen o.a. (2018) analyserar olika tekniker för detektion av skadlig programvara riktade mot enheter i IIoT- och mobilnätverk.

Nyligen har angripare initierat alltmer samordnade attacker mot IoT-system som vanligen är relaterade till botnät.[59] Att effektivt upptäcka botnät baserat på angreppaktiviteter har visat sig vara en utmanande uppgift. Sun o.a. (2019) föreslår en AI- metod för att modellera angriparaktiviteter baserat på den intuitiva observationen att attackerare i samma botnät brukar starta attacker vid ungefär samma tidpunkt. Modellen används sedan för att genomföra klusteranalys[60] och automatiskt identifiera botnät. Detta kan användas som ett verktyg av nätverksadministratörer för att skydda nätet..

---

[57] False Data Injection Attacks (FDIA) betraktas som en viktig klass av cyberattacker mot ICS (Industrial Control Systems). FDIA injicerar falsk mätning i styrsystemet i hopp om att missleda styralgoritmen. Detta hos en enda kontrollenhet eller ett sensorvärde i en anläggning kan leda till en enorm förlust för företaget eller en katastrof i anläggningsmiljön.

[58] Industrial IoT (IIoT), se även avsnitt 4.4.4

[59] Ett botnät är ett antal internetanslutna enheter som var och en kör en eller flera botar (program som kör automatiserade uppgifter över internet). Botnät kan användas för att utföra distribuerade attacker, stjäla data, skicka skräppost, etc.

[60] Inom datavetenskap är klusteranalys samlingsnamnet för olika algoritmer som används för att gruppera data i delmängder som kallas kluster.

4.4 AI-metoder på applikationsnivå

AI spelar en viktig roll för att tillhandahålla applikationstjänster till slutanvändaren. Nedan diskuterar vi några domäner där IoT-applikationer drar nytta av AI. Detta avsnitt är främst baserat på en genomgång som har gjorts av Samie o.a. (2019) och de källor som är presenterade den genomgången.

4.4.1 Hälsovård

Sjukvård och hälsovård är ett av de områdena där IoT-tekniken växer snabbt. IoT-enheter kan användas för övervakning av hälsotillståndet hos användarna genom att samla biomedicinska signaler från deras kroppar. Den insamlade informationen kan användas för övervakning av patienter, upptäckt av sjukdomar i tidigt skede, hjälp av patienter genom att reglera och kontrollera utrusning på ett optimalt sätt, aktivitetsigenkänning och övervakning av livsstil. (Samie, Bauer, & Henkel, 2019)

Tack vare bevakning av hjärtats elektriska aktivitetssignal eller elektrokardiogram (EKG) kan stress och hjärt-kärlsjukdomar upptäckas. En klassificerare[61] kan upptäcka avvikelser från hjärtslag från EKG-signaler på IoT-enheten. Klassificering av hjärtrytmen kan användas för att utveckla en bärbar EKG-diagnosanordning lämplig för kontinuerlig fjärrövervakning av patienter med kroniska hjärt-kärlsjukdomar. (Azariadi, Tsoutsouras, Xydis, & Soudris, 2016)

Hjärnans elektriska aktivitetssignal eller Elektroencefalografi (EEG) kan användas i olika tillämpningar för utökade välbefinnande och hälsa eller prognos av ett sjukligt tillstånd.

En AI-algoritm för att förutsäga epileptiska anfall som är anpassad för IoT-enheter presenterats i (Samie, Paul, Bauer, & Henkel, 2018). Denna algoritm är tillräckligt effektiv för att kunna köras på en bärbar enhet med en låg effekt utan att varken behöva stort internt minne eller kraftfull beräkningskraft. Om AI-beräkningarna ska köras på själva IoT-enheten och inte som en tjänst i en molnserver krävs det att de inneboende begränsningar som IoT-enheter har övervinns. Detta åstadkoms genom att algoritmerna modifieras så att man får lika eller tillräckligt bra resultat med begränsade resurser.

[61] Klassificerare är det gemensamma namnet för metoder och algoritmer inom AI som identifierar till vilken underkategori en ny observation tillhör. Detta görs genom att träna en modell med träningsdata som innehåller observationer vars kategorimedlemskap är känt.

För att upptäcka trötthet eller dåsighet hos en förare har Li o.a. (2015) utvecklat ett system där en huvudbindel som är kopplad till en smartklocka via Bluetooth registrerar förarens EEG-signaler. Genom att analysera signalerna kan olika grader av dåsighet upptäckas hos föraren med hög tillförlitlighet i realtid.

4.4.2 Smarta hem

Inom smarta hem använder IoT-system AI främst för att förbättra användarkomfort, optimera energiförbrukning och automatisera hemhjälp och hemsjukvård.

Upptäckt av människans närvaro, aktivitetsigenkänning, självorganiserade hushållsapparater, kontroll av luftkonditionering baserat på användarkomfort och liknande är exempel på applikationer som möjliggörs genom att AI integreras med IoT. (Samie, Bauer, & Henkel, 2019) Speciellt kommer aktivitetsigenkänning att vara av stor betydelse och användbarhet på grund av dess breda tillämpning inom automatiserad hemhjälp och hemsjukvård. Som bekant är batterilivslängd en begränsande faktor för användningen av AI inom IoT. Fafoutis o.a. (2018) presenterar en lösning för smarta sjukvårdsapparater som använder inbäddad AI, d.v.s. gör själva beräkningarna och extraherar informationen på den bärbara sensorenheten istället för att kommunicera stora mängder rådata över nätverk.

Smarta hem-konceptet innebär bland annat att de boende ska kunna kontrollera, övervaka och hantera sin energiförbrukning och därmed minska energikostnaderna och miljöpåverkan. AI och självlärande system kan vara en naturlig del av IoT-system för optimering av energiförbrukning. Li, Logenthiran, Phan, & Woo (2018) presenterar ett självlärande hemhanteringssystem. I den föreslagna lösningen integreras ett smart energihanteringssystem, både på konsument- och leverantörsida för realtidsdrift av smarta hem. Detta integrerade system använder AI för att implementera vissa förmågor såsom prisprognoser, prisklustring och avbrottvarningssystem för att förbättra dess funktioner. Enligt experiment som de utför överträffar det föreslagna systemet traditionella smarta hem genom att kunna anpassa modellen för olika typer av miljöer.

4.4.3 Smarta jordbruk

IoT-system kan använda AI-metoder för att förbättra produktiviteten och minska kostnaderna för underhåll i jordbrukssystem och jordbruk. Detta kan uppnås genom att: 1) upptäckta sjukdomar och skadedjur, och 2) upprätthålla de nödvändiga förutsättningarna som växter behöver t.ex. temperatur, fukt och jordens tillstånd. För bedömning av miljö eller

anläggning används antingen övervakningsmedel, t.ex. bild och video eller andra typer av sensorer som mäter temperatur, luftfuktighet, och liknande. (Samie, Bauer, & Henkel, 2019)

Bildklassificering kan användas för att upptäcka skadedjur och växtsjukdomar hos växter på en gård med hjälp av kamerabilder. Men IoT för jordbrukssystem har vissa egenskaper som gör att tillämpningen av AI-metoder blir extra svår. Till exempel, antalet och uppsättningen av kameror inom övervakning av jordbrukssystem är sparsam vilket leder till att bilder och videoklipp av skadedjur blir otydliga och består av få pixlar. Detta minskar sannolikheten att kunna upptäcka och klassificera skadedjur. Yue, o.a. (2018) presenterar en djupinlärningsmetod[62] som kan klara av uppgiften med högre prestanda och gör det möjligt att minska antalet kameror och därmed minska kostnaderna för IoT-infrastrukturen, vilket är av högt praktiskt värde för jordbruk.

Owomugisha & Mwebaze (2016) presenterar en annan tillämpning av AI inom jordbruk som kan ställa diagnos på en växts sjukdom (och även svårighetsgraden på sjukdomen) genom att använda bilder som har tagits med en smartphone och laddats upp till en server där själva klassificeringen äger rum.

I ett annat exempel presenterar Patil & Thorat (2016) en metod där olika miljöparametrar som temperatur, luftfuktighet och bladfuktighet för en druvväxt samlas. Den samlade informationen överförs till en server där en applikation gör en bedömning av risker för druvsjukdomar i ett tidigt stadium och meddelar jordbrukaren.

Ett smart system inom jordbruket introduceras i (Yahata, o.a., 2017) för att upptäcka blommor och fröskal i utomhusmiljöer och under naturliga förhållanden utifrån tagna bilder som skickas från en anläggning i en gård med syfte att övervaka tillväxttakten och miljöparametrar. Det slutliga målet med produkten är att tillhandahålla beslutsstöd till den yngre generationens jordbrukare som saknar de traditionella kunskaperna som den äldre generationen hade.

En av nackdelarna med befintliga lösningar inom smart jordbruk är deras beroende av molnservrar. Komplexiteten av databehandling i dessa applikationer kräver effektiv och kraftfull hårdvara för att möjliggöra beräkningarna på inbäddade IoT-enheter. (Samie, Bauer, & Henkel, 2019)

[62] Djupinlärning är en del av området AI som använder sig av artificiellt neuronnät dvs. självlärande algoritmer som försöker efterlikna funktionen i biologiska neuronnät (exempelvis hjärnan).

4.4.4 Smart industri

Smart industri eller Industriell Internet of Things (IIoT) kan definieras som ett system bestående av smarta objekt (IoT-enheter) och tillhörande IT-teknologier och infrastruktur som möjliggör realtid, intelligent och autonom tillgång, samling, analys, kommunikation och utbyte av process, produkt och/eller tjänster inom den industriella miljön för att optimera produktiviteten, energiförbrukningen och arbetskraftskostnader. (Boyes, Hallaq, Cunningham, & Watson, 2018)

Smart industri kan dra nytta av tillgängliga data och AI-metoder för att förbättra hantering av underhållsarbete, kvalitetssäkring och schemaläggning. (Samie, Bauer, & Henkel, 2019) Enligt McKinsey & Company som är en tongivande aktör inom strategi och management,[63] uppskattas den största andelen av IoT-tillväxten ske inom tillverkningsindustrin,[64] t.ex. inom det som kallas *prediktivt underhåll* (eng. *predictive maintenance*). I korthet innebär det att mäta vibrationer på komponenter i ett system och på förhand upptäcka om komponenten är på väg att gå sönder. Denna typ av förmåga är förstås önskvärd i säkerhetskritiska system (t.ex. i en jetmotor) eller i sammanhang där produktionsstopp är kostsamt. I det första fallet kan det rädda liv och i det senare fallet kan det hjälpa att undvika produktionsstopp genom att beställa komponenten och byta ur den redan innan maskinen stannat.

Att maximera produktionsavkastningen är kärnan i tillverkningsindustrin. I stora monteringsband registreras data för produkter när de går igenom varje steg. Mangal & Kuma (2016) tillämpar AI-metoder som kan förutsäga vilka delar är mest troligt att gå sönder. Således kan ett smartare feldetekteringssystem byggas som bevakar de delar som har högre risk att gå sönder och på så sätt minska driftskostnaderna och öka vinstmarginalerna. En utmaning i detta arbete har varit den högdimensionella datamängden.

Ett annat exempel på smart industri är tillämpningen av AI-metoder för att göra prognoser på efterfrågan (i frånvaro av fullständig information) och på så sätt optimera leverantörskedjan. (Carbonneau, Laframboise, & Vahidov, 2008)

Susto o.a. (2015) använder AI-metoder för att hantera underhållsfrågor i tillverkningsprocesser med tanke på det ökande behovet av att minimera

[63] https://en.wikipedia.org/wiki/McKinsey_%26_Company

[64] https://www.mckinsey.com/featured-insights/internet-of-things/our-insights, besökt 2019-12-12

driftstopp och de förknippade kostnader. Det framtagna systemet används för att upptäcka de fel som orsakas av ackumulerat slitage. Två utmaningar i detta område är: 1) obalanserade data då antalet fel som inträffar är relativt lågt, och 2) att förutsäga och förhindra problemen måste felen upptäckas innan de händer.

I ett liknande försök använder Wu o.a. (2018) AI-metoder för att diagnostisera (identifiera maskinfel och bestämma orsaken) och göra prognos (uppskatta ett fels svårighetsgrad) i industriellmiljö. Baserat på samlade data lyckas deras metod lära sig mönstren i observerade maskiners arbete och förutsäga hur länge en maskin håller innan den går sönder.

4.4.5 Smarta elnät

Enligt definitionen i *International Electrotechnical Commission*[65] är smarta elnät elektriska kraftnät som använder IT och reglerteknik, distribuerade datorsystem och tillhörande sensorer och ställdon, för att: 1) integrera beteende och handlingar hos slutanvändare och andra intressenter, och 2) effektivt leverera hållbar, ekonomisk och säker elförsörjning.[66]

Smarta elnät syftar till att förbättra kraftnätets effektivitet genom att använda de anslutna mätarna. De viktigaste problemen inom smarta kraftnät som kan utnyttja olika AI-metoder är dynamisk prissättning, integration av förnybara energier, etc.

Wei o.a. (2015) utvecklar en AI-metod för att lösa optimal batterihantering och styrningsproblem i smarta bostäder som bland annat är utrustade med laddningsbara batterier för energiförsörjning. Uppgiften är att hitta den optimala batteriladdningen/urladdningen vid varje tidssteg så att den totala kostnaden för energin från elnätet minimeras givet batteriets begränsningar.

O'Neill, Levorato, Goldsmith, & Mitra (2010) använder AI-metoder för att uppskatta det framtida energipriset (rörligt elpris) i smarta elnät och schemalägger sedan hushållsapparater för att minimera energikostnaden för bostäder och utjämna energianvändningen. Metoden bygger på en

[65] International Electrotechnical Commission (IEC), grundad 1906, är en kommission vars främsta syfte är att arbeta fram och fastställa internationella standarder inom elektroteknik och elektronik (https://www.iec.ch/).

[66] http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=617-04-13, besökt 2019-12-12

implicit uppskattning av effekterna av framtida energipriser och konsumenternas beslut på den långsiktiga elkostnaden och schemalägger elanvändningen av konsumenterna. Modellen lär sig kontinuerligt och anpassar sig till individuella konsumentpreferenser och prisändringar över tid.

En lite annorlunda metod används av Thapa o.a. (2018) som löser problemet med att schemalägga *förskjutbara* elbelastningar för flera konsumenter i smarta elnät med hjälp av spelteori. Förskjutbara belastningar i smarta elnät är de enheter som kan tolerera en viss fördröjning tills effekten levereras (t.ex. vatten- och golvvärme). Detta i motsats till *icke-förskjutbara* elbelastningar som kräver el omedelbart när de slås på (t.ex. glödlampor och TV-apparater). Eftersom de förskjutbara belastningarna kan planeras adaptivt, kan systemet jämföra energiförbrukningens kurva och välja den mest fördelaktiga tidpunkten för att leverera effekten så att elnäten inte blir överbelastade.

Ett viktigt mål för smarta elnät är att öka andelen energi från förnybara energikällor. En utmaning med att integrera förnybar energi i elnätet är att dess produktion är oregelbunden och okontrollerbar. Således är det viktigt att kunna förutsäga mängden förnybar elproduktion, eftersom nätet måste starta generatorer för att tillfredsställa efterfrågan om produktionen varierar. Medan sofistikerade prediktionsmodeller för storskaliga solcellsanläggningar kan utvecklas manuellt så är det ett utmanande problem att utveckla modeller för distribuerad elproduktion i miljoner hem spridda över hela elnätet. För att lösa problemet har Sharma o.a. (2011) utforskat en automatiskt AI- metod som använder internetbaserad väderprognostjänst för att göra platsspecifika förutsägelser för solenergiproduktion, vilket visar högre prestanda i jämförelse med mer traditionella modeller.

En exakt prognos för hushållens elförbrukning är av stor betydelse för att skapa en effektiv energipolitik för att möta befolkningens nuvarande och framtida behov. Därför kan mer informerade beslut fattas om tillförlitliga kunskaper finns om vilka faktorer (elpris, hushållens inkomst etc.) som bestämmer efterfrågan på el.

Med utvecklingen av såväl avreglerad elmarknad som smarta elnät har förutsägelse av hushållens elförbrukning fått allt större betydelse. Chen o.a. föreslår en ny AI-metod för att förutsäga hushållens årliga elförbrukning. De kombinerar en mer detaljerad datauppsättning och utvecklar flera olika prediktiva modeller och genom att kombinera dessa modeller får förutsägelser. Denna metod lyckas förutsäga hushållens elförbrukning betydligt mer exakt jämfört med de traditionella modellerna.

El är svårt och dyrt att lagra (till skillnad från bränsle) och det är viktig att upprätthålla balansen mellan produktion och efterfrågan. Därför är det mycket önskvärt att kunna göra exakta prognoser av elförbrukning. Tidsskalan för prognosen skiljer sig mellan olika intressenter. Medan elhandelsföretag är intresserade av efterfrågan för nästföljande dag för att programmera elproduktionen därefter, är elnätsbolag intresserade att kunna förutsäga elförbrukningen nästföljande år för att säkerställa att infrastrukturen räcker för behovet. För att tillhandahålla prognoser med olika tidsskalor använder Vantuch o.a. (2018) olika AI-metoder som var och en är överlägsen för respektive intresseområdet.

Ett annat användningsområde för AI-metoder inom smarta elnät är upptäckt av bedrägerier. Ford, Siraj, & Eberle (2014) tillämpar AI för analys av mätarens finkorniga data för att känna igen normala mönster av elkonsumtion och upptäcka avvikelser från detta beteende. Enligt författarna uppnår metoden en högre detekteringsfrekvens av obehörig energianvändning än andra metoder inom detta fält.

4.5 Övrigt

Förutom rena AI-tekniker så utvecklas det andra tekniker för att stödja IoT-system.

Blockkedjetekniken (eng. *blockchain*) har slagit igenom på senare tid genom att den ligger till grund för kryptovalutan Bitcoin. Den har även börjat användas i andra sammanhang, exempelvis för att skapa distribuerade digitala kontrakt. I IoT-samverkan finns en eller flera aktörer som både behöver dela data och samtidigt kunna lita på att data inte manipulerats. Blockchain-tekniken kan erbjuda den typen av säkerhet. (Pinto, 2019)

Metoder för dataaggregering (eng. *data aggregation*) och datafusion (eng. *data fusion*) uppvisar stora likheter men även vissa skillnader. Litteraturen om dataaggregering för IoT fokuserar på att reducera mängden data som sänds från en IoT-enhet (och därmed spara batterikraft och bandbredd) och berör främst fall då IoT-systemet realiseras med trådlösa sensornät (WSN). (Dehkordi, o.a., 2019) I praktiken kan datareduktionen handla om att räkna ut medelvärdet av data över tid och rum. Dataaggregering kan även vara själva syftet med IoT-systemet och inte bara ett sätt att energieffektivisera, men det perspektivet verkar inte hanteras i litteraturen.

Datafusionsmetoder syftar främst till att minska osäkerheter i data eller för att dra slutsatser om data som inte kan observeras direkt. Även här nyttjas redundans och mest som en bieffekt blir resultatet normalt en

reducerad datamängd. Men fokus är alltså på att öka kvaliteten av data och skapa ett bättre beslutsunderlag. (Alam, Mehmood, Katib, Albogami, & Albeshir, 2017; Nakamura, Loureiro, & Frery, 2007)

5 Sammanfattning och diskussion

Diskussionen i det här kapitlet är baserad på den tentativa undersökningen som redovisas i kapitel 2. Eftersom de erhållna insikterna främst är baserade på informella samtal och mejlutbyte med berörda organisationer samt observationer från exempelvis konferenser så är slutsatserna avsiktligt vagt formulerade.

Från ett försvarsmaktsperspektiv finns det anledning att följa och, i valfri utsträckning, engagera sig i den framväxande IoT-miljön (inte minst i form av ”smarta städer”). Å ena sidan erbjuder IoT-miljön en möjlighet att förstärka lägesbilder i en totalförsvarsoperation, å andra sidan uppstår det nya samhälleliga risker i IoT-miljön som det krävs beredskap för (exempelvis att ett IoT-system för trafikledning förses med felaktig information för att störa totalförsvarsaktiviteter).

Möjligheten till IoT-samverkan mellan myndigheter verkar idag vara begränsad, delvis på grund av att nyttjandegraden av IoT-system hos myndigheterna är blygsam och för att anpassningen för system- och informationsdelning är otillräckligt outredd.[67] Konsekvensen av dagens ad hoc-system för samverkan mellan myndigheter är ett ineffektivt nyttjande av samhällets resurser. (Andersson, Lindgren, Nilsson, Berglund, & Svenonius, 2019) Det finns en risk att utrustning som samhället investerat i står oanvänd då den istället skulle kunna bidra med viktig information vid t.ex. krissituationer.

Förutsättningarna för framtida IoT-samverkan ser dock goda ut. Det finns nämligen idag en befintlig infrastruktur för myndighetskommunikation i form av verktyg som Rakel, SGSI, WIS och Sjöbasis. Infrastrukturen vidareutvecklas dessutom kontinuerligt. Nya tjänster tillkommer och flera av verktygen integreras med varandra. Denna utveckling ökar möjligheterna för att introducera fler IoT-system för ökad samverkan mellan myndigheterna. Regeringsinitiativen för ett ”myndighetsmoln” och datautbyte har dessutom potential att möjliggöra en säker informationsdelningsplattform och integration av offentliga IoT-system.

Hos svenska kommuner verkar det vidare finnas en stor medvetenhet och motivation att dela offentlig data. Olika portaler för dataåtkomst finns tillgängliga. Verksamhetsmässigt finns alltså förmodligen redan beredskap för att dela även IoT-data och det tekniska steget förefaller också vara förhållandevis litet. Kommunerna är också i ett läge där en

[67] Det är värt att även påminna om den juridiska dimensionen och säkerhetsaspekterna med IoT som inte behandlas i den här rapporten, men som är avgörande för IoT-samverkan i praktiken.

gemensam datamodell behövs utvecklas, dels för att kunna utbyta och jämföra information, men också för att effektivisera implementationen av IoT-system i kommunernas verksamhet. Det är ett arbete som även myndigheter (kanske genom DIGG:s eller MSB:s försorg) samt Försvarsmakten bör ta del i för att säkra framtida IoT-samverkan.

Från ett Försvarsmakts- och totalförsvarsperspektiv (FMTF) föreslår vi för vidare arbete om IoT-samverkan att FMTF-nyttan lyfts upp och påverkar inriktningen av arbetet. Vi föreslår följande möjliga verksamheter (ej prioritetsordnade):

1. **Omvärld**
   Natogruppen NATO STO IST-147 ”Military application of the Internet of things” (år 2016-2019) har på djup teknisk nivå studerat just IoT-samverkan mellan smarta städer och militär organisation. (Johnsen, o.a., 2018) Det vore givande att i detalj studera gruppens resultat och dra lärdom av dessa.
2. **Användarfall** (use case)
   Utveckling av ett användarfall rörande Totalförsvaret som kan användas för att sätta vidare studier om IoT-samverkan i ett sammanhang, samt involvera och engagera andra myndigheter, kommuner och organisationer.
3. **Interoperabilitet**
   Delta (tillsammans med myndigheter, kommuner och andra organisationer) i utvecklingen av gemensamma standarder för IoT-samverkan (exempelvis datamodeller, ontologier, kvalitetsmått, och gränssnitt). Hur presenteras information för externa användare så att de förstår dess användbarhet? Hur hittas data och ställdon som är intressanta för den egna organisationen?
4. **Lägesbilder**
   Hur nyttiggörs på bästa sätt extern IoT-information (för att exempelvis förstärka en lägesbild)? Hur särbehandlas externa data från interna? Behöver data från externa källor anonymiseras eller aggregeras?

Litteraturförteckning

Alam, F., Mehmood, R., Katib, I., Albogami, N. N., & Albeshir, A. (den 25 april 2017). Data fusion and IoT for smart ubiquitous environments: a survey. *IEEE Access, 5*, 9533-9554. doi:10.1109/ACCESS.2017.2697839

Andersson, M., Lindgren, D., Nilsson, P., Berglund, Å., & Svenonius, O. (2019). *Delad sensordata förbättrar hantering av kriser, terrorism och höjd beredskap.* FOI Memo 6743.

Azariadi, D., Tsoutsouras, V., Xydis, S., & Soudris, D. (2016). ECG Signal Analysis and Arrhythmia Detection on IoT wearable medical devices. *5th International Conference on Modern Circuits and Systems Technologies (MOCAST).* IEEE.

Banafa, A. (den 14 March 2016). *The Last Mile of IoT: Artificial Intelligence*. Hämtat från OpenMindBBVA: https://www.bbvaopenmind.com/en/technology/artificial-intelligence/the-last-mile-of-iot-artificial-intelligence-ai/

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry, 101*, 1-12.

Carbonneau, R., Laframboise, K., & Vahidov, R. (2008). Application of machine learning techniques for supply chain demand forecasting. *European Journal of Operational Research, 184*(3), 1140–1154.

Chafii, M., Bader, F., & Palico, J. (2018). Enhancing coverage in narrow band-IoT using machine learning. *in Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, (ss. 1-6).

Chen, K., Jiang, J., Zheng, F., & Chen, K. (May 2018). A novel data-driven approach for residential electricity consumption prediction based on ensemble learning. *Energy, 150*, 49–60.

Cui, W., Kim, Y., & Rosing, T. S. (2017). Cross-platform machine learning characterization for task allocation in IoT ecosystems. *in Proc. Comput. Commun. Workshop Conf. (CCWC)*, (ss. 1-7).

Dehkordi, S. A., Farajzadeh, K., Rezazadeh , J., Farahbakhsh, R., Sandrasegaran, K., & Dehkordi, M. A. (2019). A survey on data aggregation techniques in IoT sensor networks. *Wireless networks*. doi:https://doi.org/10.1007/s11276-019-02142-z

Dias, G. M., Nurchis, M., & Bellalt, B. (2016). Adapting sampling interval of sensor networks using on-line reinforcement learning. *in Proc. WF-IoT* (ss. 460–465). IEEE.

EDA. (den 17 november 2019). *MARSUR Maritime Surveillance Networking*. Hämtat från https://www.eda.europa.eu/what-we-do/activities/activities-search/maritime-surveillance-(marsur)

Ekot. (den 30 september 2019). *Staten ska ha egna molntjänster.* Hämtat från Sveriges radio: https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=7311386

Fafoutis, X., Marchegiani, L., Elsts, A., Pope, J., Piechocki, R., & Craddock, I. (2018). Extending the Battery Lifetime of Wearable Sensors with Embedded Machine Learning. *IEEE 4th World Forum on Internet of Things (WF-IoT)* (ss. 269--274). Singapore: IEEE.

Ford, V., Siraj, A., & Eberle, W. (2014). Smart Grid Energy Fraud Detection Using Artificial Neural Networks. *Comput. Intell. Appl. Smart Grid (CIASG)*, (ss. 1-6).

Golanbari, M. S., & Tahoori, M. B. (2018). Runtime adjustment of IoT system-on-chips for minimum energy operation. *55th ACM/ESDA/IEEE Design Automation Conference (DAC)*, (ss. 1-6).

Golanbari, M. S., Kiamehr, S., Oboril, F., Gebregiorgis, A., & Tahoori, M. B. (2017). Post-fabrication calibration of near-threshold circuits for energy efficiency. *in Proc. ISQED*, (ss. 385-390).

Goldman Sachs. (den 3 september 2014). Hämtat från Goldman Sachs: https://www.goldmansachs.com/insights/pages/internet-of-things/iot-report.pdf

HiQ. (den 4 november 2019). *Till havs 24/7365*. Hämtat från https://www.hiq.se/case/kustbevakningen/

Horndahl, A., Johansson, F., Johansson, R., Mårtenson, C., Rosell, M., Pavlin, G., & Preden, J.-S. (2016). *D5.4 - Design of tools for automatic processing of heterogeneous intelligence information.* FOI-S--5538--SE.

Industrinyheter. (den 27 november 2019). *Härryda kommun satsar på IoT*. Hämtat från https://www.industrinyheter.se/20190802/28342/harryda-kommun-satsar-pa-iot

Johansson, R. (2018). *Försvarsmakten i den civila IoT-miljön.* FOI Memo 6641.

Johnsen, F. T., Bloebaum, T. H., Brannsten, M. R., & Lund, K. (2018). Using open standards for utilizing IoT sensor in a smart city scenario. *International command and control research and technology symposium (ICCRTS).* Pensacola, FL, USA.

Johnsen, F. T., Zielinski, Z., Wrona, K., Suri, N., Fuchs, C., Pradhan, M., . . . Krzyszton, M. (2018). Application of IoT in military operations in a smart city. *2018 International Conference on Military Communications and Information Systems (ICMCIS).* Budva, Montenegro.

Kamrani, F., Wedlin, M., & Rodhe, I. (2016). *Internet of Things: Security and Privacy Issues.* FOI-R--4362--SE.

Kott, A., Swami, A., & West, B. (december 2016). The Internet of Battle Things. *Computer, 49*(12), 70-75.

Kraemer, F. A., Ammar, D., Braten, E. A., Tamkittikhun, N., & Palm, D. (2017). Solar energy prediction for constrained IoT nodes based on public weather forecasts. *in Proc. Int. Conf. Internet Things*, (s. 2).

Kustbevakningen. (den 4 november 2019). *Ny generation av Sjöbasis har driftsatts*. Hämtat från https://www.kustbevakningen.se/granslos-samverkan/nyhetsarkiv/ny-generation-av-sjobasis-har-driftsatts/

Kustbevakningen. (den 4 november 2019). *Sjöbasis*. Hämtat från https://www.kustbevakningen.se/granslos-samverkan/sjoovervakningsuppdraget/samverkan-sjoinformation/

Landgren, J., & Borglund, E. (2016). *Lägesbilder – Att skapa och analysera lägesbilder vid samhällsstörningar.* MSB770.

Lee, S.-Y., Wi, S.-r., Seo, E., Jung, J.-K., & Chung, T.-M. (2017). ProFiOt: Abnormal behavior profiling (ABP) of IoT devices based on a machine learning approach. *27th International Telecommunication Networks and Applications Conference (ITNAC)* (ss. 1-6). IEEE.

Li, G., Lee, B.-L., & Chung, W.-Y. (2015). Smartwatch-Based Wearable EEG System for Driver Drowsiness Detection. *IEEE Sensors J., 15*(12), 7169-7180.

Li, W., Logenthiran, T., Phan, V.-T., & Woo, W. (2018). Implemented IoT-based self-learning home management system (SHMS) for Singapore. *IEEE Internet Things J., 5*(3), 2212–2219.

Lindgren, D., Andersson, M., Berglund, Å., Nilsson, P., Krona, M., Svenonius, O., . . . Trnka, J. (2018). *BEViS 2018.* FOI MEMO 6613.

Lindman, J., & Saarikko, T. (2018). *Internet of things: threats and opportunities for society.* MSB. Hämtat från https://www.msb.se/sv/publikationer/internet-of-things-threats-and-opportunities-for-society-study/

Linnéuniversitetet. (den 27 november 2019). *Kalmar Energi + Linnéuniversitetet + internet of things = sant!* Hämtat från https://lnu.se/mot-linneuniversitetet/aktuellt/nyheter/2019/kalmar-energi--linneuniversitetet--internet-of-things--sant/

Malmqvist, M. (den 26 september 2019). *Här är de smarta saker Ericsson ska fylla 5g-näten med.* Hämtat från Computer Sweden: https://computersweden.idg.se/2.2683/1.723983/5g-ericsson-smarta-saker-koppla-upp

Mangal, A., & Kuma, N. (2016). Using Big Data to Enhance the Bosch Production Line Performance: A Kaggle Challenge. *IEEE International Conference on Big Data (Big Data)* (ss. 2029-2035). IEEE.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *The internet of things: mapping the value beyond the hype.* McKinsey global institute.

Minerva, R., Chebudie, A., & Rotondi, D. (2014). *Towards a Definition of the Internet of Things (IoT).* IEEE Internet initiative.

Montiel-Sánchez, I. (2017). Disruptive defense innovations ahead. *European defense matters*, s. 15. Hämtat från https://www.eda.europa.eu/webzine/issue14/cover-story/defence-internet-of-things-(diot)

MSB. (2014). *Gemensamma grunder för samverkan och ledning vid samhällsstörningar.* Hämtat från https://www.msb.se/RibData/Filer/pdf/27483.pdf

MSB. (2018). *Vägledning för säker och robust samverkan version 1.0.* MSB.

MSB. (den 24 oktober 2019). *Om SGSI*. Hämtat från https://www.msb.se/sv/verktyg--tjanster/sgsi/om-sgsi/

MSB. (den 27 november 2019). *Totalförsvarsövning 2020*. Hämtat från https://www.msb.se/sv/utbildning--ovning/ovning/totalforsvarsovning-2020/

MSB. (den 14 november 2019). *WIS - webbaserat informationssystem*. Hämtat från https://www.msb.se/sv/verktyg--tjanster/wis/

Nakamura, F. E., Loureiro, A. A., & Frery, A. C. (september 2007). Information Fusion for Wireless Sensor Networks: Methods, Models, and Classifications. *ACM Computing Surveys, 39*(3). doi:10.1145/1267070.1267073

Nilsson, P., Lindgren, D., Andersson, M., & Nordlöf, J. (2018). *Myndighetssamverkan avseende bevakningssensorer.* FOI-R--4553--SE.

Noura, M., Atiquzzaman, M., & Gaedke, M. (June 2019). Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mobile Networks and Applications, 24*(3), 796-809.

NyTeknik. (den 30 september 2019). *Staten ska ha egna molntjänster: "Finns stora vinster".* Hämtat från NyTeknik: https://www.nyteknik.se/digitalisering/staten-ska-ha-egna-molntjanster-finns-stora-vinster-6973244

O'Neill, D., Levorato, M., Goldsmith, A., & Mitra, U. (2010). Residential Demand Response Using Reinforcement Learning. *Int. Conf. Smart Grid Commun. (SmartGridComm)*, (ss. 409–414).

Orhean, A. I., Pop, F., & Raicu, I. (July 2018). New scheduling approach using reinforcement learning for heterogeneous distributed systems. *Journal of Parallel and Distributed Computing, 117*, 292-302.

Owomugisha, G., & Mwebaze, E. (2016). Machine Learning for Plant Disease Incidence and Severity Measurements from Leaf Image. *15th IEEE International Conference on Machine Learning and Application* (ss. 158-163). IEEE.

Patil, S., & Thorat, S. (2016). Early Detection of Grapes Diseases Using Machine Learning and IoT. *Second International Conference on Cognitive Computing and Information Processing (CCIP).* IEEE.

Pinto, R. (den 29 maj 2019). *Demystifying The Relationship Between IoT And Blockchain.* Hämtat från Forbes: https://www.forbes.com/sites/forbestechcouncil/2019/05/29/demystifying-the-relationship-between-iot-and-blockchain/#489c7941605d den 20 november 2019

Samhällssäkerhet, M. (den 27 november 2019). Hämtat från https://www.samhallssakerhet.se/sv/om/

Samie, F., Bauer, L., & Henkel, J. (2019). From Cloud Down to Things: An Overview of Machine Learning in Internet of Things. *IEEE Internet of Things (IoT) J., 6*(3).

Samie, F., Paul, S., Bauer, L., & Henkel, J. (2018). Highly Efficient and Accurate Seizure Prediction on Constrained IoT Devices. *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, (ss. 955-960).

Sharma, N., Sharma, P., Irwin, D., & Shenoy, P. (2011). Predicting solar generation from weather forecasts using machine learning. *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (ss. 528-533). Brussels, Belgium: IEEE. doi:10.1109/SmartGridComm.2011.6102379

Sharmeen, S., Huda, S., Abawajy, J., Ismail, W., & Hassan, M. (2018). Malware threats and detection for industrial mobile-IoT networks. *Access, 6*, 15941–15957.

SOU. (2019). *Skogsbränderna sommaren 2018.* Stockholm: Statens offentliga utredningar.

Sun, P., Li, J., Bhuiyan, Z. A., Wang, L., & Li, B. (April 2019). Modeling and clustering attacker activities in IoT through machine learning techniques. *Information Sciences, 479*, 456-471.

Susto, G. A., Schirru, A., & Pampuri, S. (2015). Machine Learning for Predictive Maintenance: A Multiple Classifier Approach. *IEEE Transactions on Industrial Informatics, 11*(3), 812–820.

Sveriges Radio. (den 11 December 2019). *Regeringen vill se gemensamma it-system*. Hämtat från Sveriges radio: https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=7364612

Sydöstran. (den 27 november 2019). *Samarbete från Blekinge prisas*. Hämtat från http://www.sydostran.se/karlskrona/samarbete-fran-blekinge-prisas/

Thapa, R., Jiao, L., Oommen, B., & Yazidi, A. (2018). A Learning Automaton-Based Scheme for Scheduling Domestic Shiftable Loads in Smart Grids. *IEEE Access, 6*, 5348–5361.

Tolk, A. (2004). Composable Mission Spaces and M&S Repositories – Applicability of Open Standards. *In Spring simulation interoperability workshop.* Arlington (VA).

Trafikverket. (den 8 november 2019). *Trafikverket och MSB kompletterar Rakel med mobila datatjänster*. Hämtat från https://www.trafikverket.se/om-oss/nyheter/Nationellt/2018-10/trafikverket-och-msb-kompletterar-rakel-med-mobila-datatjanster/

US DoD. (2016). *DoD policy recommendations for IoT.* Hämtat från https://www.hsdl.org/?view&did=799676 den 15 oktober 2019

Vantuch, T., Vidal, A., Ramallo-González, A., Skarmeta, A., & Misák, S. (2018). Machine Learning based Electric Load Forecasting for Short and Long-term Period. *IEEE 4th World Forum Internet Things (WF-IoT)* (ss. 511–516). IEEE.

Wei, J., & Mendis, G. (2016). A Deep Learning-Based Cyber-Physical Strategy to Mitigate False Data Injection Attack in Smart Grids. *Cyber Phys. Security Resilience Smart Grids (CPSR-SG)*, (ss. 1-6).

Wei, Q., Liu, D., & Shi, G. (2015). Novel Dual Iterative Q-Learning Method for Optimal Battery Management in Smart Residential Environments. *IEEE Transactions on Industrial Electronics, 62*(4), 2509-2518.

Weiser, M. (1991). The Computer for the 21st Century. *Scientific American, 265*(3), 94-104.

Wikipedia. (den 15 november 2019). *Complex event processing*. Hämtat från Wikipedia: https://en.wikipedia.org/wiki/Complex_event_processing

Wu, Z., Luo, H., Yang, Y., Zhu, X., & Qiu, X. (2018). An Unsupervised Degradation Estimation Framework for Diagnostics and Prognostics in Cyber-Physical System. *IEEE 4th World Forum Internet Things (WF-IoT)* (ss. 784-789). IEEE.

Yahata, S., Onishi, T., Yamaguchi, K., Ozawa, S., Kitazono, J., Ohkawa, T., . . . Tsuji, H. (2017). A Hybrid Machine Learning Approach to Automatic Plant Phenotyping for Smart Agriculture. *Int. Joint Conf. on Neural Networks (IJCNN)* (ss. 1787-1793). IEEE.

Yue, Y., Cheng, X., Zhang, D., Wu, Y., Zhao, Y., Chen, Y., . . . Zhang, Y. (2018). Deep recursive super resolution network with Laplacian Pyramid for better agricultural pest surveillance and detection. *Computers and Electronics in Agriculture, 150*, 26-32.

Zhao, S., Li, W., Zia, T., & Zomaya, A. (2017). A Dimension Reduction Model and Classifier for Anomaly-Based Intrusion Detection in Internet of Things. *15th Intl Conf on Dependable, Autonomic and*

Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (ss. 836–843). IEEE.

Bilaga 1 – Nomenklatur

Den samling teknologi som vi idag ytligt identifierar som IoT har växt fram under decennier och under tiden har ett antal olika relaterade begrepp uppstått.

Begreppet ”Internet of things” gjordes populärt av Kevin Ashton (2009) för att beskriva fenomenet att internets virtuella cybervärld smälter ihop med den verkliga, fysiska, världen, men den grundläggande tekniken och idéerna hade växt fram under 2000-talet. Definitionen av IoT har diskuterats utförligt av Minerva m.fl. (2014) och i (US DoD, 2016). För vår rapport nöjer vi oss med att låna följande enkla definition:

> *The Internet of Things connects devices such as everyday consumer objects and industrial equipment onto the network, enabling information gathering and management of these devices via software to increase efficiency, enable new services, or achieve other health, safety, or environmental benefits.*
>
> Goldman Sachs (2014, s. 2)

Grundläggande i IoT-system är att data från noder i systemet samlas in för dataanalys eller styrning.[68] IoT har möjliggjorts av miniatyriseringen av kraftfull och energisnål beräknings- och telekomelektronik som lett till apparater som smarttelefoner, fullproppade med sensorer som GPS/GNSS, kamera, accelerometer och mikrofon.

Det handlar också om etablerade forskningsområden som trådlösa sensornätverk (eng. *wireless sensor networks*, WSN), smarta miljöer (*ubiquitous/pervasive/ambient computing*), och *cyber physical systems* (som kopplar samman WSN med ställdon).[69] Faktum är att idén med att utrusta diverse föremål med datorkraft och koppla ihop dem har sitt ursprung i Weiser (1991) [70] och IoT kan ses som en realisering av denna vision.

---

[68] Det är för tydlighets skull värt att notera att IoT definitionsmässigt handlar om uppkoppling mot nätverk av internettyp. Inom tillämpningsområdet smarta bilar är man tydlig med att detta bara är en form av flera möjliga uppkopplingssätt. Man kallar IoT ”vehicle to cloud” (V2C), men hanterar även exempelvis ”vehicle to vehicle” (V2V) och ”vehicle to infrastructure” (V2I). För att inkludera även dessa andra uppkopplingssätt inom IoT-begreppet talar man i vissa kretsar om en reviderad variant av IoT, IoT 2.0.

[69] Minerva (2014) diskuterar utförligt hur dessa begrepp förhåller sig till varandra.

[70] https://www.wespeakiot.com/meet-the-men-who-invented-iot/

Internets världsomspännande väv blev med tiden än mer tät och fick samtidigt kontakt med vår fysiska värld, och information uppsnappad där kunde bearbetas och delas i cybervärlden (genom omedelbart nyttjande av den internetteknik som införts och förfinats under de föregående decennierna) och beslut i vissa fall återföras till den fysiska världen via ställdon.

Givet den komplexa miljön som IoT verkar i, dvs. heterogena system och trådlösa nätverk som följer flera olika standarder och krav på säkerhetsaspekter, för att IoT ska fungera krävs att enheterna är utrustade med tillräcklig Artificiell Intelligens (AI) för att känna sin omgivning, interagera med andra enheter, vara kapabel att analysera resultaten, förstå förändringar och anpassa sig därefter. Därför har man börjat lansera olika begrepp som *Internet of Intelligent Things* (IoIT), *Artificial Intelligence of Things* (AIoT) och *Intelligence of Things* (IoT) för att understryka kopplingen mellan IoT och AI. Vi skiljer inte på dessa begrepp i denna rapport utan använder IoT som en övergripande term och utgår från att AI ska vara en inneboende del av IoT.

Vad gäller militär syn på IoT så beskriver U.S. DoD (2016) olika fördelar med IoT i den militära organisationen som gynnar militärmakten, bland annat möjlighet att få närmare realtidsuppsikt över de egna styrkornas och resursernas tillstånd. Kott m.fl. (2016) vid U.S. Army Research Laboratory benämner delområdet *Internet of Battle things* (IoBT) och diskuterar även nyttjandet av civil IoT. En variant är att ”battle” byts ut mot ”military” (IoMT) men betydelsen förefaller vara densamma.[71] Även EDA (European Defense Agency) identifierade nyligen militär IoT, men med den alternativa beteckningen *defense IoT* (”dIoT”), som en av tio potentiellt omvälvande tekniktrender de närmaste åren (Montiel-Sánchez, 2017). Där konstateras att IoT-teknik redan idag nyttjas av militära organisationer och att IoT-tekniken har bäring på bland annat skapandet av lägesbild[72] och man ser potentialen i att nyttja sensorer ur externa IoT-system.

[71] https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt, besökt 2019-10-25

[72] FOI deltog under år 2014-2016 i det FMV-stödda EDA-projektet IN-4-STARS2.0 som handlade om militär IoT i internationella insatser. (Horndahl, o.a., 2016)

FOI

ISSN 1650-1942

www.foi.se