Fakulteten för teknik och samhälle
Datavetenskap

Examensarbete
15 högskolepoäng, grundnivå

Internet Of Things – risker, integritet och möjligheter till skydd

Internet of things – risks, integrity issues and the possibilities of protection

Stefan Allirol-Molin
Xheniza Gashi

Examen: Kandidatexamen 180 HP
Huvudområde: Data- och informationsvetenskap
Program: Informationsarkitekt
Datum för slutseminarium: 2017-01-12

Handledare: Nancy Russo

Sammanfattning

Internet of things (IoT) är en snabbt växande teknik som sakta men säkert kommit att spela en stor roll i individens vardag. IoT har blivit populär i olika områden såsom smarta hem och e-hälsa. IoT har blivit populär inom olika områden såsom smarta hem och e-hälsa. Tillit är en viktig komponent i varje interaktion vi gör ute på nätet. Då fler och fler enheter kopplar upp sig väcker det frågor om den personliga integriteten. Syftet med denna uppsats är att undersöka riskerna, möjligheterna och integriteten med Internet of things, samt att ta reda på om konsumenterna är medvetna om eventuella risker. Litar konsumenterna på IoT-enheterna, och i så fall vad gör de för att skydda sig ifrån att deras personliga data hamnar i fel händer? Vi har använt oss av enkäter för att bilda en uppfattning om hur konsumenter uppfattar denna teknologi. Resultatet indikerar att väldigt få litar på IoT-tjänster och att de inte har tillräckligt med kunskap om säkerhetsåtgärder kring IoT-tjänster samt att många upplever att säkerheten hos IoT- enheter är låg. Trots konsumenternas oro över säkerheten med IoT-saker, så verkar de dock anse att fördelarna överväger de potentiella riskerna.

Abstract

Internet of things (IoT) is a fast-growing technology that is slowly but surely coming to play a major role in an individual's life. IoT has become popular in different areas such as smart homes and e-health. Trust is an essential component of every interaction we do on the net. As more and more devices get connected, it raises questions about privacy. The purpose of this study is to investigate the risks, opportunities and the integrity of the Internet of Things and to find out if consumers are aware of the risks. Do they trust IoT devices, and if so, what do they do to protect themselves from their personal data falling into the wrong hands? We have used questionnaires to form an idea of how consumers perceive this technology. The result indicates that few trusts IoT services, and that the participants do not have enough knowledge about security measures surrounding the IoT services. Many feels that the security of IoT devices are low. Despite consumer concern regarding the safety with IoT things, it seems, however, that they believe that the benefits outweigh the potential risks.

Innehåll

Ordförklaring

- **Internet of Things (IoT):** vardagsföremål som hushållsapparater, kläder och accessoarer men även maskiner, fordon och byggnader som har försetts med inbyggda elektroniska delar, såsom sensorer, datorer och internetuppkoppling vilket gör att föremålen kan spara och utbyta data
- **Wi-Fi**: teknik för trådlösa nätverk
- **Bluetooth:** eller Blåtand, är en standard som tagits fram för trådlös kommunikation mellan olika enheter, som till exempel en mikrofon eller tangentbord och en dator
- **DVR (Digital Video Recorder):** en liten videospelare med inspelningsfunktion (oftast i form av inbyggd hårddisk)
- **Smartphone:** en kombinerad mobiltelefon och handdator som kan användas som personlig digital assistent (PDA)
- **DDOS (Distributed Denial of Service):** en teknik som används genom att ett stort antal datorer deltar i attacken. Den kan därmed inte effektivt avvärjas genom att begränsa trafiken från enskilda IP-adresser.

1. Introduktion

Digitaliseringen har lett till ett skifte i hur människor sköter sina vardagliga sysslor. Den nya tekniken ger användarna möjligheten att koppla upp sina tv-apparater, vitvaror och träningsutrustning mot Internet. [1] Användaren kan kontrollera säkerheten i deras hem via sina smartphones eller ta reda på vilka matvaror som de behöver köpa, detta genom en sensor som finns i deras kylskåp och känner av när mjölkpaketet börjar bli tomt, denna teknik heter Internet of Things (IoT) på svenska kallas det för sakernas Internet [2]. Enligt Chen [3] finns många säkerhetsutmaningar med IoT men det finns även möjligheter. Internet of things kan med fördel förbättra vardagslivet [4]; från smarta hem, smarta telefoner till att leva i ett helautomatiskt hem där användaren kan styra allting från sin smartphone [4, 5]. Men att endast vara uppkopplade är inte det vad Internet of things innebär, utan kommunikationen mellan enheterna och användningen av insamlade data är det som gör IoT användbart för världen. Kele och Scott [4] säger att vi befinner oss i en tid där helt vanliga produkter kan kommunicera med varandra, det samlas in data och uppgifterna utförs på användarnas kommando [6].

1.1 Problematisering

Aktörer som Ericsson och Cisco uppskattar att ca 50 miljarder saker kommer att vara uppkopplade mot Internet [7]. I takt med att allt fler enheter blir uppkopplade mot Internet växer så gör även säkerhetsfrågor och integriteten [3]. Enligt Maras så har det redan stött på integritetshot genom användningen av genomträngande tjänster och produkter [8]. Medan fler saker blir uppkopplade mot Internet blir säkerheten ofta bristfällig eller icke existerande. vad kan göras/görs för att skydda data ur integritetssynpunkt. Vad kan hända om man delar med sig av för mycket information? Är användarna medvetna om dessa risker? I och med att Internet of Things är ett aktuellt ämne, fann vi att det var intressant att undersöka och analysera riskerna utifrån konsumentens perspektiv och ta reda på hur de gör för att förhindra obehöriga från att göra intrång i deras personliga sfär eller erhålla deras personliga data.

1.2 Syfte

Denna uppsats har i syfte att undersöka riskerna som IoT enheter medför och användarnas medvetande om dessa. Med så många olika saker som kopplas upp mot Internet så tror vi att riskerna är stora för att privatlivet kan kränkas då personliga och privata data kan hamna där det inte är önskvärt eller ursprungligen tänkt. Det kan även vara av vikt att tillverkare av IoT-saker har kännedom om användarnas/konsumenternas uppfattning av riskerna, och dels kunna tillverka säkrare produkter, men

även bättre kunna förmedla information och kunskap till deras kunder om hur de (kunderna) säkert och tryggt kan använda tillverkarnas produkter.

1.3 Forskningsfrågor

Vi vill ta reda på:

- Är konsumenterna medvetna om att det finns risker med IoT enheter?
- Vilka risker finns med IoT enheter ur konsumentperspektivet?
- Vad gör konsumenterna själva för att säkra sina personliga data?

1.4 Avgränsning

Internet of Things är ett brett område där det sker ständigt forskning och utveckling om hur dem ska bearbeta problem som är relaterad till säkerhet och risker på IoT – enheter. Forskning pekar på att det finns säkerhetsutmaningar med Internet of things och att användarna kan råka ut för godtyckliga attacker [1, 9, 10]. I dagsläget är IoT ett hett område och det diskuteras flitigt bland media om hur användarna och deras personliga data ofta hamnar i orätta händer vid användning av IoT enheter [11]. Därför valde vi att göra en enkät för att få en uppfattning om människor vet riskerna med IoT produkter och vilka åtgärder de tar för att förhindra obehöriga från att göra intrång. Vi valt att lägga fokus på den personliga integriteten, tillit och riskerna på IoT-plattformar utifrån konsumentens perspektiv. Då det finns många användningsområden inom IoT då tyckte vi att det var relevant att avgränsa oss till smarta hem och E-hälsa, som är sådana saker som människor använder dagligen. Dessa delar (smarta hem och e-hälsa) beskriver vi mer i detalj under sektion 3.2.

2. Metod

2.1 Metodval

Som forskningsmetod för uppsatsen valde vi bland-studie (mixed method) där vi dels gick igenom den litteratur som redan finns inom vårt valda område, men även genomförde en online enkät (via Google Forms) för att försöka ta reda på vad konsumenterna själva egentligen tycker om ämnet.

2.2 Metoddiskussion

Det största skälet till att vi valde denna metod (en litteraturstudie först och en undersökning efteråt) var att vi gjorde bedömningen att genomförandet av en litteraturundersökning först lättast skulle kunna hjälpa oss att identifiera de risker (och möjligheter) som finns med/inom IoT, så att vi sedan (när vi genomförde vår undersökning) bättre kunde veta vilka frågor som var lämpliga att ställa till våra respondenter.

Enligt Ejlertsson [9] finns det både fördelar och nackdelar med denna metod. Genom att gå igenom de undersökningar som redan gjorts inom ämnet, så fick vi dels en förståning om vilka frågor som var lämpliga att ställa i vår egen undersökning, men också vad som gjorts/görs tidigare och nu inom vårt valda ämne. Fördelar med denna metod gentemot andra metoder, är att genom kombinerandet av en enkät (vänd till de som ämnet berör direkt) samt genomläsning av tidigare forskning inom det valda området, så ökar vi chanserna att både få in mer relevant (och då framförallt mer aktuell) information från de som berörs av vår forskningsfråga (i vårt fall konsumenter) utöver det som andra redan har forskat fram tidigare. Bland nackdelarna med att använda en enkät finns dels att vi måste formulera frågorna så att det är klart för testpersonerna vad vi frågar efter (och eliminera felaktiga svar/missförstånd), men också att tiden för arbetet med uppsatsen förlängs då vi måste invänta svar från testpersonerna innan vi kan vara någorlunda säkra på de slutsatser vi senare kommer dra gällande forskningsfrågan. Bland fördelarna med att använda en enkät finns möjligheten till ”öppna frågor”, det vill säga möjligheten för respondenterna att beskriva själva vad de gör, och genom att ge oss svar vi inte hade förväntat oss få (utifrån förväntade resultat från tidigare genomförda studier), därmed ge oss möjligheten till ny kunskap.

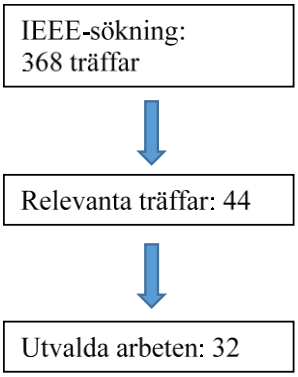
2.3 Litteratursökning

En litteratursökning gjordes för att hitta existerande kunskap inom ämnet men också bygga en teoretisk referensram. Vi använde databaserna ACM, IEEE, Science direct och Google scholar.

Arbetet började med att en sökning utfördes via databasen IEEE (se figur 1*: IEEE-sökning*) med sökorden

- Internet of things
- privacy
- integrity
- security
- consumers

Sökningen begränsades till 2015 och framåt, inkluderat patent och citat (men exkluderat böcker) samt sorterad efter relevans.



Figur 1 – IEEE-sökning

Utifrån de träffar (369 stycken) denna sökning gav (se figur 1: *IEEE-sökning*) så valdes 44 arbeten ut som potentiella för detta arbete. Utav dessa 44 arbeten bedömde vi sedan att 32 stycken var direkt relevanta för frågorna, och på de utvalda 32 arbetena utfördes sedan en litteraturstudie där ambitionen var att se om en lösning redan finns tillgänglig som kan lösa dessa frågor eller om mer forskning krävs. Vi utförde även samma sökning i databasen ACM, men då denna sökning endast genererade 3 träffar totalt så bedömde vi att den databasen inte passade våra syften.

2.4 Genomförande

Efter att ha gått igenom och sorterat ut alla de artiklar som vi bedömde vara relevanta för vårt arbete, så gick vi sedan ordentligt igenom de arbeten som vi valde att fokusera extra på.

2.5 Enkätundersökning

2.5.1 Pilotstudie

Ejlertsson säger att syftet med en pilotstudie [9] är att se om de som svarar på enkäterna tolkar frågorna på samma sätt som frågekonstruktörerna avsett. Frågorna måste därför testats i en provundersökning innan de används i den egentliga studien. Detta förs för att säkra så att enkätfrågorna uppfattas rätt av de svarande och om det saknas svarsalternativ.

Sammanlagt var det 44 personer som svarade på vår pilotstudie. Förundersökningen påbörjades med att vi delade ut enkäten till arbetskamrater och vänner, och därefter upptäckte vi brister med frågorna. Bland bristerna fanns bland annat fråga 1: *Känner du till/har hört talas om begreppet/uttrycket "Internet of Things" (även kallat IoT*). Då denna var lite otydlig (och vi riskerade att tappa dem som inte känner till begreppet men använder sådan enheter) så valde vi att i början på enkäten lägga till en introducerande text och en video som beskriver kort om vad IoT innebär, Detta gjorde vi för att säkerhetsställa att vi dels skulle få med dem som verkligen vet vad IoT är, men även de som känner till tekniken men inte begreppet (till exempel de som använder någon form IoT-enheter utan att de tänker på de)t. Vi upptäckte även att vi behövde lägga till frågan ”*Vad gör du själv för att skydda din personliga/privata information som finns lagrad i enheterna du använder*” för att kunna besvara en annan av våra forskningsfrågor och få en bild av vilka åtgärder användarna vidtar för att skydda sin egen data.

2.5.2 Huvudstudie

För att även få med vad vanliga konsumenter tyckte i ämnet, så genomförde vi en online undersökning (via Google Forms). För att öka våra chanser till svar, så valde vi (enligt Ejlertsson [9] en av fördelarna med att använda online-enkäter) att ge de som besvarade undersökningen möjligheten att besvara undersökningen helt anonymt. Skälet till detta val (anonymitet) var att vi bedömde att respondenternas vilja att besvara potentiellt känsliga och/eller personliga frågor borde öka om de visste att ingen kunde veta exakt vem som besvarat frågorna. En nackdel med denna typ av undersökning är dock att man exempelvis vid användning av ja/nej-svar måste vara väldigt noga med hur frågorna utformas [12]. Detta då alla frågor inte är lämpliga som rena ja/nej-frågor och en viss gradering av svaren (såsom “ja alltid”, “ja ibland” och så vidare) kan vara önskvärd. Det finns även en risk med undersökningar online att samma

person skulle kunna besvara enkäten flera gånger, men vi bedömde att Googles användning av “cookies” (som används för att se om samma dator/webbläsare besökt sidan innan) borde förhindra detta.

2.6 Insamlingsmetod

Undersökningen gick till på så vis att vi frågade alla vänner och bekanta via mejl och Facebook om de ville besvara vår undersökning. Då vi ville försöka få ett stickprov (se Ejlertssons bok kapitel 2) [9] utav den del av befolkningen som var bekant med ämnet för uppsatsen, så utformade vi enkäten på så vis att den första frågan var om testpersonerna kände till begreppet IoT över huvud taget (se bilaga: *Figurer, Onlineundersökning: fråga 1*). Om en testperson då svarade att begreppet var helt okänt så sorterades denne bort direkt, vilket i sin tur medförde att vi bara fick svar från de som på något vis var bekanta med begreppet. Därefter fick testpersonerna besvara en fråga om hur säkra de bedömde att de olika enheterna som finns inom IoT var/är (se bilaga: *Figurer, Onlineundersökning: fråga 7*), för att på så vis få någon form av svar på den andra delen av vår frågeställning. Resultatet av denna undersökning (med eventuella svar på vad konsumenterna gör för att själva säkra dessa enheter samt om detta påverkar deras beslut vid eventuella inköp av IoT-enheter) tar vi sedan upp i resultatdelen i slutet av denna uppsats.

2.7 Källkritik

Alla de vetenskapliga artiklar som har tagits fram är relevanta för vårt ämne och fattarna är experter inom området Internet of Things. De vetenskapliga artiklar vi valde att ta med var begränsat till 2015 och framåt då vi dels vill definiera begrepp men även vi vill ha aktuell information om de risker och hot som finns i nuläget. Artiklarnas tillförlitlighet och relevans för det berörda ämnet har undersökts genom att vi har vi granskat författarna och dess bakgrund och var deras artiklar är publicerade. Vi har också använt oss av IDG.se som Internetkälla då det anses vara ett pålitligt tidningsförlag där allt som skrivs är inom ämnet IT och av individer som behärskar området.

2.8 Validitet och reliabilitet

Enligt Ejlertsson är det naturligt att ifrågasätta om det erhållna resultatet är korrekt med det menas att om det med säkerhet mäter någon viss variabel [9] Validitet och Reliabilitet kan ses som två mått på studiens trovärdighet [13]. Validitet innebär att en studie eller fråga med hög validitet innebär att de mäter det som den avser ska mäta [9]. Reliabilitet innebär att vid upprepade mätningar får inte samma resultat. D.v.s. att de som har svarat har uppfattat frågorna rätt.

För att säkerhetsställa så att rätt frågor ställs till respondenterna så utförde vi en pilotstudie för att kontrollera om vi får in relevant data men också om respondenterna har tolkat frågorna rätt. Frågorna som utformades med hjälp av Ejlertssons litteratur och tidigare forskning ökar pålitligheten genom att liknande metod har utförts och att vår pilotstudie bekräftar reliabilitet genom att vi fick in liknanden värden som den egentliga enkäten.

3. Teoretisk bakgrund

3.1 Vad är Internet Of Things?

Internet of things (även kallat IoT) är alla de vardagsföremål såsom hushållsapparater, kläder och accessoarer, men även maskiner, fordon och byggnader, som har försetts med inbyggda elektroniska delar, (såsom sensorer, datorer och internetuppkoppling) vilket gör att föremålen kan sammankopplas fysiskt eller via trådlöst nätverk (*se Figur 2: Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things*) och därefter utbyta data (med varandra och/eller olika system) [9].

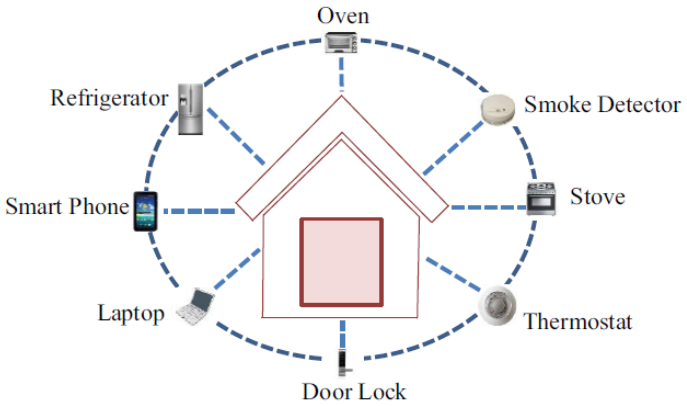


Fig. 2: Smart-Home with inter-linked Things

Figur 2: Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. Publicerad med upphovsrättsinnehavarens tillstånd

3.2 Möjligheter med IoT

Nedan kommer några användningsområden inom IoT presenteras. Det visar möjligheterna och potentialen med IoT-system.

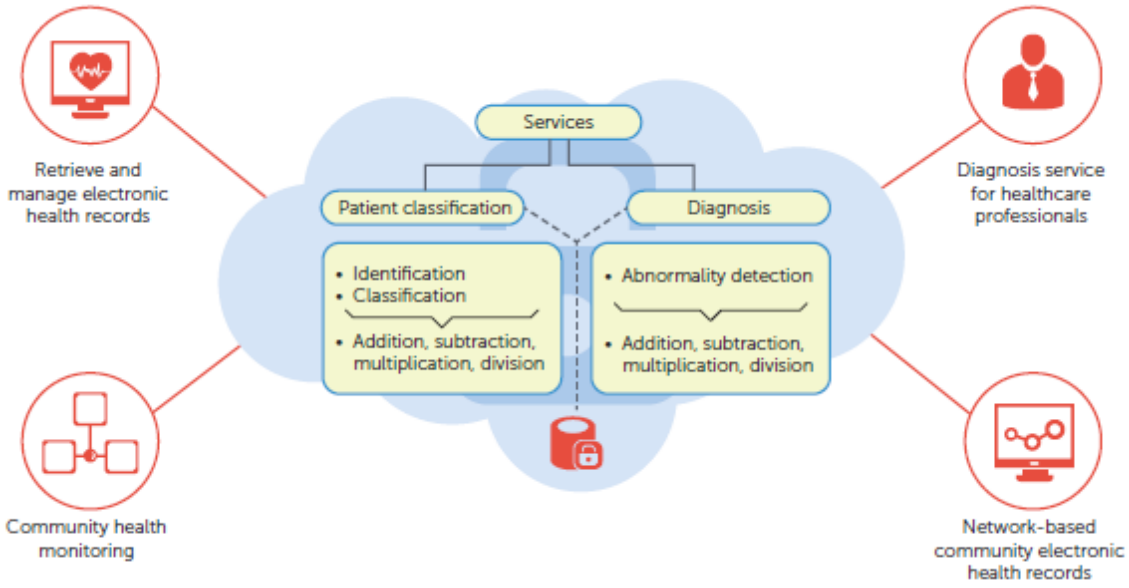
Smarta hem: Smarta hem har länge varit attraktiva, [5] Med Internet of Things tekniken behöver inte människans bekvämlighet i offras, inbyggda sensorer kan förstå och justera lufttemperaturen eller minska belysningen för att minska energi [3]. En annan möjlighet är också att kaffebryggare varnar när pulvret är lågt så nytt beställs in, eller kylskåp som känner av via sensor när mjölken börjar ta slut och beställer in nytt. Utöver detta så skapar denna teknik trygghet för individen, där de kan övervaka sina hushåll och blir varnad om problem som kan vara kostsamma. Alla husägare kan undersöka/övervaka deras ström och vattenförbrukning [5].

Sjukvård: Ett användningsområde där IoT kan tillämpas är sjukvården. IoT tekniken har gett upphov till flera möjligheter till många medicinska tillämpningar som övervakning av hälsotillstånd, kroniska sjukdomar, och äldreomsorg [13]. Individer med diabetessjukdomen kan få en s.k. blodglukos-bevakning som avslöjar patientens mönster, och detta kan vara till hjälp vid planering av måltider, aktiviteter och medicinering. Man kan utföra EKG-övervakning på distans (patienten kan exempelvis vara hemma eller på arbetet) där man på en avläsningscentral kan observera hur hjärtslagen hos patienterna slår för att kunna sedan upptäcka avvikande hjärtrytm [14]. Smarta produkter som smartphones, klockor och andra biobaserade ”wearables” är exempel på sådana enheter som kan ge personlig vård och öka livskvalité. [5], och dessa IoT - baserade hälso- och sjukvårdstjänster förväntas reducera kostnader inom vården och öka livskvalitén samt ge en bra användarupplevelse [14, 10].

3.3 Riskerna med IoT?

Eftersom inte alla tillverkare av enheter verkar ta säkerhet på så stort allvar som vore önskvärt (enligt bland annat Matherly, skaparen av sökmotorn Shodan) [15], så tillkommer även vissa säkerhetsrisker med alla enheter som nu kopplas upp mot nätet. Det finns olika exempel såsom babymonitorer (där användarkontot är av standardtyp med användare = admin och lösenord = password, 123456, blankt (inget lösenord) eller har ett hårdkodat lösenord som inte går att ändra, (se bilaga *Figurer: Figur 8 - Babymonitors - flaws*) [16] (vilka sedan kan användas för att övervaka om någon är hemma) DVR-enheter (inspelare av tv-program) [16] eller IP-kameror som kan användas i DDOS-attacker mot andra sidor/tjänster [17]. Ett exempel på detta är när drygt 147 000 infekterade DVR-enheter och IP-kameror användes för att överbelasta en Minecraft-server som fanns hos den franska förvaltningsfirman OVH. Denna attack skedde på så vis att varje enskild enhet kunde skicka mellan 1 till 30 megabit data per sekund (vilket gav en total belastning på drygt 1,5 terabit data) vilket i sin tur var mer än vad systemet var designat att hantera [17].

Andra riskområden är smarta system för strömförbrukning eller larm [18] som (om de hackas) kan avslöja om/när någon är hemma och/eller kan användas för att bryta sig in utan att förstöra någon dörr/fönster under intrånget. Även inom området e-hälsa finns det risker, som att den information som inte borde spridas till de som inte borde/skall ha tillgång till personlig hälsoinformation kan (om enheten/enheterna hackas) användas för att antingen missbruka denna information mot individen i sig och/eller användas för att ta reda på information om verksamhetens system och/eller nätverkets sammansättning (se figur 3: Sammansättning av hälsoinformation nedan) [19].



Figur 3: Sammansättning av hälsoinformation. Publicerad med upphovsrättsinnehavarens tillstånd

4. Resultat

I detta avsnitt kommer materialet presenteras från de enkäter som utfördes av respondenterna. Vi har även med hjälp av litteraturen kunnat identifiera ett intressant område som personlig integritet.

4.1 Personliga integriteten - IoT

Några av de risker som en del varnar för med IoT enheter är de risker som kan finnas för den personliga integriteten. Ett exempel är så kallade RFID-taggar (nyckelbrickor) [20, 21] som används för in/utpassering. De listor som genereras vid användningen av dessa brickor skulle kunna användas till andra syften än att bara kontrollera om någon får komma in eller inte. Ett potentiellt scenario är ett försäkringsbolag som köper listan över ett hushåll för att se om de verkligen är hemma eller inte (svårt att bevisa vid hushåll med fler personer men lättare med singlar) när de anmält sjukdom. En annan risk är ex. de smarta tv-apparater/smarta klockor [22, 23 som blivit mer och mer populära. Någon skulle kunna hacka sig in på enheten och genom att gå igenom vilka program någon tittat använda denna information för att bygga upp en bild av vad personen gillar och potentiellt använda den informationen för att hota skada en individs rykte om denne inte utför en viss handling (exempelvis identitetskapning där hackade uppgifter kan användas för att handla saker med den hackades kontokortsuppgifter som sedan levereras till hackaren eller en tredje part).

4.2 Användarnas perspektiv

Sammanlagt var det 31 personer som utförde enkäten. Majoriteten av de individer som svarade var 18–25 år gamla (dvs. 24 personer) och resterande 6 personerna var 35–54 (19,4%) 1 person som svarade var (55-70 3.2 %) (se Bilaga *Figurer: Onlineundersökning, fråga 2*). Denna form av undersökning gjordes för att få en uppfattning av vad användarna har för inställning till IoT kopplade enheter och tjänster, samt deras inställning till risker, integritet och de åtgärder som tar för att skydda deras personliga data. För att säkerhetsställa att användarna har någorlunda kunskap om området IoT är första frågan, ”Känner du till/har hört talas om begreppet/uttrycket "Internet of Things" (även kallat IoT)?” där användarna är tvungna till att veta vad IoT är för att besvara enkäten, detta för att få in relevant data.

4.2.1 Perception och bekantskap

Första frågan i undersökningen lyder ”Känner du till/hört talas om begreppet/uttrycket ”Internet of Things” (även kallad för IoT) ” (Se figur 4: Onlineundersökning, fråga 1 nedan och Bilaga *Figurer: Onlineundersökning, fråga 1*). Av de deltagare som svarade på enkäten var det 90 % som hade kännedom om IoT. De resterande 10 % av deltagarna har (troligen) inte hört talas om IoT. Detta innebär de 90 % som svarade att de känner till IoT förstår helhet med begreppet IoT (och att smarta objekt är en del av de begreppets innebörd), medan de 10 % som svarade att de inte kände till begreppet IoT inte vet vad termen IoT betyder men kan känna till vad smarta objekt är.

Figur 4: Onlineundersökning, fråga 1

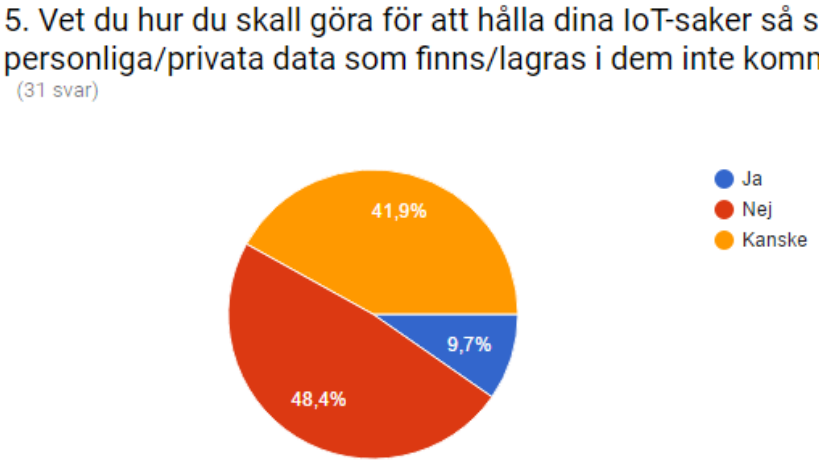
På frågan ”Hur stor kunskap skulle du säga att du har om vad Internet of Things är?” (se bilaga *Figurer: Onlineundersökning, fråga 3*) svarade 15 personer (48,4 %) att de har en viss kunskap om vad det är, 9 personer (29 %) svarade att de har en aning om vad det är, 6 personer (19.4 %) svarade att de har full kunskap om det är och 1 person som svarade att de inte hade en aning om vad det är.

4.2.2 Användarnas syn på säkerhetsrisker – IoT

Enligt vår undersökning så anser flertalet (41 %) av respondenterna att säkerheten är god på IoT-enheter (se bilaga Figurer: Onlineundersökning, fråga 7), men samtidigt litar bara 17 % på dem tillräckligt för att vilja lagra personlig/privat information på dem (se bilaga *Figurer: Onlineundersökning, fråga 8*).

På frågan ”Hur god säkerhet tror du att sakerna/enheterna har (på en skala mellan 1 till 5 där 1 är inte säkert alls och 5 är väldigt säkert)?” (Se bilaga *Figurer: Onlineundersökning, fråga 7*) valde 13 av respondenterna (41.9 %) att kryssa in på skala 3 vilket tyder på att människor känner sig kluvna över säkerhet som IoT produkter och tjänster har.

På frågan ”Vet du hur du skall göra för att hålla dina IoT-saker så säkra att den personliga/privata data som finns/lagras i dem inte kommer i orätta händer?” (Se figur 5: Onlineundersökning, fråga 5 nedan och bilaga *Figurer: Onlineundersökning, fråga 5*) svarade 15 personer (48.4 %) nej, 13 personer (41.9 %) svarade kanske, och 3 (9,7 %) personer svarade ja vilket stämmer bra överens med de som svarade på frågan.



Figur 5: Onlineundersökning, fråga 5

På frågan ”Vad gör du själv för att skydda din personliga/privata information som finns lagrad i enheterna du använder” svarade enbart 4 av de 31 respondenter som besvarade undersökningen vad för saker de gör för att försöka skydda sina personliga data. De fyra respondenterna svarade enligt följande. (Se bilaga *Figurer: Onlineundersökning, fråga 6*)

1. Respondent A
   ”Kryptera data.”

2. Respondent B
   ”Kryptering flera lager av säkerhet”

3. Respondent B
   ”Virusprogram på pc.”

4. Respondent C
   ”Använder bara https, gör inte mycket mer.”

Av de 31 respondenterna var det alltså bara 4 som valde att svara på denna fråga. Detta verkar alltså visa att det inte är så många som vet hur man skyddar sig från att deras personliga data hamnar i orätta händer, men det kan även tyda på att människor rent generellt inte bryr sig om olika säkerhetslösningar.

4.2.3 Användarnas åtgärder

Vår undersökning gav inget konkret svar på vad användarna rent generellt gör själva då enbart fyra personer besvarade den frågan. De som besvarade frågan angav dock kryptering som egen åtgärd (se bilaga *Figurer: Onlineundersökning, fråga 6*). Då enbart 4 av de 31 som besvarade undersökningen angett saker de gör för att försöka skydda sin privata/personliga information.

4.2.4 Tillit till IoT

På enkätfrågan “Litar du tillräckligt mycket på IoT-enheter för att vilja lagra din personliga/privata information på dem” (Se bilaga *Figurer: Onlineundersökning, fråga 8*) så svarade 14 personer (45.2%) att de kanske gjorde det, 11 personer (35,5%) svarade att de inte litar tillräckligt på IoT enheter och tjänster, och enbart 6 personer (19,4%) svarade att de litar tillräckligt mycket på IoT-enheternas säkerhet för att vilja lagra sina personliga data på dem. Detta verkar visa att majoriteten som svarade kanske känner sig kluvna på just denna fråga eller känner att de har inte tillräckligt med kunskap för att kunna ta ett sådant beslut.

Utöver de frågor som respondenterna skulle besvara, så kunde man även på sista frågan lägga till kommentarer (se bilaga *Figurer: Onlineundersökning, fråga 9*). Sammanlagt var det 4 personer som svarade och deras svar lyder:

1. Respondent A
   ” Jag vet hur man bör hålla sin privata data säker, men finns det säkerhetsbrister på min IoT device så är det ju dock svårt.”

Detta tolkar vi som att respondent A gör så gott denne kan för att skydda sig, men är begränsad i sina val utifrån eventuella brister som tillverkaren av enheten har i enheten.

2. Respondent B
   "Det är oklart vad som räknas som full kunskap eller viss kunskap om IoT. Filmen ger en bra överblick hur IoT fungerar och dess möjligheter men tar inte upp eventuella säkerhetsrisker vilket inte ger enkätdeltagaren en rättvis bild av IoT. Utan någon mer information om säkerhet kring IoT är det svårt att sätta sig in i frågan om man litar på IoT-enheter eller inte."

Detta tolkar vi som att respondent B menar att den film från Intel [24] som inleder undersökningen inte är tillräcklig för att bedöma eventuella risker som finns med IoT då detta inte tas upp i den filmen. Därmed blir det även svårt att besvara frågorna om säkerhet gällande IoT för den som inte har djupare kunskap om ämnet.

3. Respondent C
   "Är inte rädd att dela med mig av information om mig själv men är irriterad på att det fungerar som det gör och att andra kapitaliserar på information om oss. Men är för lat att egentligen bry mig om det eller känna att det spelar någon roll om jag delar med mig eller inte."

Detta tolkar vi som att respondent C inte är orolig för delning av information via IoT-enheter i sig, men att denne inte gillar att den kan säljas till tredje part utan att ha något att säga till om saken.

4. Respondent D
   "Jag anser att mina svar på frågorna skulle påverkas av flera faktorer. T.ex. vilken typ av enhet det handlar om, vilken leverantör som tillhandahåller enheten samt vilken och i vilket syfte datan lagras. Att göra informerade val i varje enskilt fall anser jag vara viktigt för min upplevelse samt ställning kring informationssäkerhet och lagring av information. Svaret på frågorna i enkäten är högst generella och kan inte appliceras på enskilda fall och min inställning till säkerhet och framförallt kunskap kring påverkan på säkerhet."

Detta tolkar vi som att respondent D gör så gott denne kan för att skydda sig på olika sätt utifrån vilken IoT-enhet det gäller. Däremot menar respondenten att de frågor vi ställt i undersökningen var/är för allmänna, och att vi troligen skulle få andra/olika svar om vi frågat om specifika enheter då säkerheten är olika från enhet till enhet.

4.2.5 Konsumenters medvetenhet om riskerna

Vår preliminära slutsats efter genomläsning av de olika utvalda arbetena (samt efter att ha genomfört vår online-undersökning) är att folk i allmänhet (48,4%) är medvetna om att det finns risker med IoT, men att de inte verkar ha den kunskap som krävs/behövs om hur de skall kunna säkra sina personliga/privata data (se bilaga *Figurer, fråga 5*) från att hamna i orätta händer (enbart 9 % säger sig vet hur de skall skydda sig).

4.2.6 Vad de gör själva för att minimera riskerna

De fyra som valde att lämna kommentarer har alla valt liknande lösningar, och det är någon form av kryptering av den data som lagrats/lagras i IoT-enheter. Valet av kryptering som skydd skulle kunna innebära att även om lagrad data i en IoT-enhet stjäls, så kan den som kommer över denna information inte utnyttja informationen så lätt då den är oläslig (och därmed oanvändbar) utan rätt dekrypteringsnyckel. En av respondenterna har valt ett antivirusprogram som skydd, vilket i sin tur skulle kunna innebära ett visst skydd mot exempelvis trojanprograms möjlighet att komma över den lagrade datan utan användarens vetskap.

5. Analys

5.1 Hur användarna uppfattar riskerna

Enligt en undersökning genomförd av Milykh, Vavilov, Platonov och Anisimov [22] så var många konsumenter (53 %) mer oroliga över privatlivs- och säkerhetsrisker än andra potentiella negativa saker med IoT. Även en undersökning genomförd av D. O'Brien, R. Budish, R. Faris, U. Gasser och T. Lin [1] pekar på detta, och vår egen analys av ämnet verkar indikera att detta stämmer generellt. Konsumenterna är oroliga över säkerheten med IoT-saker, men verkar anse att fördelarna överväger de potentiella riskerna (drygt 64,5 % (se bilaga: *Figurer, fråga 4*) överväger ett köp av en IoT-kapabel enhet inom de närmaste två åren).

5.2 Vad krävs från användarna

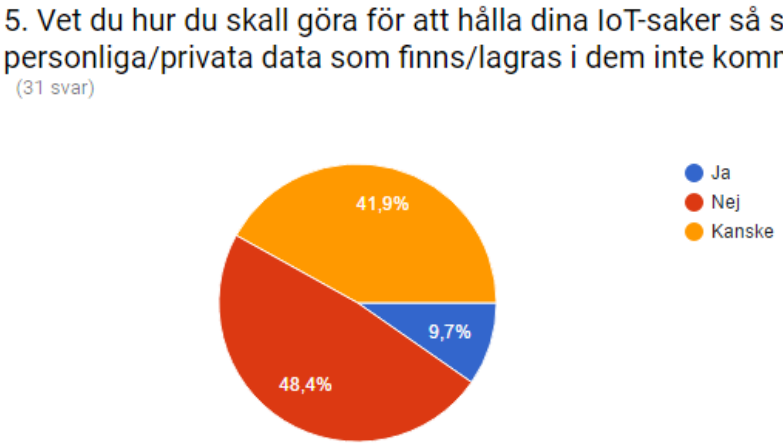
Utöver att sätta press på tillverkarna (genom att exempelvis inte köpa osäkra produkter (något som exempelvis John Matherly, grundare av sökmotorn Shodan förespråkar) [15] från tillverkare som inte tar säkerheten på allvar eller slarvar genom att ex. sätta standardlösenord (vilket BBC-News påpekade i sin artikel om babymonitorer) [16] på sina produkter) så är det vår uppfattning att en större riskmedvetenhet bör läras ut till konsumenterna via exempelvis arbetsplatser, vid försäljning av olika IoT-enheter eller via olika former av riskutbildningar (exempelvis genom allmänna studieförbund).

5.3 Användarnas Perception

En liknande studie som gjordes i USA (och som heter Securing the Internet of Things Survey), gjordes av SANS institute infosec Reading [25] men gentemot organisationer. Deras resultat gällande användarnas perception av IoT var att 58 % kände att de hade kunskap om IoT medan 27.7 % hade en aning om vad IoT är, vilket stämmer överens med det resultatet som vi fick in på vår enkät där 29 % angav att de har en aning om vad IoT är. Författarna pratar om att den höga nivån av respondenternas uppfattning och den låga nivån av deras kunskap visar tecken på självselektion att de som har besvarat enkäten har valt att utgå ifrån att dem sannolikt vet vad begreppet innebär [51]. SANS säger att om de hade tagit en bredare provtagning skulle resultatet sannolikt visa lägre kunskap om IoT. [25] Deras tolkning bekräftade vår tolkning att skulle vi göra en bredare undersökning med fler respondenter skulle de sannolikt visa att få människor inte vet innebörden av IoT och det bekräftas ytterligare av vår pilotundersökning (där vi hade 13 respondenter mer), där 31.8% inte kände till begreppet IoT och att 25 % har ingen kunskap om IoT. Detta kan som SAMS nämnde bero på att de som har svarat på enkäten sannolikt var erfarna inom området.

5.4 Säkerhetsrisker ur konsumenternas perspektiv

48,4% av de respondenter som svarade sade att de inte vet hur man skall hålla sina IoT enheter/tjänster och 41,9% svarade att de kanske vet hur man säkrar IoT enheter (se Figur 6: Onlineundersökning, fråga 5 nedan och bilaga *Figurer: Onlineundersökning: fråga 5*). Detta kan tolkas som att dem har lite kunskap om hur man skyddar sin personliga data men att de troligtvis inte har riktigt kunskap om hur man skyddar deras privata information.



Figur 6: Onlineundersökning, fråga 5

Trots att användarna svarade att säkerheten för IoT enheter/tjänster är relativt låg (se bilaga *Figurer: Onlineundersökning, fråga 7*), så var det ändå 25 % som svarade att de kommer köpa IoT-enhet och 64,5% överväger att inom två år köpa en IoT-enhet. Detta kan bero på att användarna inte riktigt inser riskerna och hur deras privata information kan användas, vilket kan vara en anledning till varför så många personliga intrång sker eller att utvecklarna inte bygger säkra system. Forskning visar också att det finns många säkerhetsrisker och att man försöker bearbeta de problem som är relaterade till säkerhet och risker på IoT – enheter.

5.5 Ytterligare skydd av konsumenternas data, vad kan göras?

Vi har tyvärr inte hittat så många sätt som en konsument själv kan ta för att säkra att ens personliga/privata information hamnar i orätta händer utöver de skydd som eventuellt finns inbyggt i IoT-saker. Att mer forskning behövs inom bland annat utbildning i riskmedvetande är dock helt klart nödvändigt, och detta särskilt om man tänker på den senaste tidens attacker på olika tjänster som skett med hjälp av olika IoT-enheter.

6. Diskussion

På detta avsnitt kommer vi inledningsvis diskutera studiens resultat och reflektera över vårt metodval och forskningsstrategi, nästkommande del diskuterar vi krav på användare och lösningsförslag.

6.1 Resultatdiskussion

Resultatet från vår studie och de faktorer som framkom utifrån analys visar att användarnas medvetande om risker och hot är relativt hög, och enkäten visar också användarna uppfattning om säkerheten med IoT enheter var låg. Användarna har då en möjlighet att påverka deras säkerhet och skydda sin privata information genom att ta säkerhetsåtgärder som att läsa policy och ifrågasätta insamling och hantering av information.

Vår studie visar att endast 4 av 31 personer som svarade, skyddar sin personliga data som är lagrade på deras IoT-enheter. Utifrån vår analys så tolkar vi det som att dem resterande 27 respondenterna inte vidtar några säkerhetsåtgärder vilket är oroväckande med tanke på att dem upplever att säkerheten för dessa enheter är låg.
Enligt Peppet [26] så upplever användarna att säkerhetspolicy och användarpolicy är förvirrande och svårlästa, det anges inte tydligt vem som äger användarnas data och vilken data som samlas men ändå pekar vår enkät att många av användarna inte bryr sig om att skydda sin data. Trots att användarna är medvetna om riskerna och 35,5% inte litade på IoT enheter så var det till vår förvåning 25 % som kommer att köpa IoT produkter dem två närmsta åren och 64.5% kanske kommer göra ett köp vilket kan tolkas som att de sannolikt kommer att göra detta, vår förväntning var att färre människor kommer att göra inköp av IoT och pga. enkäten visade att den upplevda säkerheten är relativt låg.

Enligt Peppet så ökar utveckling av antal IoT produkter eftersom dem eftertraktas och köps av konsumenterna, [13] Peppet nämner även att användarna inte tänker på enheternas negativa sidor utan att bekvämligheten oftast kommer i första hand [13]. Det kan förklara resultatet som vi fick på frågan litar du på IoT-enheter (se bilaga *Figurer: Onlineundersökning, fråga 8*). Alltså att användarna tänker mer på positiva med enheterna snarare än det negativa.

6.2 Metodreflektion

Vi valde att göra en litteratursökning som hjälpte oss besvara vår första forskningsfråga ”Vilka risker finns det med IoT enheter” sedan och för att besvara resterande forskningsfrågor utforma vi en enkät för att få en djupare förståelse för det faktiska

problemet men också tidsramen för arbetet. Innan vi gjorde den empiriska undersökningen gjorde vi en litteratursökning för att se vilka risker och hot det finns med IoT enheter. Under litteratursökning upptäcker vi att det inte finns mycket studier användarens synd kring IoT produkter, vilket vi ansåg var en svaghet och bidrog att vi begränsade oss till de få litteraturer som vi hittade.

Vi använde oss av en kvantitativ studie där flera respondenter kunde medverka, fördelarna med att utföra en enkät enligt Jacobsen är att de etiska aspekterna d.v.s. graden av anonymitet, det går inte att identifiera vem som har svarat vad. En annan fördel enligt Ejlertsson [9] är att man kan studera användarnas mönster i hur människor tänker och uppfattar frågor, vilket hjälpte oss under analysen att hitta faktorerna till varför användarna svarade som det gjorde.
Den kvantitativa studien bidrog till en större generaliserbarhet, och med det menas att området undersöktes mer på ytan. Vi anser att en kvalitativ ansats också borde ha tillämpats, där vi man hade utfört intervjuer med människor som är experter inom området för att förstärka vårt empiriska resultat. Enligt Jacobsen [27] så bidrar en kvalitativ ansats till att man forskare får en klarare och djupare förståelse för ämnet. Nu i efterhand insåg vi att vi hade kunnat öka äktheten genom att använda en kvalitativ ansats.

6.3 Krav på användaren

Eftersom användarnas kunskaper om riskerna med IoT-enheter och säkerheten på dessa varierar så är de krav man kan ställa på användarna även de olika, men det minsta man kan begära är att de innan de använder en enhet tar reda på vilken säkerhet som finns (och om det finns någon) på enheten, och vem som kan ha/få tillgång till den data som lagras på enheten. Det vore även önskvärt om användarna gick någon form av utbildning om riskmedvetande för IoT-enheter för att på så vis öka deras medvetande om vad som kan hända med den data som många idag lite aningslöst lagrar på enheterna.

Samtidigt som leverantörerna bör ha tydlig säkerhetspolicy och användarvillkor bör användarna också vara med kritiskt till de enheter som dem köper och granskar policyn innan dem accepterar då det ligger även på användarens ansvar för det som de väljer att dela med sig.

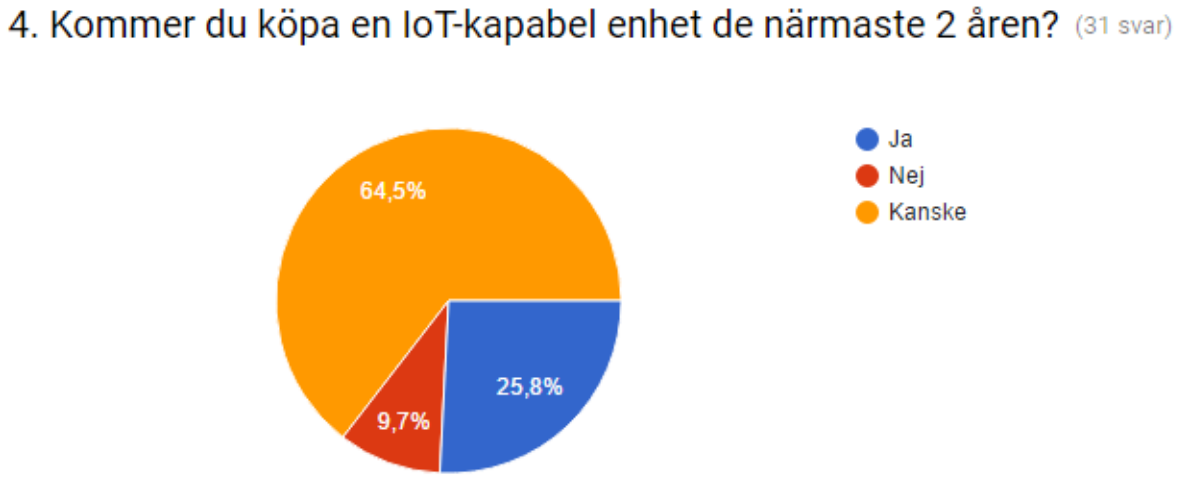
6.4 Lösningsförslag

Olika lösningar finns på de problem vi upplever med säkerheten med IoT och användarnas möjligheter att påverka denna, men en sak som kan göras är att användarna sätter press på tillverkarna av IoT-enheter att skärpa säkerheten på deras enheter ge-

nom att inte köpa enheter med ingen eller bristfällig säkerhet (samt meddela tillverkarna att man inte gjort ett köp av ovan nämnda orsak/orsaker). Utöver det har vi inte kommit på så många lösningar som berör användarna själva utan de flesta lösningar verkar ligga mer på tillverkarna eller möjligen på lagstiftarna.

7. Slutsats

Litteraturen och studien visar att användarna är medvetna om att säkerheten hos IoT enheter är låg, det indikerar också på att användarna spelar en stor roll när det gäller uppkomsten av intrång då det verkar som att många användare inte vidtar några åtgärder för att skydda sin personliga data. Trots att enkäten visar att dem är medvetna om riskerna så anser vi inte att det finns tillräcklig med kunskap om hur de skall skydda sina enheter. Vi kunde också med hjälp av litteraturen dra slutsats att användarna oftast accepterar säkerhetspolicyn och användarvillkor utan att dem begriper vad det är för data de delar med sig och hur det hanteras samt att de prioriterar funktionalitet mer än säkerhet. Vårt empiriska resultat visar att trots låg uppfattning om säkerhet överväger dem ändå att köpa IoT enheter (se figur 7: Onlineundersökning, fråga 4 nedan och bilaga *Figurer: Onlineundersökning, fråga 4*). Då bara 4 av 31 valde att kommentera vad de gör för att skydda sig (se bilaga *Figurer: Onlineundersökning, fråga 6*) så antar vi att de övriga litar på eventuellt befintligt skydd i IoT-enheterna.



Figur 7: Onlineundersökning, fråga 4

Vi har tyvärr inte hittat så många sätt som en konsument själv kan ta för att säkra att ens personliga/privata information hamnar i orätta händer utöver de skydd som eventuellt finns inbyggt i IoT-saker.

7.1 Vidare forskning

Att mer forskning behövs inom bland annat utbildning i riskmedvetande är dock helt klart nödvändigt, och detta särskilt om man tänker på den senaste tidens attacker på olika tjänster som skett med hjälp av olika IoT-enheter.

Litteraturförteckning

[1] D. O'Brien, R. Budish, R. Faris, U. Gasser och T. Lin,
”Privacy and Cybersecurity Research Briefing,” 01 09 2016. [Online].
Available: https://dash.harvard.edu/handle/1/28552575. [Använd 09 11 2016].

[2] Wikipedia, ”Sakernas internet,” 22 08 2016. [Online].
Available: https://sv.wikipedia.org/wiki/Sakernas_internet. [Använd 17 10 2016].

[3] Y. K. Chen, ”Challenges and opportunities of internet of things,” i *17th Asia and South Pacific Design Automation Conference*, Sydney, Australia, 2012.

[4] D. Scott och M. Ketel, ”Internet of Things: A useful innovation or security nightmare?,” i *SoutheastCon 2016*, Norfolk, USA, 2016.

[5] R. Alur, E. Berger, A. W. Drobnis, L. Fix, K. Fu, G. D. Hager, D. Lopresti, K. Nahrstedt, E. Mynatt, S. Patel, J. Rexford, J. A. Stankovic och B. Zorn, ”Systems Computing Challenges
in the Internet of Things,” 09 22 2015. [Online].
Available: http://cra.org/ccc/wp-content/uploads/sites/2/2015/09/IoTSystems Challenges.pdf. [Använd 09 11 2016].

[6] B. Wasik, ”In the Programmable World, All Our Objects Will Act as One,” Wired, 14 05 2013. [Online]. Available: https://www.wired.com/2013/05/internet-of-things-2/. [Använd 01 11 2016].

[7] C. Malm, ”Varningen: Stora integritetsrisker med Internet of Things,” 13 01 2015. [Online]. Available: http://www.idg.se/2.1085/1.604280/varningen--stora-integritetsrisker-med-internet-of-things. [Använd 01 11 2016].

[8] M. H. Maras, ”Internet of Things: security and privacy implications,” *International Data Privacy Law,* vol. 5, nr 2, pp. 99-104, 2015.

[9] K. N. Tongay, ”Sensor data computing as a service in Internet of Things,” i *2016 Symposium
on Colossal Data Analysis and Networking (CDAN)*, INDORE, India, 2016.

[10] S. M. Riazul Islam, D. Kwak och H. Kabir, ”The Internet of Things for Health Care: A Comprehensive Survey,” *IEEE Access,* vol. 3, pp. 678-708, 2015.

[11] IDG, ”Allt om Internet Of Things på IDG.se,” 19 05 2016. [Online]. Available: http://www.idg.se/2.1085/1.198072/internet+of+things. [Använd 4 10 2016].

[12] G. Ejlertsson, Enkäten i praktiken, Lund: Studentlitteratur, 2000.

[13] M. Björklund och U. Paulsson, Seminarieboken – att skriva, presentera och opponera, Lund: Studentlitteratur, 2003.

[14] Wikipedia, ”Radio Frequency Identification,” 26 08 2016. [Online]. Available: https://sv.wikipedia.org/wiki/Radio_Frequency_Identification. [Använd 17 10 2016].

[15] S. Nilsson, ”Shodan-skaparen om ddos-attackerna: sluta köpa usla uppkopplade prylar,” 28 10 2016. [Online]. Available: http://techworld.idg.se/2.2524/1.668377/shodan-skapare-usla-uppkopplade-prylar. [Använd 09 11 2016].

[16] BBC News, ”Web baby-monitoring cameras open to hacking, study warns,” BBC, 03 09 2015. [Online]. Available: http://www.bbc.com/news/technology-34138480. [Använd 01 10 2016].

[17] P. Oropeza, ”Armé av hackade smarta apparater utför kraftfulla attacker,” 27 09 2016. [Online]. Available: http://pcforalla.idg.se/2.1054/1.666204/arme-av-hackade-smarta-apparater-utfor-kraftfulla-attacker. [Använd 09 11 2016].

[18] M. Andersson och M. Rubenson, ”Inför säkerhetskrav på uppkopplade prylar för att skydda internets infrastruktur,” 24 10 2016. [Online]. Available: http://www.idg.se/2.1085/1.668122/uppkopplade-prylar-infrastruktur. [Använd 09 11 2016].

[19] S. Campanello, ”145000 hackade övervakningskameror bakom världens kraftigaste ddos-attack,” 29 09 2016. [Online]. Available: http://techworld.idg.se/2.2524/1.666468/hackade-overvakningskameror. [Använd 09 11 2016].

[20] L. Onita, ”Warning over 'internet of things' and privacy,” *Engineering & Technology,* vol. 10, nr 1, pp. 13-13, 2015.

[21] BBC, ”CES 2015: Warning over data grabbed by smart gadgets,” 07 01 2015. [Online]. Available: http://www.bbc.com/news/technology-30705361. [Använd 09 11 2016].

[22] V. Milykh, D. Vavilov, I. Platonov och A. Anisimov, ”User behavior prediction in the “offline”
smart home solutions,” i *Zooming Innovation in Consumer Electronics International Conference (ZINC), 2016*, Novi Sad, Serbia, 2016.

[23] J. Singh, T. Pasquier, J. Bacon, H. Ko och D. Eyers, ”Twenty Security Considerations for Cloud-Supported Internet of Things,” *IEEE Internet of Things Journal,* vol. 3, nr 3, pp. 269-284, 2016.

[24] *Internet of Things explained simply.* [Film]. USA: Intel.com, 2014.

[25] SANS Institute, “Sans,” 2014. [Online]. Available: https://www.sans.org/reading-room/covert/securing-internet-things-survey-34785. [Accessed 01 11 2016].

[26] S. R. Peppet, ”Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent,” *Journal of Texas Law Review,* vol. 93, nr 1, pp. 85-176, 2014.

[27] D. I. Jacobsen, Vad, hur och varför? Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen, Lund: Studentlitteratur AB, 2002.

[28] S. Sikari, A. Rizzardi, A. Griecco och A. Coen-Porisini, ”Security, privacy and trust in Internet
of Things: The road ahead,” *Computer Networks,* vol. 15, nr 01, pp. 146-164, 2015.

[29] IEEE, ”IEEE Xplore digital Library,” [Online]. Available: http://ieeexplore.ieee.org/search/searchresult.jsp?queryText=((((internet%20of%20things)%20AND%20privacy)%20AND%20integrity)%20AND%20consumers)&refinements=4291944822&refinements=4291944246&refinements=4294965216&refinements=4291944245&refinements=undefin. [Använd 01 10 2016].

[30] S. Campanello, ”Så använder hackare dina uppkopplade prylar i ddos-attacker,” 22 09 2016. [Online]. Available: http://techworld.idg.se/2.2524/1.665893/hackare-uppkopplade-prylar. [Använd 09 11 2016].

[31] S. Nilsson, ”Säkerhetsupprop mot internet of things: "Låt oss se källkoden!",” 27 01 2016. [Online]. Available: http://www.idg.se/2.1085/1.648532/iot-kallkod. [Använd 09 11 2016].

[32] S. Moore, P. Armstron, T. McDonald och M. Yampolskiy, ”Vulnerability analysis of desktop 3D printer software,” *Resilience Week (RWS),* pp. 46-51, 16-18 8 2016.

[33] M. Hossain, M. Fotouhi och R. Hasan, ”Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,” i *2015 IEEE World Congress on Services*, New York, USA, 2015.

[34] Y. Li, T. Nakasone, K. Ohta och K. Sakiyama, ”Privacy-mode switching: Toward flexible privacy protection for RFID tags in Internet of Things,” i *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, USA, 2014.

[35] S. Chakrabarty och D. W. Engels, ”A secure IoT architecture for Smart Cities,” i *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2016.

[36] M. A. Crossman och H. Liu, ”Study of authentication with IoT testbed,” i *Technologies for Homeland Security (HST), 2015 IEEE International Symposium on*, Washington, DC, 2015.

[37] Y. Sun, L. Wu, S. Li, T. Zhang, L. Zhang, J. Xu och Y. Xiong, ”Security and Privacy in the Internet of Vehicles,” i *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, Beijing, 2015.

[38] I. Alqassem och D. Svetinovic, ”A taxonomy of security and privacy requirements for the Internet of Things (IoT),” i *2014 IEEE International Conference on Industrial Engineering and Engineering Management*, Selangor, Malaysia, 2014.

[39] B. Tank, H. Upadhyay och H. Patel, ”A Survey on IoT Privacy Issues and Mitigation Techniques,” i *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, Udaipur, India, 2016.

[40] R. Selt, C. Yacine och N. Benblidia, ”Internet of things context-aware privacy architecture,” i *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, Marrakech, Morocco, 2015.

[41] M. Amadeo, C. Campolo, A. Iera och A. Molinaro, ”Information Centric Networking in IoT scenarios: The case of a smart home,” i *2015 IEEE International Conference on Communications (ICC)*, London, UK, 2015.

[42] K. Flittner, ”Surprised? Turns out, consumers don’t trust IoT security,” Auth0, 06 11 2015. [Online]. Available: https://auth0.com/blog/surprised-turns-out-consumers-dont-trust-iot-security. [Använd 09 11 2016].

[43] P. P. Ray, ”Generic Internet of Things architecture for smart sports,” i *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, Noorul islam University, India, 2015.

[44] W. Shi, J. Cao, Q. Zhang, Y. Li och L. Xu, ”Edge Computing: Vision and Challenges,” *IEEE Internet of Things Journal,* vol. 3, nr 5, pp. 637-646, 2016.

[45] N. Cam-Winget, A.-R. Sadeghi och Y. Jin, ”Invited: Can IoT be secured: Emerging challenges in connecting the unconnected,” i *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, Austin, USA, 2016.

[46] P. A. Laplante och N. L. Laplante, ”A Structured approach for describing healthcare applications for the Internet of Things,” i *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*, Milan, Italy, 2015.

[47] D. He, S. Zeadally, N. Kumar och J.-H. Lee, ”Anonymous Authentication for Wireless Body Area Networks With Provable Security,” *IEEE Systems Journal,* vol. PP, nr 99, pp. 1-12, 2016.

[48] S. Raza, P. Misra, Z. He och T. Voigt, ”Bluetooth smart: An enabling technology for the Internet of Things,” i *Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on*, Abu Dhabi, UAE, 2015.

[49] T. Shuhaili, N. L. Clarke och S. M. Furnell, ”An Analysis of Information Security Awareness within Home and Work Environments,” i *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, Reggio Calabria, Italy, 2010.

[50] M. Weber och M. Boban, ”Security challenges of the internet of things,” i *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2016.

[51] R. Want, B. N. Schilit och S. Jenson, ”Enabling the Internet of Things,” 04 01 2015. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.6666&rep=rep1&type=pdf. [Använd 01 11 2016].

[52] H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari och X. Yi, ”Secure Data Analytics for Cloud-Integrated Internet of Things Applications,” *IEEE Cloud Computing,* vol. 3, nr 2, pp. 46-56, 2016.

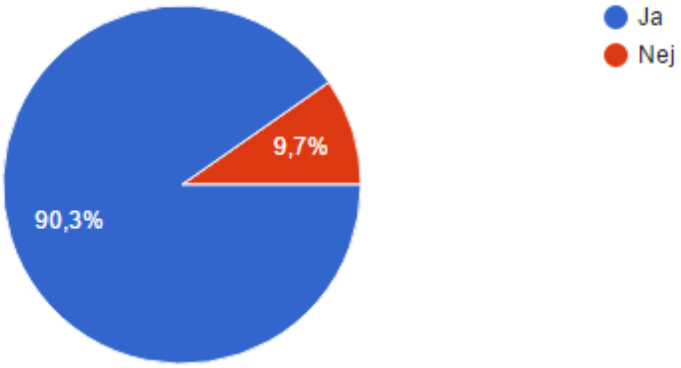
[53] CBC News, ”ISS 3D printer makes first part in space,” CBC News, 26 11 2014. [Online]. Available: http://www.cbc.ca/news/technology/iss-3d-printer-makes-first-part-in-space-1.2850833. [Använd 01 11 2016].

[54] L. Atzori, A. Iera och G. Morabito, ”The Internet of Things: A survey,” *Computer Networks,* pp. 2787-2805, 28 10 2010.

[55] A. Zanella, L. Vangelista, N. Bui och M. Zorzi, ”Internet of Things for Smart Cities,” *IEEE INTERNET OF THINGS JOURNAL,* vol. 1, nr 1, pp. 22-32, 2014.

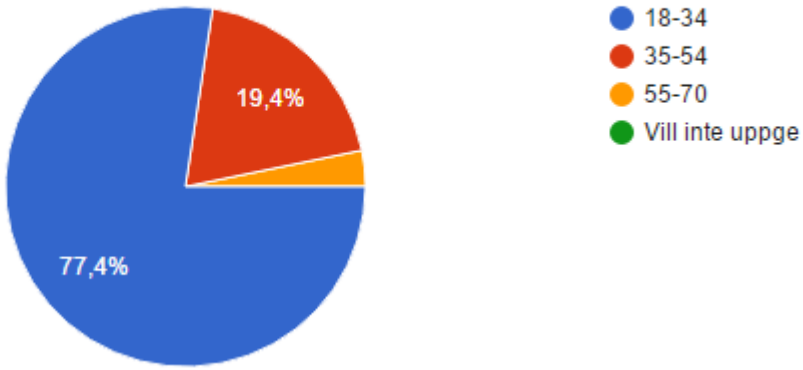
Bilaga figurer

1. Känner du till/har hört talas om begreppet/uttrycket "Internet of Things" (även kallat IoT)?
(31 svar)



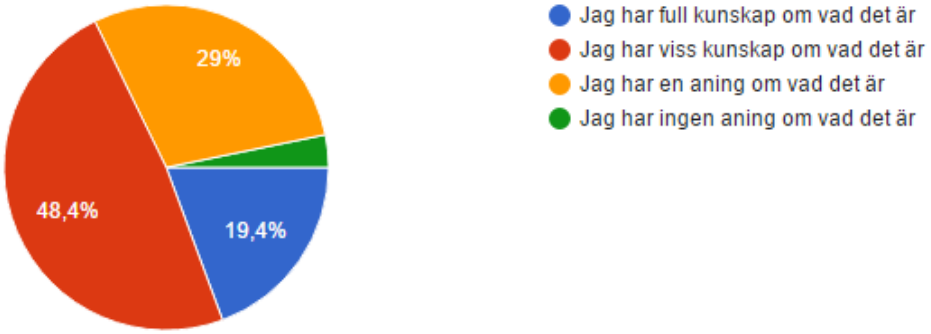
Onlineundersökning, fråga 1

2. Hur gammal är du? (31 svar)



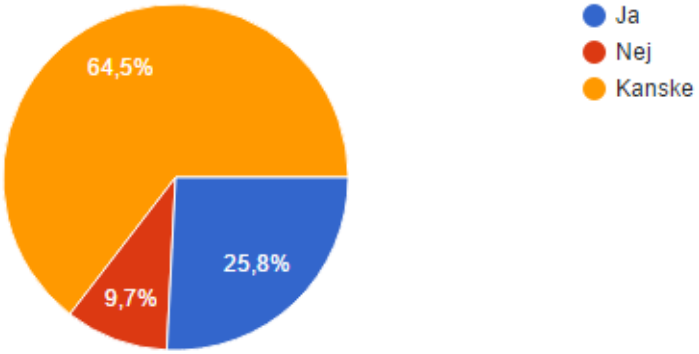
Onlineundersökning, fråga 2

3. Hur stor kunskap skulle du säga att du har om vad Internet of Things är?
(31 svar)



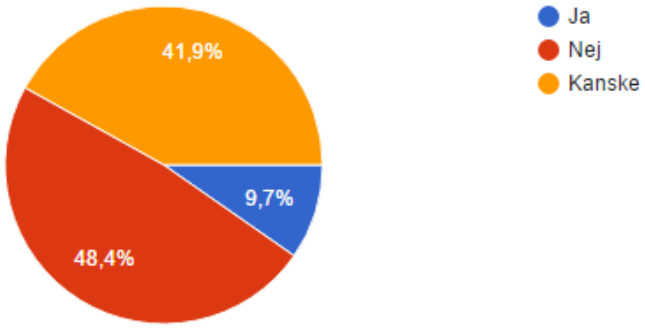
Onlineundersökning, fråga 3

4. Kommer du köpa en IoT-kapabel enhet de närmaste 2 åren? (31 svar)



Onlineundersökning, fråga 4

5. Vet du hur du skall göra för att hålla dina IoT-saker så säkra att den personliga/privata data som finns/lagras i dem inte kommer i orätta händer?
(31 svar)



Onlineundersökning, fråga 5

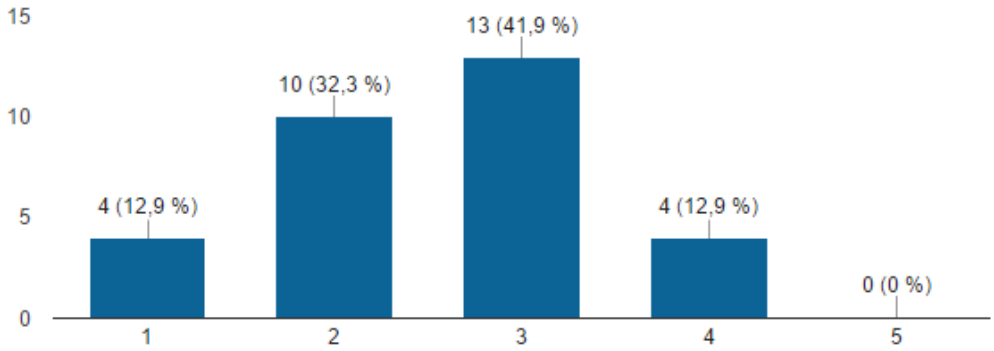
6. Vad gör du själv för att skydda din personliga/privata information som finns lagrad i enheterna du använder
(4 svar)

Krypterar data
Virusprogram på pc
använder bara https minst. gör inte mycket mer.
Kryptering. Flera lager av säkerhet

Onlineundersökning, fråga 6

7. Hur god säkerhet tror du att sakerna/enheterna har (på en skala mellan 1 till 5 där 1 är inte säkert alls och 5 är väldigt säkert)?

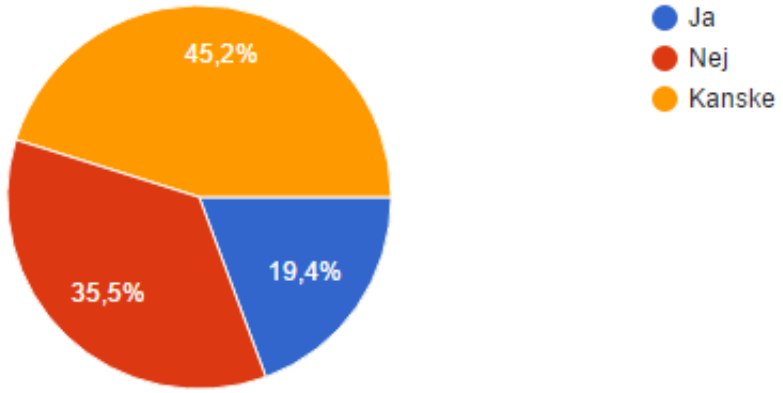
(31 svar)



Onlineundersökning, fråga 7

8. Litar du tillräckligt mycket på IoT-enheter för att vilja lagra din personliga/privata information på dem?

(31 svar)



Onlineundersökning, fråga 8

9. Något du vill tillägga? Var något oklart? (4 svar)

Det är oklart vad som räknas som full kunskap eller viss kunskap om IoT. Filmen ger en bra överblick hur IoT fungerar och dess möjligheter men tar inte upp eventuella säkerhetsrisker vilket inte ger enkätdeltagaren en rättvis bild av IoT. Utan någon mer information om säkerhet kring IoT är det svårt att sätta sig in i frågan om man litar på IoT-enheter eller inte.
Jag vet hur man bör hålla sin privata data säker, finns det säkerhetsbrister i min IoT device så är det ju dock svårt.
Är inte rädd för att dela med mig av informationen om mig själv men är irriterad på att det fungerar så som det gör och att andra kapitaliserar på informationen om oss. Men är för lat för att egentligen bry mig om det eller känna att det spelar någon roll om jag delar med mig eller inte.
Jag anser att mina svar på frågorna skulle påverkas av flera faktorer. Tex. vilken typ av enhet det handlar om, vilken leverantör som tillhandahåller enheten samt vilken och i vilket syfte datan lagras. Att göra informerade val i varje enskilt fall anser jag vara viktigt för min upplevelse samt ställning kring inflormationssäkerhet och lagring av information. Svaret på frågorna i enkäten är högst generella och kan inte appliceras på enskilda fall och min inställning till säkerhet och framförallt kunskap kring påverkan på säkerhet.

Onlineundersökning, fråga 9

KNOWN VULNERABILITIES	OLD VULNERABILITIES THAT SHIP WITH NEW DEVICES
Cleartext Local API	Local communications are not encrypted
Cleartext Cloud API	Remote communications are not encrypted
Unencrypted Storage	Data collected is stored on disk in the clear
Remote Shell Access	A command-line interface is available on a network port
Backdoor Accounts	Local accounts have easily guessed passwords
UART Access	Physically local attackers can alter the device

Table 1, Common Vulnerabilities and Exposures

Figur 8 - Babymonitors – flaws, Publicerad med upphovsrättsinnehavarens tillstånd