**Datasäkerhet och Datasekretess inom IoT, samt NFC-baserad nätverksautentisering för IoT-enheter**

Rasmus Karlsson, 41001  
Kandidatavhandling i Datavetenskap  
Handledare: Jerker Björkqvist  
Fakulteten för Naturvetenskaper och Teknik  
Åbo Akademi  
2019

**Referat**I den här avhandlingen undersöks vilka faktorer som påverkar datasäkerheten och datasekretessen i traditionella datasystem, i IoT-system, och skillnaderna mellan dem. Bland annat behandlas användarsäkerhet, fysisk säkerhet och andra faktorer, vilka påverkar datasäkerheten, medan det för datasekretessens del tas upp hur lagstiftning kan användas för att ge användare bestämmanderätt över sin information. En metod för att bygga upp ett IoT-nätverk genom NFC-kommunikation, kombinerat med asymmetrisk kryptering och digital signering, undersöks även för dess användarvänlighet och eliminering av datasäkerhetsrelaterade riskfaktorer. Även olika typer av attacker mot datasystem presenteras med beskrivningar av de motiveringar och mål som brukar ligga bakom dem.

Innehållsförteckning

[1. Introduktion 1](#__RefHeading___Toc465_2258805889)

[2. Bakgrund och motiveringar för avhandlingen 3](#__RefHeading___Toc467_2258805889)

[2.1 Termerna datasäkerhet och datasekretess 3](#__RefHeading___Toc469_2258805889)

[2.2. Datasäkerhet inom traditionella datasystem och IoT 4](#__RefHeading___Toc471_2258805889)

[2.3. Datasekretessens roll i nätuppkopplade system 5](#__RefHeading___Toc473_2258805889)

[2.4. Potentiella säkerhetsrisker och attackmetoder för IoT 6](#__RefHeading___Toc475_2258805889)

[3. Metoder för garanterande av datasäkerhet och datasekretess inom IoT 9](#__RefHeading___Toc477_2258805889)

[3.1. Fysisk säkerhet, en förutsättning för alla datasäkerhetsåtgärder 9](#__RefHeading___Toc654_2481017766)

[3.2. Användarnas säkerhetspraxis 9](#__RefHeading___Toc479_2258805889)

[3.3. NFC-baserad autentisering med asymmetrisk kryptering och digital signatur 11](#__RefHeading___Toc481_2258805889)

[3.4. Metoder för upprätthållande av datasekretessen 16](#__RefHeading___Toc483_2258805889)

[4. Slutsatser 18](#__RefHeading___Toc823_1007979479)

[5. Källor 19](#__RefHeading___Toc825_1007979479)

# 1. Introduktion

Ursprungligen skapades vad vi nu kallar internet för att möjliggöra kommunikation över långa distanser mellan datorer, med hjälp av relativt enkla meddelanden. Under årtiondenas lopp har internet utvecklats till någonting som kan användas för i stort sett alla tänkbara typer av datakommunikation, från enkla textbaserade kommunikationsmetoder såsom e-post, ända till nätbaserade plattformar, där man kan ladda upp och komma åt ett praktiskt taget obegränsat utbud av filmer, videor, foton och andra typer av digitala medier. En annan utveckling som skett är att nätet inte endast används av vad som kunde kallas traditionella datorer. Även andra typer av apparater har nämligen börjat utvecklas för att dra nytta av att det finns ett enkelt, standardiserat sätt att möjliggöra datakommunikation överallt där det kan ge produkten någon fördel över icke-uppkopplade alternativ.

Benämningen IoT, som framöver kommer att användas, härstammar från engelskans Internet of Things som på svenska kallas sakernas internet. Termen används vanligen för att beskriva alla slags apparater med nätverksuppkoppling som inte kan klassas som traditionella datorer. Till traditionella datorer räknas i IoT-sammanhang de vanliga bordsdatorerna samt de bärbara datorerna, men även vissa enheter som klarar av att utföra lika mångsidiga och komplicerade uppgifter, däribland surfplattor och smarttelefoner. Det är värt att notera att det inte finns någon exakt definition för vilka typer av enheter som anses höra till IoT, och somliga personer väljer till exempel även att kalla smarttelefoner för IoT-enheter. De som däremot alltid klassas som IoT-enheter är andra typer av nätverksuppkopplade föremål och maskiner, som i allmänhet har en mera specifik roll. Ett bra exempel på en sådan enhet som är skapad för att utföra en specifik uppgift och använder sig av en nätverksuppkoppling är en termostat, som kan justeras via nätet.

En sak som måste tas i betraktande, då allt fler apparater är uppkopplade till och skickar data över nätet, är att dessa data i vissa fall inte får falla i fel händer. Det innebär att man precis som i traditionella it-system måste ta hänsyn till datasäkerhet och datasekretess, då man utvecklar kommunikationsprotokoll och hårdvara för IoT. En annan sak som många vill vara medvetna om, är vilken information som dessa IoT-enheter samlar in och skickar ut till olika aktörer, samt hur informationen i slutändan används. En mindre hederlig IoT-aktör kunde exempelvis utnyttja sensorer och andra metoder i sina produkter för att samla in helt annan information än man kunde förvänta sig av en dylik enhet, för att sedan sälja vidare informationen till marknadsföringsföretag och andra som kan utnyttja informationen på olika sätt.

En av grundtankarna bakom IoT är att de nätverkskopplade apparaterna ska kunna kommunicera med varandra för att uppnå sina mål. En garagedörr kan till exempel tända lamporna i huset då man kommer hem, medan lamporna kan använda externa ljussensorer för att justera sin ljusstyrka utifrån det verkliga ljusbehovet i rummet. Dessa saker leder till de frågor som denna avhandling kommer att undersöka. Den största frågan är hur man kan göra det möjligt för IoT-enheter att kommunicera med varandra utan hinder i de situationer där det är meningen att de ska få göra det, medan datasäkerheten upprätthålls och datakommunikationen hålls skyddad mot olika typer av attacker. På samma gång måste även användarvänligheten hållas på en sådan nivå att en normal användare ska kunna konfigurera och använda systemet utan någon specialkunskap. Avhandlingen är litteraturbaserad, och del av de saker som tas upp i är inspirerande av Alasdair Gilchrists bok IoT Security Issues [1]. I avhandlingen kommer olika faktorer som påverkar datasäkerheten och datasekretessen i traditionella datasystem och inom IoT att undersökas. Särskilt fokus kommer att läggas på ett exempel på en möjlig framtida autentiseringsmetod för kommunikation mellan IoT-enheter, som använder sig av en trådlös kommunikationsstandard med kort signalstyrka och räckvidd, kombinerat med asymmetrisk kryptering och digital signatur för att öka användarvänligheten och motverka vissa av de säkerhetsrisker som traditionella autentiseringsmetoder medför.

# 2. Bakgrund och motiveringar för avhandlingen

## 2.1 Termerna datasäkerhet och datasekretess

Då man börjar analysera vad termerna datasäkerhet och datasekretess i praktiken betyder, så kan det hända att man lägger märke till att det kan vara svårt att förstå skillnaden mellan de två termerna. Enligt IAPP, eller International Association of Privacy Professionals [2], står termen datasäkerhet för det skyddssystem för data som upprätthålls för att skydda det från missbruk, icke-auktoriserad användning och dylikt. Termen datasekretess står i sin tur för individers, gruppers och institutioners rätt att bestämma när och hur deras information används, samt med vilka andra aktörer som ska ha tillgång till deras information.

I praktiken är datasäkerheten ett förhandskrav för att datasekretessen ska kunna upprätthållas i ett datasystem, eftersom datasäkerheten till stor del finns till för att garantera att endast auktoriserade aktörer har tillgång till informationen eller datasystemet, samt att de endast har tillgång till den information eller de funktioner som de behöver. Datasäkerheten har dock även en annan roll än att detta, nämligen att skydda datasystemet från andra typer av attacker än sådana vilkas mål är att komma åt information. I ett traditionellt datorsystem kunde dessa attacker till exempel kunna ha som mål att orsaka skada i form av ekonomisk förlust, tidsförlust, dataförlust eller till och med fysiskt skadad hårdvara. Detta var fallet med Stuxnet, en internetmask, det vill säga ett datorvirus som sprids automatiskt från dator till dator genom nätverk, som blev världskänd inom datasäkerhetsindustrin då den upptäcktes. Stuxnets mål var nämligen att skada centrifuger som användes för uranberikning i Iran [3].

Termen datasekretess kan, förutom den ovannämnda bestämmanderätten över ens information, även behandla lagstiftning och övriga regelverk som bestämmer vilken information privatpersoner, företag och övriga organisationer får lagra om andra aktörer, och hur lagringen ska gå till. Ett aktuellt exempel på sådan lagstiftning är den europeiska General Data Protection Regulation, mera känd under förkortningen GDPR. Denna lagstiftning finns bland annat till för att skydda privatpersoners identifierande data från att lagras och användas utan den berörda personens personliga godkännande, medan den även ger personen rätt att kräva tillgång till informationen som lagras, att den raderas eller att dess användning begränsas [4].

## 2.2. Datasäkerhet inom traditionella datasystem och IoT

Innan man börjar tänka på risker och lösningar som berör säkerheten i vilket datasystem som helst, så måste man förstå vilka säkerhetsrisker som kan påverka systemet, och som man därmed behöver motverka. I allmänhet kan man påstå att ett datasystem behöver säkras för att se till att endast de personer som bör ha tillgång till information i systemet verkligen har tillgång till den. En annan viktig del av datasäkerheten är att se till att systemet inte kan manipuleras av icke-auktoriserade personer på sådana sätt som potentiellt kan orsaka problem av varierande grad av allvarlighet i datasystemet och hos eventuella maskiner som är kopplade till systemet. Detta är dock lite av en överförenkling, och orsakerna till att datasäkerheten och -sekretessen är viktiga att ta i betraktande i datasystem kan variera beroende på systemet i fråga. Det värsta som kan hända i vissa datasystem är att någon kommer åt en skolelevs senaste uppsatser, en temperaturavläsning utanför en byggnad eller någonting motsvarande. Medan denna typ av säkerhetsbrister kan anses vara irriterande, så är situationer som de ovan nämnda inte direkt sådana att de kan klassas som katastrofala händelser, till skillnad från följderna av motsvarande säkerhetsbrister i datasystem använda av företag, ett lands försvarsmakt och dylika organisationer. Hos dem kan en läckt fil eller tillgång till sensorer plötsligt orsaka stor ekonomisk skada, eller i militärens fall till och med påverka ett lands säkerhet och stabilitet.

Med andra ord så behövs datasäkerheten bland annat för att kunna garantera att affärs-, militär- och privata hemligheter inte läcker ut, för att stoppa datasystem från att kunna manipuleras av andra än dem som bör ha tillgång till sådana, för att garantera privat kommunikation och överhuvudtaget se till att den digitala informationen endast finns lagrad och tillgänglig där det är meningen att den ska vara det.

## 2.3. Datasekretessens roll i nätuppkopplade system

Datasekretessen är ett ärende som diskuterats en hel del i medierna under den senaste tiden tack vare GDPR, en uppsättning europeiska regler som behandlar lagring och användning av privat information inom Europa [4]. Det är viktigt att tänka på datasekretessen i dagens nätuppkopplade värld, eftersom de flesta individerna i dagens samhälle använder sig av nätet på daglig basis, vilket ger otaliga företag en möjlighet att ta reda på mera än man kanske skulle tro om enskilda personer. Denna information kan sedan lagras i företagens datasystem för att senare kunna användas inom företaget eller säljas till andra företag som i allmänhet är verksamma inom nätmarknadsföringsindustrin, och kan använda sådan information för att visa reklam som bäst lämpar sig för en specifik användares intressen. Detta är något som alla användare inte vill att deras information ska användas till, medan andra av olika orsaker helt enkelt inte vill att deras information överhuvudtaget ska få samlas in.

Oberoende av motiveringarna till att man inte vill att specifika företag ska få lagra ens personliga information, så är grundtanken i datasekretessen att man ska få bestämma över sin egen information. Detta är något som ofta kan gå emot företagens intressen då det bland annat försvårar marknadsföring och kommunikation med potentiella kunder, och därför kan man inte endast förlita sig på att företag ska agera i privatpersoners bästa intresse och garantera deras rätt till sekretess. Därför är lagar och regelverk såsom GDPR näst intill nödvändiga för att kunna garantera denna rättighet till att få bestämma över sin privata information.

Efter att frågorna om datasekretess har behandlats och en person har valt i vilken mån deras information får lagras och användas, så är det dags att lagra informationen i företagets datasystem. Här kan det återigen konstateras att datasäkerheten och datasekretessen har ett näst intill symbiotiskt förhållande, eftersom det nu är företagets uppgift att se till att informationens lagring garanterar att personens begränsningar för spridningen av informationen kan garanteras. Med andra ord så måste företagets datasystem vara tillräckligt säkert för att kunna garantera att endast användaren själv, och övriga som fått tillstånd att använda informationen, faktiskt har tillgång till den.

## 2.4. Potentiella säkerhetsrisker och attackmetoder för IoT

De flesta attackerna mot datasystem kan grupperas enligt målet bakom attackerna. I Threat Implications of the Internet of Things [5] delas de potentiella attackerna mot IoT-apparater upp i tre olika kategorier, baserade på deras mål. Den första typen av attacker som författaren tar upp är kapningsattacker. Dessa attacker har som mål att kapa system eller den information ett system behandlar. Dessa attacker kan till exempel ge attackeraren tillgång till ett nätverk genom att få tillgång till en otillräckligt skyddad IoT-enhet i nätverket, genom fysiska attacker såsom att koppla in hårdvara i nätverket eller genom en hel del andra metoder. Dessa attacker kan ha allvarliga konsekvenser, då de beroende på det aktuella datasystemet kan tänkas få tillgång till sekretessbelagd information som attackeraren sedan kan fortsätta med att samla in under en längre tid, ifall attacken inte upptäcks.

Följande typ av attacker som diskuteras är sådana attacker som har som mål att orsaka störningar och problem för attackens mål. Dessa attacker kan till exempel göras genom så kallade Distributed Denial of Service (DDoS) - attacker som har som mål att överbelasta enheten, eller nätverksanslutningen, som attacken är riktad mot. I allmänhet fungerar dessa attacker genom att en tillräcklig mängd nätverksförfrågningar skickas till attackens mål, för att förbruka så mycket nätverks- eller processorresurser för att datasystemet inte längre ska ha tillräckliga resurser för att kunna fungera normalt [6]. Medan dessa attacker inte i allmänhet innebär att någon information läcker ut, så kan de ändå orsaka ekonomisk skada och andra problem som kan uppstå då datakommunikationen i det påverkade datasystemet störs. Det finns även fall där dessa DDoS-attacker använts för att distrahera från en annan attack [7].

Den tredje och sista attacktypen som författaren tar upp är vad han kallar manipuleringsattacker. I dessa attacker är målet att komma åt att manipulera ett IoT-systems funktionalitet genom att i någon del av dataflödet komma åt att ändra på informationen som apparaterna försöker skicka till varandra eller till externa servrar. Dessa attacker kan till exempel vara så kallade man-i-mitten-attacker [8], där man avlyssnar nätverkskommunikationen och kan ersätta informationen som skickas med sin egen för att påverka ett system. Även dessa attacker kan ha stora konsekvenser då de kan få datasystem att göra alldeles andra saker än de borde göra. Sådana attacker kan i värsta fall påverka digitala röstningar, militära datasystem eller andra säkerhetskritiska system, eller orsaka allvarliga dataläckor.

Alla attacker är beroende av olika slags säkerhetsbrister i systemet som attacken riktar sig mot, och därför är det viktigt att vara medveten om vilka potentiella attackvektorer det kan finnas i ett datasystem. Då man vet detta, så kan man börja analysera ett system för att identifiera på vilka sätt det specifika systemet kan tänkas attackeras och hur säkert det behöver vara, så att man vet vilka säkerhetsåtgärder som är lämpade för implementering i systemet. Det är praktiskt taget omöjligt att skriva en komplett lista över alla tänkbara faktorer som kan påverka säkerheten i ett system, men till exempel kan användarnas säkerhetspraxis, dåliga lösenord, brist på säkerhetsuppdateringar för systemet eller enheten, otillräcklig kryptering och nätverkssäkerhet och dålig fysisk säkerhet nämnas som några av de viktiga sakerna man bör tänka på.

# 3. Metoder för garanterande av datasäkerhet och datasekretess inom IoT

## 3.1. Fysisk säkerhet, en förutsättning för alla datasäkerhetsåtgärder

En av datasäkerhetens grundpelare är att ett datasystem måste vara tillräckligt väl skyddat för att endast auktoriserade personer ska kunna få fysisk tillgång till datasystemets enheter och nätverk. Orsaken till detta är egentligen väldigt simpel, eftersom en person med fysisk tillgång till systemet inte nödvändigtvis överhuvudtaget påverkas av hur säker själva mjukvaran i enheterna är, eller av olika typer av datasäkerhetsåtgärder som gjorts i nätverket. Då man har fysisk tillgång till systemet så kan man helt enkelt byta ut all hårdvara som är ”för säker” för att få tillgång till systemet, installera sin egen mjukvara på enheter, installera sina egna enheter i nätverket, orsaka fysisk skada eller helt enkelt direkt stjäla de enheter där informationen, som man vill ha, finns lagrad. Det är med andra ord viktigt att komma ihåg att den fysiska säkerheten är en förutsättning för att de flesta av de härefter presenterade lösningarna ska kunna vara så effektiva som möjligt då det gäller att garantera datasäkerheten och datasekretessen inom IOT-system.

## 3.2. Användarnas säkerhetspraxis

En viktig aspekt inom datasäkerheten, som är lätt att glömma bort, är användarsäkerheten, och hur viktigt det är att användarna av ett datasystem är medvetna om deras roll för att upprätthålla datasäkerheten. Det har gjorts undersökningar där man tagit reda på i hur stor del av alla datasäkerhetsintrång som användarna har varit en bidragande faktor. I en sådan undersökning som utförts av det kanadensiska företaget Shred-it, konstateras det att över 40% av alla rapporterade säkerhetsintrång åtminstone delvis berott på mänskliga misstag [9].

Till säkerhetsriskerna, som användarna genom sitt agerande kan skapa, hör bland annat olika problem med lösenordssäkerheten, däribland återanvändning av lösenord för många tjänster eller datasystem, för enkla eller allmänt kända lösenord (1234, password, ett allmänt känt födelsedatum eller dylikt) och otillräckligt hemlighållande av lösenord som annars kunde vara tillräckligt säkra [10]. Det finns även många användare som aldrig ändrar, eller ens är medvetna om att de borde ändra, standardanvändarnamn och lösenord som enheterna har då man köper dem, vilket kan leda till att utomstående som känner till tillverkarens standardinloggningsuppgifter kan komma åt enheten väldigt lätt [1]. Dessutom finns det även de klassiska nätfiskeattackerna, som går ut på att på olika sätt lura användarna till att ge ut sina inloggningsuppgifter eller annan hemlig information, och de minst lika välkända virusinfekterade filerna i e-postmeddelanden, som på något sätt övertygar användaren om att öppna filen för att infektera datorn eller nätverket.

Vissa av de aspekter av användarsäkerheten som är viktiga i traditionella datasystem är kanske mindre relevanta i IoT-system, medan andra kan vara desto mer viktiga. I stort sett gäller ändå samma principer med hänsyn till lösenordssäkerhet och tillräcklig skolning av användarna för att de ska kunna identifiera vanliga attacktyper och undvika dem. Då det kommer till IoT-enheter, som är avsedda för användning i hemmiljön så kan det dock vara väldigt svårt att lära användarna viktiga säkerhetsprinciper. Därför är det bättre att, genom intelligenta designval, försöka eliminera specifika säkerhetsrisker, så användarnas handlingar för med sig mindre risk för säkerhetsproblem. Problemet med standardinloggningsuppgifter på enheter är väldigt lätt att lösa genom att helt enkelt se till att enheten kräver att de byts ut mot säkrare användarnamn och lösenord i det skede då de tas i bruk, och på samma gång kan användaren introduceras till hur man skapar säkra lösenord innan enheten kan börja användas. Hela problemet med lösenordssäkerhet kan även undvikas från första början till exempel genom att implementera den NFC-baserade autentiseringen som beskrivs nedan, eller genom motsvarande metoder som ser till att lösenord helt enkelt aldrig används i enheterna.

## 3.3. NFC-baserad autentisering med asymmetrisk kryptering och digital signatur

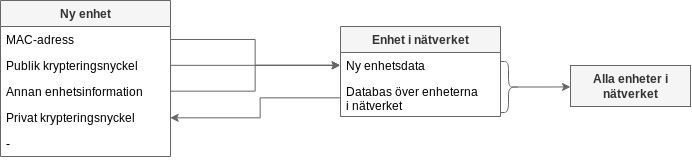
Ett sätt att minimera datasäkerhetsrisker, som beror på yttre faktorer såsom användare och deras datasäkerhetspraxis, dataläckor och dylika händelser som är utanför systemutvecklarens kontroll, kunde vara att använda ett autentiseringssystem som inte använder sig av klassiska lösenord för att koppla ihop enheter. I stället kunde ett autentiseringssystem utvecklas med hjälp av NFC-teknologin som presenteras nedan för parning av enheter, samt asymmetrisk kryptering och digitala signaturer för att möjliggöra säker kommunikation inom nätverk som byggs upp med detta autentiseringssystem.

Grundprincipen bakom asymmetrisk kryptering är att varje apparat, till skillnad från symmetrisk kryptering, har en privat krypteringsnyckel som endast enheten själv får känna till, samt en publik nyckel som är till för att dela ut åt alla, som behöver kunna skicka data till innehavaren av den privata nyckeln. Den publika nyckeln kan sedan användas för att kryptera data som endast innehavaren av den privata nyckeln kan dekryptera och läsa. I symmetrisk kryptering används däremot samma krypteringsnyckel både för kryptering och dekryptering. Med andra ord så är alla IOT-enheter som behöver kommunicera med en specifik enhet tvungna att få dess publika nyckel i ett system som använder sig av asymmetrisk kryptering [11].

NFC som står för engelskans Near Field Communication, eller på svenska närfältskommunikation, är en trådlös kommunikationsteknologi som är till för kommunikation på korta avstånd, med en maximal räckvidd på omkring 10 centimeter. NFC kan användas i antingen aktivt eller passivt läge, och skillnaden mellan dessa lägen är att båda enheterna som kommunicerar skapar sin egen signal och har en egen strömkälla i aktivt läge, medan det passiva läget fungerar genom att endast en enhet läser och skriver till en enhet utan egen strömkälla. Passiv NFC används bland annat i bankkort som tillåter kontaktlös betalning, och för den nedan beskrivna autentiseringsmetoden är aktiv NFC den relevanta teknologin [12].

Genom att använda NFC-teknologin kan användaren ta två IoT-enheter, trycka på en fysisk knapp för att koppla på parningsläget i enheterna och sedan lägga apparaterna bredvid varandra. Därefter kan enheterna skicka sina publika krypteringsnycklar och MAC-adresser, eller Media Access Control-adresser, som är en unikt identifierande adress för en fysisk nätverksenhet [2], till varandra via NFC. Därefter kan enheterna, med hjälp av dessa publika nycklar, kommunicera öppet med varandra då de kopplas till samma nätverk. I praktiken behöver Mac-adresserna skickas, eftersom många användare använder sig av dynamiskt allokerade IP-adresser, vilket gör det svårt att veta till vilken IP-adress som informationen ska skickas för att den ska nå rätt apparat. Då sändaren har mottagarens mac-adress lagrad, så kan den genom några olika metoder få reda på mottagarens IP-adress, förutsatt att mottagaren är kopplad till samma nätverk. Ett alternativ är att utnyttja ARP, eller Address Resolution Protocol för detta, då ARP är ett nätverksprotokoll som kopplar ihop fysiska MAC-adresser med digitala IP-adresser, och därmed gör det möjligt att hitta en specifik fysisk enhet i nätverket [13]. Ett annat alternativ är att alla enheter skickar ut periodiska meddelanden till alla enheter på nätverket för att berätta vilken enhet de är och vilken IP-adress de har.

Då man sedan vill utvidga nätverket till mer än två enheter, så blir det snabbt arbetsdrygt att behöva para ihop en ny enhet med varje enhet som finns i nätverket sedan tidigare. Därför är det bra ifall det räcker att en ny enhet som ska läggas till i systemet endast behöver paras ihop med en av de enheterna som redan finns i nätverket. Detta kan uppnås genom att den nya enheten gör samma typ av NFC-parning som ovan till en av enheterna i systemet, och den nya enhetens krypteringsnyckel och övrig information läggs till i den databas över publika nycklar och övrig information om alla andra enheter som finns på den enhet till vilken parningen görs. Denna enhet kan sedan efter parningen dela ut den nya versionen av tabellen till alla andra enheter i nätverket. Det lönar sig även att tidsstämpla tabellen, så enheter som till exempel varit avstängda vet ifall tabellen hos de andra enheterna är nyare än dess lagrade version. Se figur 3.3.A för en illustration över dataflödet.

*Figur3.3.A: Dataflödet mellan enheterna som paras ihop och övriga IoT-nätverket.*

Slutresultatet av detta är att alla enheter som tidigare lagts till i nätverket får tillgång till den nya enheten, och samma databas över publika nycklar kan redan i parningsskedet delas till den nya enheten, vilket möjliggör kommunikation mellan alla enheter inklusive den nya enheten som introducerats i systemet. Detta innebär att en av grundtankarna bakom IoT uppnås, nämligen öppen kommunikation mellan enheter, men som ändå möjliggör ett användarvänligt sätt att hantera autentiseringen samt krypteringen av datakommunikationen.

Ett problem finns dock kvar, om man lämnar systemet på denna nivå, eftersom tanken bakom asymmetrisk kryptering är att publika nycklarna per definition är publika, och det bör inte orsaka någon slags säkerhetsproblem ifall en sådan nyckel läcker ut ur vårt nätverk. I det här skedet förlitar sig systemet dock på att de publika nycklarna hålls hemliga och information krypterad med en av de publika nycklarna är från en enhet som man kan lita på. Därför behövs det någon metod för att verifiera identiteten på den enhet som krypterat och skickat informationen, för att se till att den verkligen är en av de enheter som lagts till i nätverket. Ett alternativ för att göra detta kunde vara att ha ett lösenord eller liknande unikt identifierande kod i varje enhet, som skulle läggas till i enhetsdatabasen som finns i alla enheter. Detta kan dock, särskilt om lösenorden kan modifieras av användaren, vara mottagligt för liknande säkerhetsbrister som ett traditionellt lösenordsbaserat autentiseringssystem. I stället kunde systemet använda sig av av en digital signatur för att verifiera att meddelandet som mottagits verkligen skickats av en av enheterna i systemet. Digitala signaturer använder sig av en enhets privata nyckel för att ”skriva under” den informationen som skickas. Denna signatur är sedan verifierbar med hjälp av den skickande enhetens publika nyckel, vilket betyder att enheten som mottagit någon information, kan bekräfta att meddelandet är underskrivet av en av enheterna som finns i databasen över auktoriserade enheter i nätverket. Detta innebär att systemet kan filtrera ut eventuell information som skickats av utomstående enheter som fått tag på en publik nyckel [14].

En fråga finns eventuellt ännu kvar, och det är huruvida en läckt, publik nyckel kan låta en utomstående läsa information som skickas inom nätverket. Detta borde dock inte vara ett problem, eftersom ett meddelande som skickas till en specifik enhet krypteras med den enhetens publika nyckel, innan meddelandet skickas ut på nätverket. Sedan kan endast mottagaren, med sin privata nyckel, dekryptera och läsa meddelandet [11].

Det finns tyvärr inga datasäkerhetsåtgärder som kan garantera total säkerhet, och ofta innebär förbättringar i användarvänligheten och användbarheten även att säkerheten försämras. Även den ovan beskrivna autentiseringsmetoden har sina brister. Medan NFC-teknologin gör systemet väldigt användarvänligt, så är det trots allt frågan om ett trådlöst kommunikationsprotokoll, och i teorin kan det gå att avlyssna datakommunikationen. Lyckligtvis gör signalens korta, 10 centimeters räckvidd detta väldigt svårt, men i teorin kan kommunikationen avlyssnas på lite längre avstånd [15]. I det här fallet är sannolikheten liten för att någon skulle lyckas avlyssna de enheter som använder denna autentiseringsmetod, eftersom den ovan beskrivna lösningen är ämnad för användning i hem och inom andra områden som allmänheten inte har tillgång till. Dessutom skulle avlyssningen behöva ske precis vid det skedet då parningsläget i två enheter kopplats på och information skickas mellan dem, eftersom det är den enda situationen där data skickas via NFC. Avlyssningen kunde dessutom försvåras ytterligare genom någon form av kryptering på själva NFC-kommunikationen. Förutom detta så kan den här autentiseringsmetoden även påverkas av faktorer som kan bryta säkerheten hos den asymmetriska kryptering som används. Något av det värsta som kunde ske vore att en eller flera av enheternas privata nycklar skulle läcka ut, vilket kunde ge en attackerare full tillgång till informationen som krypterats med den motsvarande publika nyckeln. Förutsatt att enheterna är programmerade så att de privata nycklarna inte under några som helst omständigheter ska gå att avläsa, och att endast auktoriserade användare har fysisk tillgång till enheterna, så bör de ovannämnda faktorerna inte i allmänhet påverka datasäkerheten negativt.

I Secured and Easy-to-Use NFC-Based Device Configuration for the Internet of Things [16] behandlas ett system för konfigurering av IoT-enheter som på vissa sätt påminner om den NFC-baserade autentiseringen. Där konstaterar författaren att ett av problemen inom IoT-industrin är den bristfälliga säkerheten i de system som används för att uppdatera mjukvaran i samt för att konfigurera IoT-enheter. I artikeln konstateras det även att säkrare sätt att hantera uppdateringen och konfigurationen har en tendens att påverka användbarheten negativt, och därför presenteras tre olika system som använder sig av NFC för att hantera de sakerna. Det av artikelns tre alternativ som mest påminner om den NFC-baserade autentiseringen, är vad författaren kallar “NFC-Based Configuration”, eller NFC-baserad konfiguration. Grundtanken där är att en nätverksuppkopplad telefon eller motsvarande enhet kan läsa IOT-enhetens ID, läsa in en korrekt konfiguration eller mjukvara från en server, och flytta över dem till IOT-enheten via NFC. Där används med andra ord NFC för att undvika osäkra nätbaserade konfigurerings- och uppdateringslösningar, som dessutom kan vara komplicerade att använda. Detta baserar sig i grund och botten på samma tankar som i den NFC-baserade autentiseringen, där informationen av samma orsaker flyttas mellan IoT-enheter, i stället för mellan en telefon och en IoT-enhet. I många fall kan även denna NFC-baserade konfiguration vara ett nödvändigt tillägg om IOT-enheten inte endast är en passiv sensor, som inte har stöd för någon som helst slags uppdateringar eller konfigurering. Som författaren konstaterar så är användarvänligheten hursomhelst en av fördelarna med ett NFC-baserat system, då det för de mest grundläggande operationerna endast kräver att enheterna placeras inom några centimeter från varandra, medan resten sköts automatiskt.

## 3.4. Metoder för upprätthållande av datasekretessen

Det är svårare att ge konkreta lösningar för hur datasekretessen kan garanteras inom IoT eller andra nätverkssystem, eftersom det i en högre grad än då det gäller datasäkerheten grundar sig på tillit. Användare måste helt enkelt kunna lita på att deras data används på de sätt som användaren gett tillåtelse till. Dessutom så är ju datasekretessen absolut beroende av god datasäkerhet, eftersom informationsläckor per definition innebär att datasekretessen inte kunnat upprätthållas. Förutsättningarna för att datasekretessen ska kunna upprätthållas, då datasäkerheten är tillräcklig, behandlas bland annat i Big Data Privacy in the Internet of Things Era [17].

För att upprätthålla datasekretessen är det första steget som den entitet som erbjuder en IOT-tjänst måste ta, att entiteten måste få användarens tillstånd till att få lagra och använda den information som det är frågan om. Då kan användaren kan göra ett informerat val beträffande vilken information som lagras, hur den används, vem som har tillgång till informationen och alla andra faktorer som användaren kan behöva veta. Problemet med många av de användaravtal som i dagens läge används är att de är väldigt långa och komplicerade, och ofta bara godkänns av användarna för att komma vidare i ibruktagningen av tjänsten eller produkten i fråga. Därför borde avtalen i stället finnas tillgängliga i ett sådant format som användarna realistiskt kan läsa och förstå, till skillnad från de nuvarande avtalen som främst lämpar sig för bruk av advokater i eventuella rättegångar. I vissa fall kan det även vara att ett företag helt enkelt bryter avtalet, eller utnyttjar något kryphål i avtalet för att göra andra saker än användaren trott med den data de fått tillgång till. Följande, precis lika viktiga steg som IoT-aktören i fråga behöver säkerställa är att användarna ska ha full kontroll över informationen som lagras. Med detta avses det att användaren själv ska kunna se, ladda ner, flytta eller radera all information gällande dem själva.

Eftersom datasekretessen till en så stor del är baserad på tillit, så är det viktigt att det finns olika slags regler och förordningar, som både ser till att användarnas rättigheter upprätthålls och håller företag och andra aktörer ansvariga, ifall de bryter mot dessa datasekretessförordningar. Ett aktuellt exempel på sådana förordningar är Europas GDPR [4], som presenterades kort i kapitel 2.3. Tack vare GDRP har man bland annat kunnat bötfälla vissa aktörer som inte följt datasekretessförordningarna. Det största fallet hittills har varit en bot på 50 miljoner euro som företaget Google förelagts av de Franska dataskyddsmyndigheterna [18].

En intressant egenskap hos IoT är att enheterna kan finnas stort sett var som helst, och samla in information med mikrofoner, kameror, trådlösa kommunikationsmetoder och diverse sensorer. Därför kan det vara i stort sett omöjligt att be varje individ som rör sig nära en IoT-enhet om tillstånd att använda eller lagra information som kan beröra dem. Till exempel så kan det finnas någon röststyrd enhet i en byggnad som konstant lyssnar på vad som sägs i omgivningen, vilket en besökare inte nödvändigtvis ens är medveten om. Sådana system skulle åtminstone behöva informera omgivningen om att de finns där genom varningsskyltar som berättar att de finns och vad de gör. Detta skulle göra det möjligt för en person att undvika området, ifall de inte vill att deras information ska lagras. I praktiken finns det, åtminstone för vissa typer av datalagring från omgivningen, någon typ av lagstiftning som begränsar hur detta får ske och hur informationen får användas. I Finland finns det till exemel lagstiftning som berör kameraövervakning på arbetsplatser [19].

# 4. Slutsatser

Det är i praktiken omöjligt att lista alla tänkbara säkerhetsåtgärder som kunde göras i ett IoT-system, eftersom det till exempel konstant skapas nya kommunikationsprotokoll och -metoder och nya typer av enheter, medan användarnas beteende även utvecklas. Man kan inte heller alltid nödvändigtvis implementera alla idéer som kunde göra ett givet system så säkert som möjligt, eftersom saker som kan öka datasäkerheten även kan ha en negativ inverkan på systemets användbarhet och funktionalitet. Ett klassiskt exempel på detta är att en lagringsenhet är väldigt säker, om den är inlåst i ett kassaskåp vars nyckel förstörts, utan elektricitet eller kontakt till något nätverk, men en sådan lösning gör det även närapå omöjligt att komma åt informationen på lagringsenheten.

Även denna NFC-baserade autentiseringslösning har vissa potentiella brister, precis som de flesta andra säkerhetsåtgärder. Till exempel så finns det i den ovan beskrivna funktionen ingenting som stoppar en person med fysisk tillgång till en av enheterna från att lägga till en ny enhet i systemet, vilket till exempel kunde motverkas genom att kräva lösenord för att koppla på parningsläget. I det här fallet var målet dock att göra systemet så användarvänligt som möjligt, och göra sig av med lösenord och andra försvårande faktorer. I allmänhet kan det konstateras att det lönar sig att utforska vilka faktorer som kan orsaka säkerhetsproblem i just det system som man vill säkra, och implementera tillräckliga säkerhetsåtgärder av olika typ för att försöka säkra alla attackvektorerna.

Vad datasekretessen beträffar så kan det konstateras att den i en väldigt stor utsträckning är beroende av och ett resultat av tillräcklig datasäkerhet. Även lagstiftning och avtal mellan tjänster och användare är dock viktiga faktorer för att garantera att användarna är medvetna om och kan bestämma var och hur deras information används. Om företag kunde använda, sälja och dela ut användarnas personliga information utan begränsningar eller användarnas kännedom, så skulle hemlig information snabbt kunna läcka ut till och missbrukas av obehöriga aktörer. Detta kunde medföra potentiellt katastrofala resultat för de användare, företag och övriga organisationer vars information fallit i fel händer, vilket är varför GDPR och motsvarande regelverk har en stor roll i vårt moderna, nätkopplade samhälle.

# 5. Källor

[1] A. Gilchrist, *IoT Security Issues*, Boston: DEG Press, 2017.

[2] International Association of Privacy Professionals, ”Glossary of Privacy Terms”, *International Association of Privacy Professionals*. [Online]. Tillgängligt: <https://iapp.org/resources/glossary/>. [Läst 3 januari, 2019].

[3] D. Kushner, ”The Real Story of Stuxnet”, *IEEE Spectrum*, 26 februari, 2013. [Online], Tillgängligt: <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/>. [Läst 3 januari, 2019].

[4] European Comission, ”Data Protection”, *European Comission*. [Online]. Tillgängligt: <https://ec.europa.eu/info/law/law-topic/data-protection_en>. [Läst 3 januari, 2019].

[5] M. Covington och R. Carskadden, ”Threat implications of the Internet of Things” i 2013 5th International Conference on Cyber Conflict (CYKON 2013), 2013, Tillgängligt: <https://ieeexplore.ieee.org/document/6568380>. [Läst 5 januari, 2019].

[6] K. Stefanidis och D. N. Serpanos, ”Countermeasures Against Distributed Denial of Service Attacks” i 2005 IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2005. Tillgängligt: <https://ieeexplore.ieee.org/document/4062170> [Läst 8 mars, 2019]

[7] S. Shead, ”Symantec: Data-stealing hackers use DDoS to distract from attacks”, *zdnet.com*, 9 Oktober 2012 [Online]. Tillgängligt: <https://www.zdnet.com/article/symantec-data-stealing-hackers-use-ddos-to-distract-from-attacks> [Läst 20 mars, 2019]

[8] M. Ordean och M. Giurgiu, ”Towards securing client-server connections against man-in-the-middle attacks” i 2012 10th International Symposium on Electronics and Telecommunications, 2012. Tillgängligt: <https://ieeexplore.ieee.org/document/6408076> [Läst 8 mars, 2019]

[9] Shred-it, ”State of the Industry”, [www.shredit.com](http://www.shredit.com/), 2018. [Online]. Tillgängligt: <https://www.shredit.com/getmedia/b5de58fd-7e17-4d18-b718-9eca8d0665a6/Shred-it-2018-North-America-State-of-the-Industry.aspx?ext=.pdf> [Läst 8 mars, 2019]

[10] A. Adams och A. Sasse, ”Users are not the enemy”, Communications of the ACM, vol. 42 n. 12, s. 40, 1999. Tillgängligt: [http://discovery.ucl.ac.uk/20247/2/CACM%20FINAL.pdf](http://discovery.ucl.ac.uk/20247/2/CACM FINAL.pdf) [Läst 8 mars, 2019]

[11] N. Saini, N. Pandey och A. Singh, ”Enhancement of security using cryptographic techniques” i 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) ( Trends and Future Directions), 2015. Tillgängligt: <https://ieeexplore.ieee.org/document/7359224> [Läst 8 mars, 2019]

[12] N. Shobha, K. Aruna, M. Bhagyashree och K. Sarita, ”NFC and NFC payments: A review” i 2016 International Conference on ICT in Business Industry & Government (ICTBIG), 2016. Tillgängligt: <https://ieeexplore.ieee.org/document/7892683> [Läst 8 mars, 2019]

[13] IBM, ”Address Resolution Protocol”. [Online]. Tillgängligt: <https://www.ibm.com/support/knowledgecenter/en/ssw_aix_71/com.ibm.aix.networkcomm/protocols_addr_resolution.htm> [Läst 21 mars, 2019]

[14] J. Shang, ”A study on application of digital signature technology” i 2010 International Conference on Networking and Digital Society, 2010. Tillgängligt: <https://ieeexplore.ieee.org/document/5479249> [Läst 21 mars, 2019]

[15] H. Kortvedt och Stig Mjølsnes, ”Eavesdropping Near Field Communication” i The Norwegian Information Security Conference (NISK), 2009. Tillgängligt: <https://www.researchgate.net/publication/265976861_Eavesdropping_Near_Field_Communication> [Läst 21 mars, 2019]

[16] T. Ulz, T. Pieber, A. Höller, S. Haas och C. Steger, ”Secured and Easy-to-Use NFC-Based Device Configuration for the Internet of Things”, IEEE Journal of Radio Frequency Identification, vol. 1 n. 1, s. 75, mars 2017. Tillgängligt: <https://ieeexplore.ieee.org/document/8019776> [Läst 21 mars, 2019]

[17] C. Perera, R. Ranjan, L. Wang, S. Khan och A. Zomaya, ”Big Data Privacy in the Internet of Things Era”, IT Professional, vol. 17 n. 3, s. 32, Juni 2015. Tillgängligt: <https://ieeexplore.ieee.org/document/7116422/> [Läst 22 mars, 2019]

[18] J. Porter, ”Google fined €50 million for GDPR violation in France”, *theverge.com*, 21 januari, 2019. [Online]. Tillgängligt: <https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil> [Läst 25 mars, 2019]

[19] ”Lag om integritetsskydd i arbetslivet”, Finlands Lag, 759/2004, 5 kap, 16§ och 17§. Tillgängligt: [http://www.finlex.fi/sv/laki/ajantasa/2004/20040759#L5](http://www.finlex.fi/sv/laki/ajantasa/2004/20040759" \l "L5) [läst 28 mars, 2019]