Examensarbete

HÖGSKOLAN I SKÖVDE

Hur bör manipulation av IoT-enheter i det smarta hemmet hanteras och åtgärdas av användare och utvecklare?

En systematisk litteraturstudie för att kartlägga åtgärder för smarta hem.

How should manipulation of IoT devices in the smart home be handled and addressed by users and developers?

A systematic literature study to map best practices for smart homes.

Examensarbete i informationsteknologi med inriktning mot nätverks- och systemadministration
Grundnivå 22,5 högskolepoäng
Vårterminen 2020

Mathias Rosell
c14matni@student.his.se
IT610G
2020-06-25

Handledare: Dennis Modig
Examinator: Ali Padyab

Sammanfattning

IoT-enheter är för många människor idag en del av vardagen och fler och fler enheter ansluts till människors hushåll. Smarta hem har allt från kylskåp och övervakningskameror som är anslutna till ett nätverk och internet. Problematiken med det är att många av dessa enheter har inte tillräcklig kapacitet eller en avsaknad av tillräckliga säkerhetsåtgärder för att skydda sig mot potentiella attackvektorer. Bristande säkerheten för enheter i det smarta hemmet kan leda till att enheterna blir hackade och manipulerade av angripare. Den som kan skydda det smarta hemmet mot manipulation av dess IoT-enheter är både användare i det smarta hemmet och utvecklare av enheterna. Men det är inte alltid tydligt för vem åtgärden gäller, vilket är något den här studien vill klargöra.

Den här litteraturstudien utgår från befintliga åtgärder identifierade av tidigare forskning. Den skiljer sig från den tidigare forskningen genom att kartlägga vilka åtgärder som är applicerbara för användare och utvecklare för att skydda det smarta hemmet mot manipulation.

Med hjälp av en systematisk litteratursökning valdes 22 studier ut för att besvara studiens frågeställning. För att besvara studiens forskningsfråga används en kartläggande granskningsmetod. Metoden används för att kartlägga och identifiera vilka åtgärder som rekommenderas för både användare och utvecklare. Med hjälp av den tidigare forskningen framställs ett ramverk för att förtydliga vad användaren i det smarta hemmet själv utföra och vilka åtgärder utvecklare kan och bör utföra. Ramverket demonstrerar dessutom en rekommenderad ordning från författaren som åtgärderna bör utföras i.

Nyckelord: smarta hem, internet of things, manipulering av IoT-enheter, säkerhetsåtgärder.

Abstract

Users of IoT devices are for many people today part of everyday life and more and more devices are connected to people's households. Smart homes have everything from refrigerators and surveillance cameras connected to a network and the internet. The problem with this is that many of these units do not have sufficient capacity or lack adequate security measures to protect themselves against potential attack vectors. Lack of security for devices in the smart home can cause the devices to be hacked and manipulated by attackers. Those who can protect the smart home from tampering with its IoT devices are the users in the smart home and the developers of the IoT devices. Although it is not always clear for whom the security measures apply to, which is something that this study aims to clarify.

This literature study is based on existing security measures identified by previous research. It differs from previous research by mapping out which security measures and best practices that are applicable to users and developers to protect the smart home from being manipulated.

Using a systematic literature search, 22 studies were selected to answer the study's question. To answer the study's research question, a mapping method is used. The method is used to map and identify which actions are recommended for both users and developers. Using the previous research, a framework is created to clarify what the user in the smart home can do and what actions developers can and should take. The framework also demonstrates a recommended order from the author in which the measures should be carried out.

Keywords: smart home, internet of things, manipulation of IoT-devices, best practice.

Innehållsförteckning

1. Introduktion

Vi människor lever idag i en ständigt utvecklande teknologisk värld som möjliggör att digitalisera vardagliga föremål för att underlätta vår vardag. Dessa föremål går under benämningen *Internet of Things* vilket är en term för vardagliga föremål som har möjlighet att anslutas till internet eller andra typer av nätverk som till exempel AD-hoc nätverk (Shemshadi, Sheng, Qin, Sun, Zhang, 2017). *Internet of things* förkortas till IoT och dessvärre medför ämnet hot som behöver bemötas. Den här studien fokuserar på hotet att IoT-enheter och andra nätverksanslutna enheter i hushållet kan bli angripna och ge åtkomst till någon obehörig. Hushåll med implementerade IoT-enheter kallas för smarta hem och är i dagsläget en plats som lagrar en stor mängd information om den som bor i hemmet. Att digitalisera och automatisera det traditionella hushållet blir allt mer vanligt med tiden då digitala enheter blir både billigare och mer populära (Jose, Malekian & Ye, 2016; Geneiatakis, Kounelis, Neisse, Nai-Fovino, Steri & Baldini, 2017). Det smarta hemmet kan bestå av IoT-enheter men också andra nätverksanslutna enheter som möjliggör en väg in för angripare. Digitala enheter som, exempelvis en smartphone, kan kontrollera intrigerade IoT-enheter i det smarta hemmet är en väg in för angripare.

I en vitbok för antivirusföretaget Bitdefender undersökte Pascau (2018) vilka de vanligaste hoten mot smarta hem var genom att samla in data angående vilka former av attacker sker mot olika smarta enheter i hemmet. Pascaus (2018) studie är för ett kommersiellt företag och lägger sitt fokus mot hur användare i det smarta hemmet drabbas vid attacker. För den vardagliga användaren är möjligheten att säkra IoT-enheter som TV-apparater och andra mer vardagliga enheter i hemmet svårare då klassiska säkerhetsåtgärder inte alltid är möjliga. En temporär lösning på problemet skulle vara att göra användare mer säkerhetsmedvetna (Pascau, 2018). Ansvaret är dock inte enbart användarens utan ligger också hos utvecklarna av enheterna. Utvecklare av IoT-enheter tillverkar snabbt nya innovativa produkter att sälja på marknaden men kan samtidigt missa att implementera tillräcklig säkerhet som *end-to-end* kryptering (Pascau, 2018).

På grund av mängden och betydelsen av data som finns i användarens smarta hem är det en attraktiv plats för angripare att attackera. Om en angripare får åtkomst till det smarta hemmets nätverk eller någon IoT-enhet finns risken att enheter kan bli manipulerade utan användarens vetskap.

Jose et al. (2016) betonar hur betydelsefullt det är att ha tillgång till det smarta hemmet över internet men diskuterar även säkerhetsproblem med det. På grund av att det smarta hemmet går att nå över internet kan även angripare få tillgång till det från sitt eget hem. Makhdoom, Abolhasan, Lipman, Liu & Ni (2019) beskriver ett exempel när en angripare hackar en smart öppen spis och kan avlägset tända brasan och det sättet orsaka en olycka.

Även om datorer i hemmet är den klassiska enheten som får säkerhetsuppdateringar som till exempel antivirusskydd så betonar Pascau (2018) att inga IoT-enheter skall överses.

"No smart device is insignificant, as each represents a potential attack avenue hacker can manipulate to get inside a home network and take control over all devices linked to it."

(Pascau, 2018, s.4)

Åtgärder behöver tas för att skydda det smarta hemmet och informationen som lagras där. *Best practice* är en term som kan översättas till det bästa åtgärderna för ett område. Studiens perspektiv utgår från vilka åtgärder det smarta hemmets användare och utvecklarna för IoT-enheterna har möjlighet till.

Behov och konsekvenser skiljer sig beroende på vilken typ av enhet som används i hemmet men sårbarheterna följer samma tema med bristande säkerhet som kryptering, autentisering och otillräcklig kunskap från användare. Studiens syfte är inte att hitta en syndabock för vem som möjliggör attacker mot det smarta hemmet. Syftet med studien är istället att framhäva vilka säkerhetsåtgärder som bör tas för att bemöta hoten. Genom åren har utvecklingen dessutom skapat nya utmaningar och förändrat kraven för att skydda sig från externa och interna hot.

För att besvara frågeställningen genomförs en systematisk litteraturstudie med en kartläggande granskningsmetod för att sammanställa tidigare forskning. Studien utgår från redan befintliga åtgärder för smarta hem som identifierades i en tidigare litteraturstudie av Abdullah, Ali, Malebary & Ahmed (2019). Åtgärderna som används anses vara applicerbara för att motverka manipulation av det smarta hemmet, mer information och ytterligare förklaring kring Abdullah et al. (2019) studie diskuteras i kapitel *2.3.1 Tidigare identifierade åtgärder*. I korrelation med ibid används tidigare forskning för att undersöka för vem åtgärderna är ämnade för, användaren i hemmet eller utvecklaren av IoT-enheterna.

2. Bakgrund

För att ge läsaren en tydligare uppfattning om ämnet inleds det här kapitlet med att förklara det centrala begreppet *internet of things* förklaras, vad det är för något och vart det förekommer. Därefter diskuteras attackvektorer mot IoT-enheter för att förtydliga hur manipulation av IoT-enheter kan uppstå. Därefter presenteras tidigare identifierade åtgärder baserat på Abdullahs et al. (2019) studie som anses skydda det smarta hemmet. Slutligen diskuteras det hur tidigare forskning har bemött ämnet och vart det anses finnas en saknad i den forskningen. Kombinationen av tidigare forskning och problemen som uppstår kring attackvektorerna leder till den här studiens frågeställning. Även till ett behov av en sammanställande litteraturstudie med ett ramverk för hur problemet skall bemötas.

2.1 Internet of Things

Följande kapitel beskriver mer djupgående vad begreppet *Internet of Things* innebär.

Med den ständiga utvecklingen i världen förlitar människor sig allt mer på att olika maskiner och enheter ska förenkla vår vardag. I samband med det ökar kraven på vilka maskiner ska finnas och vad de ska klara av. Många gånger förväntas det att maskinerna håller oss säkra och skyddar vår privata information som lagras på olika enheter. Detta kan vara allt från foton tagna med en mobilkamera till medicinska uppgifter.

I samband med människans ökade krav på teknik har det har skett en kraftig ökning med enheter och maskiner som går under benämningen *Internet of Things* som förkortas till IoT.

IoT är en enhet eller maskin som har möjlighet att vara uppkopplad mot ett nätverk eller kan kommunicera med andra enheter via medel som exempelvis Bluetooth, Ad-Hoc-nätverk och andra radiotekniker för kommunikation (Makhdoom et al. 2018). Grundtanken med IoT-enheter är att de skall förenkla eller göra människans vardag mer effektiv. Till exempel att ha en hörselapparat sammankopplad till användarens mobiltelefon för att justera inställningar. I en privatpersons vardag kan användningsområdet av IoT-enheter också bestå av exempelvis smarta kylskåp, smarta glödlampor, smarta tv-apparater och smartklockor. Dessa enheter kan i dagsläget vara de mest naturliga att betrakta som IoT-enheter men på grund av den stora ökningen av krav på IoT-enheter i samhället utökas det även till större och mer kritiska användningsområden.

“The video created by Massachusetts Institute of Technology [1] shows that all devices that fall under the cluster of IoT reach all corners of infrastructure such as Telecommunications, Healthcare, Manufacturing, Public Sector, Finance, etc. This is also supported by the way in which we as a population interact with devices daily, such as ATM machines to withdraw money, Point of Service devices, coffee machines and smartphones.”

(Whitter-Jones, 2018, s.163)

Whitter-Jones (2018) diskuterar här större användningsområden som fortfarande kan betraktas som vardagliga men har en större inverkan på allmänheten om tjänsterna har bristande säkerhet.

Människor blir allt mer beroende av IoT för att bibehålla ett hållbart samhälle då hela städers infrastruktur baseras runt det. Maayan (2020) diskuterar att det år 2020 finns 30 miljarder installerade IoT-enheter i kontrast till 2013 då det beräknades finnas runt 9,9 miljoner anslutna IoT-enheter. Det är på grund av den kraftiga ökningen som enheterna behöver vara skyddade mot potentiella hot och att användarna skall ha möjligheten att skydda sig. Hot mot sårbara IoT-enheter kan i dagsläget påverka till exempel användares ekonomiska tillgångar och deras hälsa (Han, Jeon & Kim, 2015).

Från ett säkerhetsperspektiv är varje ansluten IoT-enhet en potentiell sårbarhet för attackvektorer som kan komma över känslig data eller manipulera IoT-enheter (Vojković, Milenković & Katulić, 2019). Dock med den ökande användning av IoT-enheter i hemmet ökar även hoten och antalet attackvektorer som kan drabba hushållet samt behovet att kunna åtgärda det.

” With the high adoption rate of Internet of Things, more and more devices are connected to the Internet. Every day, these smart objects are becoming target for information security risks.”

(Kumar, Vealey, Srivastava. 2016, s.5774)

2.2 Attackvektorer för att möjliggöra manipulering av IoT-enheter

I takt med att IoT utvecklas ökar även hoten mot enheterna och metoderna som kan vara skadligt för dem. Varje hot som kan drabba IoT i smarta hem är tillräckligt stort för sin egen studie och det kommer därför inte att diskuteras på djupet hur varje form av attack mot IoT-enheter fungerar. Istället kommer följande kapitel ge läsaren en övergripande kunskap om attackvektorer som kan användas för att möjliggöra manipulering mot IoT-enheter och nätverksanslutna enheter i smarta hem.

Då den här studien undersöker åtgärder för manipulering av IoT och smarta enheter i det smarta hemmet behöver vanliga attackvektorer och sårbarheter undersökas för att veta hur åtgärder kan användas. Det finns många olika tekniker för att angripa det smarta hemmet men den här studien fokuserar på tekniker som leder till manipulering av IoT-enheter. Karimi & Krit (2019) diskuterar potentiella hot i det smarta hemmet och kategoriserar interna hot och externa hot. Interna hot som Karimi & Krit (2019) diskuterar är primärt gällande enhetsfel som strömavbrott och fel på mjukvara medan externa hot är bland annat hoten som diskuteras i följande delkapitel. Då interna hot kan göra att användardata förloras och temporärt bromsa det smarta hemmet kan de externa hoten orsaka fler hot mot användarens data och enheter.

2.2.1 Den mänskliga faktorn

Följande kapitel beskriver ett av hoten som den mänskliga faktorn kan leda till, manipulering och övertagna IoT-enheter utan användares vetskap.

Om olyckor eller medvetna hot drabbar det smarta hemmet kan det ofta härledas till den mänskliga faktorn. Några av de vanligaste attackvektorerna som förekommer är utvecklingsfasen, användarna och människorna som väljer att angripa IoT-enheter. Enligt Vojković et al. (2019 är bristande utbildning och användarmedvetenhet något som gör både användare och utvecklare sig själva möjliga offer och ökar risken för potentiella hot.

Pascu (2018) menar att mycket ansvar ligger hos utvecklarna men att även användare behöver bli mer medvetna om deras egna IoT-enheter för att fullt kunna skydda sig mot yttre hot.
Fakroon, Alshahrani, Gebali, Traore (2020) menar dock att svaga autentiseringsmetoder i kombination att användarna själva står för att implementera den säkerheten är en svaghet i smarta hem idag.

Makhdoom et al. (2018) lyfter dock fram problematiken att implementera en genomgående säkerhet då IoT-enheter skiljer sig så mycket från varandra eftersom det saknas i dagsläget en universal standard. Det finns i dagsläget ingen universal standardisering för protokoll i IoT-enheters arkitektur, istället finns en heterogenitet mellan de olika IoT-enheterna (Al-Qaseemi, Almulhim, Almulhim, Chaudhry, 2016). Det faller ett stort ansvar med utveckling, implementation och användning av IoT-enheter då det blir mer och mer integrerat i hemmet. Det finns även ett problem med firmware då inte alla IoT-enheter erbjuder regelbundna uppdateringar.

Lin & Bergmann (2016) skriver att en anledning kan vara att det inte anses vara lönsamt att fortsätta med nya patch-versioner för enheter som inte kostar så mycket pengar. Även Davis, Mason, & Anwar (2020) identifierar att säkerheten kan påverkas beroende på hur välkänd enheten kan vara. Säkerheten hos IoT-enheterna tycks påverkas beroende på om företaget som utvecklar produkten är välkänt eller ej. För det problemet skrivs det dessvärre enbart en önskan till vidare forskning för att kunna utveckla bättre säkerhet för mindre kända utvecklare (Davis et al. (2020).

Enligt Lin & Bergmann (2016) kan dock den största sårbarheten vara bristen på dedikerade säkerhetsexperter som kan hantera komplexiteten i ett smart hem. Istället så faller ansvaret ofta på mindre tekniska användare som behöver lära sig hur deras hem skall vara säkert.

Brister i den mänskliga faktorn är en sårbarhet som möjliggör hot mot det smarta hemmet. Den här studien undersöker inte social manipulering från grunden utan mer vilka säkerhetsåtgärder som kan tas för att skydda det smarta hemmet.

2.2.2 Malware

Malware är i grunden en form av manipulering och förklaras i sin helhet i det här kapitlet.

Manipulering av nodbaserade applikationer kan ske på grund av och även leda till ytterligare *malware* infektioner. Clincy & Shahriar (2019) beskriver *malware* som en övergripande term för sabotageprogram eller skadegörande kod som är i huvudsak ämnad att få åtkomst till och skada en dator eller server utan användarens vetskap. Den här studien kommer inte att bryta ner *malware* i alla dess olika former utan kommer hantera det som en övergripande paraplyterm men bidra med exempel för att ge djupare förståelse hur IoT-enheter och andra nätverksanslutna enheter kan bli drabbade.

Lin & Bergmann (2016) anser att en stor sårbarhet i smarta hem är den faktiska nätverkstillgången som IoT-enheterna i det smarta hemmet har. På grund av det kan attacker utföras avlägset över nätverket eller att enheterna laddar ner malware.

Malware finns i flera olika variationer som till exempel virus, trojaner och ransomware varav alla har som syfte att orsaka skada och kan ta över enheter som de infekterar. Hackare kan manipulera applikationer på de enheter de befinner sig på genom att utnyttja sårbarheter på IoT-enheten och installera *rootkit*.

Enligt Zhang, Sun, Sun Lou & Hou (2016) har en cyberattack mot en enhet två steg, det första steget är att få root-privilegier och det andra är att dolt behålla kontrollen över systemet genom att installera rootkit.

En form av *malware* som används mot IoT-enheter är internetmasken Mirai som används för DDOS-attacker. Under en tidigare Mirai-attack blev 900 000 användare offline varav två av dessa var kritiska för infrastrukturen i samhället (Whitter-Jones, 2018). Internetmasken Mirai hade som syfte att leta efter standarduppgifter i system som inte hade ändrats som till exempel att standardlösenordet kan vara Admin i ett system.

Serror, Henze, Hack, Schuba & Wehrle (2018) har som exempel en övervakningskamera som kan utnyttjas till att ge ut otillåten root-rättigheter via *malware*. En angripare kan utnyttja att flera IoT-enheter är anslutna till samma hemmanätverk som den kameran. Serror et al. (2018) ser själva nätverket som en stor svaghet i hushållet.

Det finns många olika sätt att användare får deras digitala enheter infekterade av *malware.* Följande är fyra exempel som enligt Geneiatakis et al. (2017) ett smart hem kan infekteras av *malware.*

1. Köpa begagnade enheter som redan har blivit infekterade av malware. En angripare kan till exempel ha köpt flera olika enheter och själv infekterat dem med malware och säljer dem vidare.

2. Likt internetmasken Mirai kan angripare använda falska uppgraderingar för användare. När en användare till exempel försöker uppdatera sin firmware är det en infekterad uppdatering av en angripare som istället infekterar enheten med *malware.*

3. Ett vanligt sätt att styra IoT-enheter i hemmet är i dagsläget via applikationer i sin smarttelefon. Om smarttelefonen är redan infekterad av *malware* kan applikationen äventyra hemmets säkerhet då den styr någon form av enhet där.

4. Onlinetjänster som interagerar med hushållets smart hub kan vara en svag länk i det smarta hemmet. Genom attacker via internet kan en angripare få kontroll och manipulera IoT-enheterna.

Det traditionella skyddet mot *malware* är antivirusprogram som kan installeras på IoT-enheter som stödjer det. Dock kan även antivirusprogram uppleva problem då de till exempel inte kan upptäcka ny och okänd *malware*.

Med hjälp av till exempel krypteringsverktyg är det också möjligt att kringgå antivirusprogrammen (Ali & Hameed, 2019). Trots ett befintligt antivirusprogram kan användare omedvetet infektera enheter med *malware*.

Det är därför väldigt viktigt att enheter är säkrade mot att manipuleras eller gör det möjligt att spåra manipulering. I ett smarthem är till exempel övervakningskameror sårbara för manipulering genom att visa gamla övervakningsfilmer som kan kartlägga användarnas aktiveter i hemmet (Kumar & Srivastava, 2016). Makhdoom et al. (2018) menar att enheter som övervakningskameror saknar dessvärre ofta skydd mot manipuleringstekniker.

2.2.3 Avlyssning & imitering

I vissa fall kan en angripare använda sig av imitering i ett försök att skada användaren eller för att möjliggöra avlyssning (Abdullah et al. 2019). Genom att komma åt information som kan ge åtkomst till IoT-enheter, som användares inloggningsuppgifter, kan en angripare imitera och agera i en användares ställe (Geneiatakis et al. 2017). I ett smart hem kan detta ske genom att angriparen kommer över inloggningsuppgifter och kan då få mycket kontroll över IoT-enheterna (Karimi & Krit, 2019). Detta kan till exempel utföras genom att angriparen kommer åt en unik ID som genereras av en smart hub när enheter ansluter till den. En smart hub kan ofta känna igen IP-adressen så en angripare behöver även få tag på denna (Geneiatakis et al. 2017).

Enligt Park, Oh & Lee (2019) kan *malware*-mjukvara installeras på enheter med AI-högtalare. Om det sker kan avlyssning utföras utan användarens vetskap då mjukvaran är aktiverad i bakgrunden av samtal. Utöver avlyssning kan en angripare med hjälp av detta manipulera AI-högtalaren genom att duplicera egna röstkommandon och sända information (Park et al. 2019)

Tanwar, Patel, Patel, Tyagi, Kumar & Obaidat (2017) betonar att säkerhetsåtgärder för det smarta hemmet finns i dagsläget men anser också att det inte är tillräckligt för att skydda och få användaren att känna sig säker. Det används ofta i olika former av sensorteknik i hemmet som till exempel mäter av temperatur, tryckkänslighet, GPS och RFID sensorer (Kumar & Srivastava, 2016).

Att samla information om den fysiska världen och använda den datan för IoT-enheter i det smarta hemmet kan drabbas av andra attackvektorer (Suo, Wan, Zou & Liu, 2012). Dessa attackvektorer kan till exempel vara avlyssning av kommunikation mellan enheter för att skicka privat information om användare.

Genom avlyssning och att skicka ut korresponderande nätverkssignaler kan en angripare identifiera IoT-enheterna i det smarta hemmet (Geneiatakis et al. 2017). I Följd av det kan angriparen försöka digitalt imitera den riktiga användaren i hemmet och få åtkomst till IoT-enheterna i hemmet. Angriparen kan sen kontrollera IoT-enheterna för att till exempel avbryta deras tjänster och även extrahera data från dem (Geneiatakis et al. 2017).

Andra metoder för att ta över och infektera IoT-enheter kan vara *Sniffing* attacker. Dessa utförs genom att placera obefogade sensorer nära IoT-enheterna för att få information från dem. Det blir problematiskt när privat information om användarna hamnar i fel händer, vilket dessvärre möjligt då dagens IoT-enheter lagrar stora mängder data om användares information och dagliga rutiner (Kumar & Srivastava, 2016). Andra attacker som man-in-the-middle kan också användas, då blir kommunikationen mellan två eller fler enheter avlyssnad av en angripare. De två parterna är omedvetna om att deras kommunikation blir avlyssnad och angriparen har möjligheten att bland annat komma över privata krypteringsnycklar. Angriparen har möjligheten att agera som en proxy och kan både avlyssna, injicera egna kommandon och modifiera överförd data (Anthi, Williams, Słowińska, Theodorakopoulos & Burnap, 2019).

2.3 Tidigare forskning

Ämnet *internet of things* och smarta hem är i dagsläget två områden som har blivit rikligt forskade om. Forskningen är omfattande och varje del kan delas upp i flera studier, därför kommer den här studien förhålla sig primärt till studier som diskuterar manipulering av IoT-enheter i smarta hem. Hoten som diskuteras är inriktade mot vad användare av IoT-enheterna samt utvecklarna för enheterna ett smart hem kan, till sin bästa förmåga, åtgärda. Området blir snabbt komplext då det smarta hemmet bygger på IoT och dessa enheter kan variera från en övervakningskamera till ett barns leksak.

Enligt Geneiatakis et al. (2017) kan ett smart hem beskrivas som symbios för flera olika enheter som sensorer, anslutningar och applikationer som tillsammans arbetar för att bygga en heterogen IoT-arkitektur.

Detta för att effektivt hantera hemapparater och ge de boende i hushållet avancerade tjänster (Geneiatakis et al. 2017). Trots att ibid undersöker olika sårbarheter och attackvektorer framgår det inte tydliga metoder för att bemöta det. Istället diskuterar ibid problematiken att åtgärda de identifierade hoten.

Makhdoom et al. (2019) utför en övergripande studie där de undersöker hot mot IoT i både större områden som smarta städer och hälsorelaterade organisationer. Smarta hem diskuteras i samband med vilka sårbarheter det kan utsättas för men också att det kan leda till att användares privata data och nätverkstrafik blir analyserad och hamnar i obehöriga händer. Makhdoom et al. (2019) kartlägger hot mot själva arkitekturen hos IoT-enheter med fokus på *malware* som attackvektor. De diskuterar i samband med detta olika säkerhetsåtgärder som tas för att skydda enheterna som till exempel kryptering och autentisering (Makhdoom et al. 2019).

Karimi & Krit (2019) utförde en mer inriktad studie för hot mot smarta hem där en smartmobil har möjligheten att styra det IoT-enheter som är anslutna i hushållet. Karimi & Krit (2019) identifierar olika metoder en angripare kan använda sig av för att ta över och manipulera IoT-enheter i det smarta hemmet. Till exempel skriver Karimi & Krit (2019) om *malware*-attacker för att infektera enheter och tillåta angriparen att ta kontroll över IoT-enheter. En annan övertagningsmetod Karimi & Krit (2019) diskuterar är *man-in-the-middle* attacker för att möjliggöra att angriparen kan ta del av trafiken mellan två parter utan deras medvetande och kan även förändra information som skickas. Likt Makhdoom et al. (2019) diskuterar Karimi & Krit (2019) hot som kan drabba IoT-enheter och presenterar liknande data som Makdoom et al. (2019) undersökte i form av sabotageprogram. Dock med mer fokus på det smarta hemmet identifierar Karimi & Krit (2019) även fysiska hot som kan drabba användaren på grund av att IoT-enheter manipuleras.

Det diskuteras dock inte i tydlighet vilka åtgärder en användare bör ta och vad en utvecklares ansvar ligger. Om inga åtgärder tas för att säkra till exempel säkerhetskameror i det smarta hemmet kan dessa bli övertagna av en angripare. Detta kan resultera att angriparen kan se när användaren är hemma eller ej och manipulering av IoT-enheter kan då leda till fysiska hot mot användaren (Karimi & Krit, 2019).

Lin & Bergmann (2016) anser att ett av de största hoten mot smarta hem är just otillåten tillgång av systemkontroll eller någon enhet med administratörsrättigheter.

Detta kan i följd göra att hela det smarta hemmets enheter blir utsatta för fara. Enligt Lin & Bergmann (2016) kan detta bland annat ske genom otillräckliga lösenord och hantering av krypteringsnycklar eller någon otillåten enhet som ansluts till nätverket.

Även Chu, Apthorpe & Feamster (2019) upptäckte bristande implementerad säkerhet i applikationer som används till barnleksaker. De upptäckte bland annat att källkoden för en produkt kallad *smart-pet* sparade information i klartext. Information i klartext kan innehålla exekverbardata som gör att en angripare avlägset kan starta delar i koden för att exempelvis köpa tillägg till applikationen åt användarens vägnar (Chu et al. 2019). Ibid diskuterar IoT-enheter som mycket väl kan förekomma i smarta hem, som ett barns smarta leksaker. Dock diskuterar ibid enbart allmänt om enheterna bör säkras men inte hur användare bäst bör hantera enheterna.

De tidigare studierna som har beskrivits i det här kapitlet har identifierat sårbarheter, olika metoder för manipulering mot det smarta hemmet och även potentiella åtgärder. Dock om åtgärder beskrivs i artikeln framgår det inte i studierna en tydlig avgränsning för vem som kan använda sig av åtgärden, användare eller utvecklare. Den här studien strävar efter att bemöta det och ta med det för att bidra till forskningen en tydlighet för både användare och utvecklare. För att göra det behöver tydliga åtgärder användas som en utgångspunkt. Dessa tidigare identifierade åtgärder beskrivs i följande kapitel och utgår från Abdullahs et al. (2019) studie om hot mot smarta hem.

2.3.1 Tidigare identifierade åtgärder

Som det diskuterades har Abdullah et al. (2019) undersökt hur cyberhot kan drabba det smarta hemmet genom att identifiera sårbarheter, hot och åtgärder. Den här studien är baserad på de befintliga åtgärdsrekommendationer som Abdullah et al. (2019) presenterar. Dock skiljer sig den här studien genom att använda de befintliga åtgärderna för att kartlägga om de är applicerbara för användare eller utvecklare. Ibids studie granskades för vilka säkerhetsåtgärder kan appliceras i smarta hem och användas för den här studien.

Följande är de sju åtgärder som ibid presenterar som en lösning för cyberhot mot det smarta hemmet:

1. *Updating the Software*
    - Den första åtgärden som ibid anser skall användas är att uppgradera mjukvaran för enheter i hemmet. Genom att använda och hålla brandväggar uppdaterade kan hot som *malware* motverkas. Att sedan använda den senaste uppdateringen firmware är viktigt för att säkerställa att enheten har möjlighet att möta nya hot som kan uppstå.

2. *Utilizing Effective Encryption*
    - Likt Makhdoom et al. (2019) rekommenderar Abdullah et al. (2019) att nätverkstrafiken mellan enheterna behöver vara krypterad. Användandet av effektiv kryptering kan hjälpa motverka att privat data läcker. Krypterad data minskar risken för obehörig tillgång till IoT-enheterna i hemmet.

3. *Using Private Network*
    - Enligt Abdullah et al. (2019) kan användningen av privata nätverk säkra det smarta hemmet genom att bara behöriga kan få åtkomst till nätverket. Detta kan göras med till exempel VPN vilket är en kommunikationskanal som blir svårare att få åtkomst till för angriparen.

4. *Applying up-to-date Protocols*
    - Abdullah et al. (2019) anser att aktuella protokoll behöver användas för IoT-enheter. Ibid anser också att utvecklare av IoT-enheter behöver implementera uppdaterade kommunikationsprotokoll för att enheterna skall vara säkra mot aktuella hot.

5. *Changing Credentials Regularly*
    - Enligt Abdullah et al. (2019) bör IoT-enheter uppmana användarna till att byta inloggningsuppgifter från standardinloggningen som medföljer. Till exempel kan admin vara både användarnamn och lösenord på kommersiella routrar. Ibid anser även att lösenordet bör ändrats var tredje månad och att inte använda samma lösenord för alla enheter.

6. *Backup Significant Information*
    - För förebygga mot eventuella attacker rekommenderar Abdullah et al. (2019) att genomföra regelbundna säkerhetsuppdateringar av data som inte användaren vill förlora och förvara den fysiskt eller digitalt.

7. *Monitoring the Network*
    - En bra metod för att upptäcka potentiellt digitalt intrång i det smarta hemmet är att övervaka nätverkstrafiken. Genom att använda program för att övervaka nätverket kan sårbarheter upptäckas och vissa program kan även bidra till att uppdatera IoT-enheterna (Abdullah et al. 2019).

Abdullah et al. (2019) anser att de sju presenterade åtgärderna kan användas för att motverka cyberhot mot det smarta hemmet. Dock strävar den här studien efter att identifiera åtgärder mot hotet av manipulation och övertagningen av det smarta hemmet. Utifrån den synvinkeln identifierades två presenterade sårbarheter från ibids studie som kan möjliggöras till åtgärder i den här studien.

8. Heterogeneous Architecture
    - Likt Geneiatakis et al. (2017) anser Abdullah et al. (2019) att problematiken med heterogeniteten hos IoT-enheter behöver åtgärdas. I det smarta hemmet används många olika enheter som behöver samarbeta med varandra trots att de använder olika system. På grund av den heterogena arkitekturen behöver utvecklare i nuläget arbeta fram strategier för att säkra deras IoT-enheter. För att sträva mot en homogen arkitektur anser ibid att medvetenheten kring IoT applikationer och system är viktigt.

9. *Limited Storage and CPU*
    - Enligt Abdullah et al. (2019) kan begränsad hårdvara och processorkraft vara en sårbarhet hos IoT-enheter som kan i följd leda till att cyberattacker kan angripa enheterna enklare. Utvecklingen för att förbättra hårdvaran kan därför vara en åtgärd att utforska.

Utöver Abdullahs et al. (2019) presenterade åtgärder och sårbarheter identifierar de även behovet av att bedöma risker i förväg för att skydda det smarta hemmet. Likt punkt 8 och punkt 9 som härstammar från sårbarheter kan även denna användas som en tionde åtgärd från ibids studie.

10. Riskbedömning
    - Abdullah et al. (2019) anser att det är viktigt att i tid identifiera möjliga säkerhetsrisker i det smarta hemmet för att göra det möjligt att kunna säkra hemmet mot yttre hot. Genom att bedöma sårbarheter, risker och hot kan bättre strategier för det smarta hemmet användas.

De tre sista åtgärderna som diskuterades presenterar Abdullah et al. (2019) inte deras kapitlet för åtgärder utan de förekommer mer som förslag mot identifierade sårbarheter. Dock anses de vara applicerbara åtgärder för att motverka manipulering av det smarta hemmet. Åtgärderna från Abdullah et al. (2019) är ämnade för att motverka cyberattacker mot det smarta hemmet men likt de andra studierna som har diskuterats i kapitel *2.3 Tidigare forskning* framgår det inte alltid en tydlig avgränsning för vem som har möjlighet att utnyttja rekommenderade åtgärder, användare eller utvecklare.

3. Problembeskrivning

Följande kapitel kommer att gå igenom varför IoT-enheter och andra nätverksanslutna enheter i hemmet kan bli problematiska och diskutera studiens syfte och frågeställning.

Som det har diskuterats har IoT-enheter som syfte att göra olika aktiviteter mer användarvänliga i människors vardag och kan effektivt implementeras i det smarta hemmet. I ett hem kan IoT-enheter variera allt från smarta Tv-apparater till elektroniska lås till ytterdörrar. Att enheter i hemmet använder sig av någon form av nätverkskommunikation skapar dock problem. Hemmet blir i följd utsatt för utomstående hot, användarna i hemmet samt brister från utvecklingsfasen av olika IoT-enheter. Till exempel undersöker Fouladi & Ghanoun (2013) sårbarheter med protokollet Z-wave. Fouladi & Ghanoun (2013) upptäcker bland annat att dörrlås med Z-wave AES kryptering kunde bli avlägset hackade för att få full kontroll över låset. På så sätt kan en angripare låsa upp dörraren utan användarens medvetenhet. Det framgår dock inte tydligt i studien vad en användare kontra utvecklare har kontroll över i den situationen.

Antalet studier som genomförs inom ämnet är väldigt omfattande och presenterade åtgärdsförslag kan upplevas som utspritt utan en tydlig identifiering av gemensamma nämnare. På grund av att fler hot och olyckor drabbar det smarta hemmet blir det desto svårare att säkra användare utan deras hjälp och säkerhetsmedvetenhet (Vojkovic et al. 2019). Forskningen finns men eftersom manipulerade IoT-enheter kan drabba majoriteten av hushåll behövs det undersökas hur detta kan bemötas och åtgärdas för både användarna och utvecklarna.

3.1 Syfte & motivering

Studien syfte är inte att hitta en förbestämd skurk för vem den skyldige är angående manipulation av IoT-enheter i hemmet. Utan istället, med hjälp av tidigare forskning, sammanställa de åtgärder som kan tas för att säkra det smarta hemmet och kartlägga användningen för både användare och utvecklarna.

Det upplevs som att det i nuläget inte finns klara riktlinjer för vilka åtgärder användare och utvecklare kan är rekommenderade att ta. Samt om det finns några åtgärder som de båda parterna kan ta i symbios med varandra. Den här studien har som syfte att förtydliga dessa tankar genom att utgå från Abdullahs et al. (2019) åtgärder och kartlägga vilka åtgärder rekommenderas för de båda parterna. Genom att använda en systematisk litteraturstudie som metod kan åtgärderna kartläggas och identifiera gemensamma nämnare för att undersöka hur manipulering mot det smarta hemmet kan bemötas från de båda parterna.

Som det har diskuterats i kapitel *1. Introduktion* och *2. Bakgrund* i den här studien så finns det diverse hot som kan drabba det smarta hemmet på grund av IoT-enheter men också potentiella åtgärder. Anledningen till att undersöka manipulering av IoT-enheter i det smarta hemmet är på grund av antalet människor som lever i smarta hem idag och hur manipulation av deras IoT-enheter kan direkt drabba hushållets förmåga.

Det är inte enbart användares ansvar att säkra IoT-enheterna i det smarta hemmet. I exempelvis Chu et al. (2019) studie ledde sårbarheterna för smartprodukterna till att utvecklarna var under pågående utredning. En av produkterna som undersöktes var en vattenflaska som anslöts till en applikation för att kontrollera hur mycket användaren drack. Vattenflaskan kunde anslutas via Wi-Fi och Bluetooth och när Chu et al. (2019) undersökte källkoden på vattenflaskan upptäckte de att den skickade ut användardata till 12 fjärrvärdar. Fjärrvärdarna var utvecklarna av produkten men också tredje parter som tog del av användardata (Chu et al. 2019). Ibid upptäckte också att enheter kunde skicka meddelanden i klartext vilket en angripare kan avlyssna för att få tag på inloggningsuppgifter. Att implementera sådana smarta enheter i hemmet kan leda till att angripare får kontroll över hemmet. Ansvaret för att säkra det smarta hemmet är då fördelat mellan utvecklarna av produkten och användarna som intrigerar den smarta vattenflaskan i sitt nätverk i hemmet. Dock framgår det inte tydligt i Chu et al. (2019) studie vem som primärt kan implementera åtgärder mot sådana produkter.

Det är inte utan anledning att IoT-enheter möter stora hot när de blir uppkopplade mot ett nätverk då enheterna i grund har samma sårbarhet. Till skillnad från en traditionell dator som är uppkopplad till ett nätverk har inte alla IoT-enheter samma resurser som kan hjälpa säkra dem. Till exempel har en traditionell dator möjlighet till större lagringsutrymme, processorstyrka och mer effektiv energiförbrukning oavsett om den är trådbunden eller ej. Därför kan traditionella maskiner ha bättre säkerhet implementerad utan att belasta resurser som en IoT-enhet behöver göra (Makhdoom et al. 2018).

IoT-enheter autentisering kan brista då en enheterna inte alltid har samma förutsättningar som en dator. Lösenord för IoT-enheter kan ibland vara begränsade till ett visst antal tecken eller siffror och det är inte alltid möjligt att välja lösenordets längd eller kombinera bokstäver, siffror och specialtecken (Karimi & Krit, 2019).

Valet av att undersöka rekommenderade åtgärder för både användare och utvecklare är på grund av hypotesen att säkerhetsmedvetenhet hos de båda parterna kan hjälpa säkra det smarta hemmet mot manipulation.

3.2 Frågeställning

Utifrån problematiken med IoT-enheter i hemmet kan studiens frågeställning summeras till en fråga:

Hur bör manipulation av IoT-enheter i det smarta hemmet hanteras och åtgärdas av användare och utvecklare?

Det finns många former av användare i ett smart hem som är mer eller mindre teknologiskt kunniga. Den typen av användare som den här studien hänvisar till är den som administrerar i det smarta hemmets system.

Sårbarheter och hot från tidigare nätverksenheter och okända IoT-enheter har drivit forskningen till att undersöka vad för hot IoT potentiellt kan drabba smarta hem. Likt studierna som diskuteras i kapitlet *2. Bakgrund* kommer det här arbetet fokusera på manipulering av IoT-enheter i det smarta hemmet och den mänskliga faktorn kring det i form av användare och utvecklare. Detta görs av två anledningar, den första är eftersom det direkt påverkar en hemanvändares IoT-enheter som kan drabba det smarta hemmet. Den andra anledningen är att se vad användaren i hemmet, till sin bästa förmåga, kan åtgärda och hur utvecklarna av IoT-enheterna kan tillföra till säkerheten. Som det diskuteras i kapitel *2.3.1 Tidigare identifierade åtgärder* kommer den här studien kommer att använda sig av totalt tio identifierade åtgärder från Abdullahs et al. (2019) studie som en grund för åtgärder mot manipulation av det smarta hemmet. Med hjälp av en litteraturstudie som metod kan det vara möjligt att besvara vem som åtgärderna är användbara eller ämnade för, användaren i det smarta hemmet eller utvecklaren av enheterna.

3.2.1 Forskningsmål

Genom att besvara forskningsfrågan kan studien förhoppningsvis bidra till kunskap för användare och utvecklare. Att bidra med rekommendationer för användare kan hjälpa dem att säkra systemen i sitt smarta hem för att motverka manipulering. Detta kan bli som ett ramverk som användare bör tänka på. Ramverket blir helt enkelt *best practice* för att sätta upp smarta hem och på så sätt hjälpa den som ska sätta upp systemet med förebyggande åtgärder. Målet att bidra information till utvecklarna av IoT-enheterna är liknande genom att bidra med en rekommendation och klargöra vad tidigare forskning visar för åtgärder som utvecklarna kan använda sig av.

Genom att klargöra vad användare och utvecklare kan göra kan det bli tydligare för utvecklare vem som bär vilket ansvar i det smarta hemmet och vad som krävs för att säkra deras produkter.

3.3 Avgränsningar

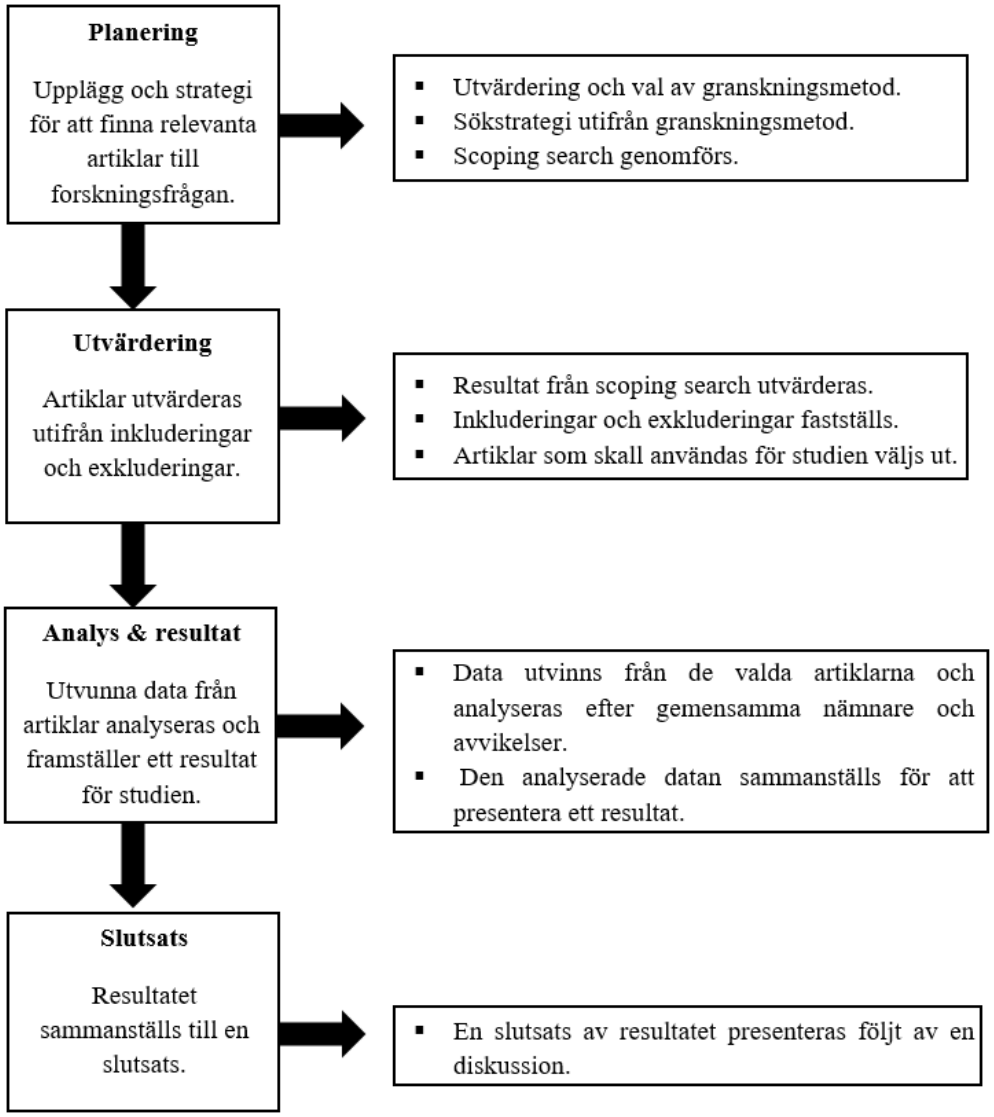
Då sårbarheter har diskuterats i tidigare kapitel kommer resultatet fokusera på vilka åtgärder kan göras av användare och utvecklare för att stärka sig mot hotet av manipulering av IoT-enheterna. Studien kommer fokusera på manipulation av IoT-enheter och de former åtgärder som kan användas för det.

Studien utgår från Abdullahs et al. (2019) studies åtgärder men om det framgår ytterligare åtgärder från litteratursökningen som anses vara applicerbara för användare eller utvecklare kan den också användas. Studien utgår från tidigare åtgärder men behöver fortfarande vara öppen för ytterligare åtgärder som kan identifieras. Andra attackvektorer som de identifierade åtgärderna bidrar till ytterligare skydd till kommer inte att diskuteras på djupet, detta för att behålla studiens fokus.

Som det skrevs tidigare anser Lin & Bergmann (2016) att mycket ansvar faller på mindre tekniska användare som behöver säkra sitt system. Det breda spannet av användare inom smarta hem gör det problematiskt att bedöma den tekniska förmågan för gemene man. Den tekniska förmågan av användare kommer inte att bedömas utan formen av användare som studien fokuserar på är den som administrerar ett smart hem.

4. Metod

För att besvara frågeställningen behöver en granskning av tidigare studier som utforskar ämnet utföras. Frågeställningens natur gjorde därför att en litteraturstudie upplevdes som den mest effektiva metoden eftersom *internet of things* är ett rikligt utforskat ämne. Detta gör att det finns både data och utrymme för en sammanställande studie för åtgärder mot hoten. En systematisk litteraturstudie ökar dessutom chanserna att få ut relevant data från forskning för studien och se vad de utvalda artiklarna har och inte har undersökt. En tydlig metod hjälper även läsaren att navigera och tolka studien (Booth, Papaioannou & Sutton, 2016). För att ge läsaren en överblick på hur metoden kommer att genomförs presenteras ett sammanfattande flödesschema nedanför.



Figur 1: Sammanfattande flödesschema för genomförande av metod. (Författarens egen)

För att studien skall utföras korrekt kräver det att allt relevant material blir undersökt. Inkluderingar och exkluderingar behöver därför tillämpas på de artiklar som framkommer från den initiala sökningen (Booth et al. 2016). Upplägget för att nå användbara artiklar för studien utgår från Booth et al. (2016) och Parés & Kitsious (2017) metoder för att utföra en litteraturstudie. Metoderna delar upp studien i olika stadier så den kan utföras strukturerat. Metoden är effektivt för att avgränsa artiklar och nå dem som förhåller sig till frågeställningen. Booth, et al. (2016) går igenom olika metoder för att utföra en systematisk litteraturstudie och det är upp till författarens bedömning att avgöra vilken metod som är bäst lämpad för studien.

Booth, et al. (2016) diskuterar att en litteraturstudie bör utföras systematisk för att minska sannolikheten att granskningen blir partisk. Trots det är det dock inte alltid lämpligt att utföra en systematisk granskning utan det beslutet behöver tas beroende på frågeställningen. När frågeställningen ställs mot olika granskningsmetoder för en systematisk litteraturstudie kan ett beslut tas om den är lämpad för det eller ej. Det är i samband med det väsentligt att frågeställningen är ledande i litteraturstudien. Detta eftersom frågeställningen i samband med granskningsmetoden avgör vilken information som samlas och utvärderas (Booth et al. 2016). Kastner, Tricco, Soobiah, Lillie, Perrier, Horsley & Straus (2012) upplever utmaningen av att välja ut rätt metod för att sammanställa litteratur och betonar även här vikten av att rätt metod behövs för att kunna besvara frågeställningen. För att undvika villospår använder den här studien sig av ett ramverk framtaget av Booth, et al. (2016) som de kallar för SALSA som förklaras i kapitel *4.1 Granskningsmetod*.

4.1 Granskningsmetod

Booth, et al. (2016) har arbetat fram ett ramverk med granskningsmetoder för hur en systematisk litteraturstudie kan utförs som de själva kallar för SALSA. De demonstrerar flera olika granskningsmetoder där författaren själv får avgöra vilken som är bäst lämpad för studien utifrån frågeställningen som ställs. Metoderna följer fyra följande steg:

1. *Search*
2. *Appraisal*
3. *Synthetis*
4. *Analysis*

De fyra stegen bildar metoden SALSA och varje steg har olika utföringar beroende på den valda granskningsmetoden.

Syftet är att tillsammans stärka granskningen och hjälpa författaren att vara opartisk. Stegen innefattar att söka efter relevant litteratur, värdering av den funna litteraturen, sammanfattning och analys. De fyra stegen gör att författaren kan besvara frågeställningen och nå ett resultat. Den granskningsmetod som var bäst lämpad för den här studien var ansågs vara *Mapping review/systematic map,* en kartläggande granskning, i kombination med en *scoping search* (Booth, et al. 2016). Valen baseras på hur en *scoping search* och en kartläggande granskning söker och utvärderar litteratur då det är lämpat för en frågeställning för ett väl forskat område.

4.1.1 Inkluderingar & exkluderingar

För att välja relevanta forskningsartiklar för studien behövdes det etableras tydliga mål för vad som skall inkluderas i artiklarna samt vad som behöver exkluderas. Kriterierna som ställs på forskningsartiklarna är dels hur väl författaren anser dem förhåller sig till frågeställningen och även krav för att upprätthålla en akademisk standard. Kriterierna hjälper i följd studien att eliminera artiklar som inte är tydligt i linje med frågeställningen (Paré & Kitsiou, 2017).

Artiklarna som analyseras för sammanställning i studien angående hot och åtgärder mot smarta hem förhåller sig till följande inkluderingar och exkluderingar:

Tabell 1: Inkluderingar för artiklar som skall utvärderas (Författarens egen).

1. Artikeln skall vara tillgänglig via en kostnadsfri databas via Högskolan i Skövde.
2. Artikeln skall vara möjlig att nå via framtagna söktermer och granskning av referenslistor. Termer kan även justeras för att få fram mer relevant forskning beroende på använd databas.
3. Artikeln skall ha uppnått en akademisk standard genom att vara *peer reviewed* så den har blivit godkänd av experter inom området. Det här med syftet att den data som utvinns från varje artikel inte är missvisande eller partisk.
4. För att forskningen ska vara relevant behöver artiklarna vara från 2015–2020. Detta eftersom IoT-enheter hastiga utveckling påverkar hur det ser ut i dagsläge. Dock studier en fem års period anses fortfarande kunna ge relevant information. Forskningen tycks dessutom ha ökat från 2015, se figur 2 & figur 3.
5. Artiklarna bör, men är inte begränsade till att, vara skrivna på engelska för att bredda forskningsområdet och undvika partiska språkbarriärer (Booth, et al. 2016).
6. Artikeln behöver vara relevant och gynna frågeställningens syfte för den här studien. Den är inte nödvändigtvis användbar genom att enbart diskutera ämnet IoT-enheter.
7. Förbättringsförslag eller åtgärder behöver diskuteras i studien.
8. Både kvalitativa och kvantitativa studier kan inkluderas för att bredda sökresultaten.

Tabell 2: Exkluderingar för artiklar som skall utvärderas i studien (Författarens egen).

1. Böcker skall inte redovisas då det inte går i linje med arbetets storlek eller tidsplan.
2. Exkludera artiklar som enbart identifierar hot utan att bidra med förbättringsförslag eller åtgärder.
3. Exkludera dubbletter som förekommer på flera databaser.

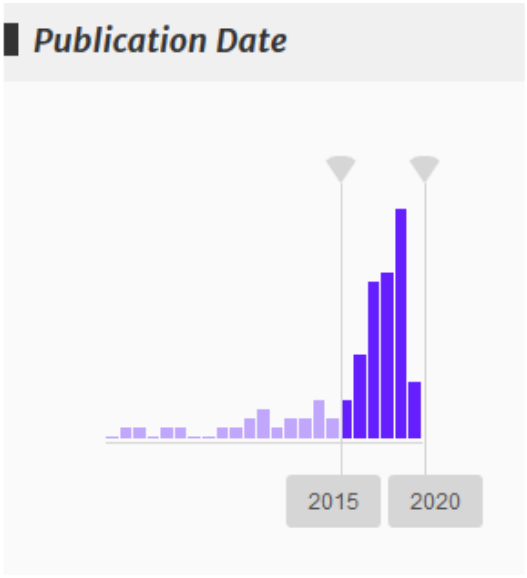
Inkluderingskrav 1 är på grund av författarens resurser och då Högskolan i Skövdes bibliotek möjliggör kostnadsfri litteratursökning på databaser.

Inkluderingskrav 2 är ämnad för att förhålla sökresultatet opartiskt genom att nå studier via söktermer som är framtagna med hjälp av nyckelord från en *scoping search.* Inkluderingskrav 2 hjälper även läsare som själva vill ta del av litteratursökning inom ämnet då söktermer kan återanvändas.

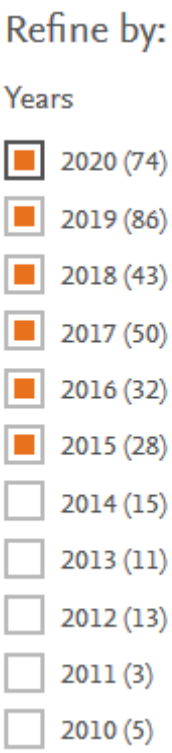
Inkluderingskrav 3, 4, 5, 6 och 7 är ämnade för att säkerställa att studier upprätthåller en akademisk standard och förhåller sig med relevant information för forskningsfrågan som ställs i den här studien.

Utöver inkluderingar och exkluderingarna som lades till så rekommenderar även Booth et al. (2016) att använda sig av databaser och sökmotorers egna filter i uppsökning av litteratur.

Som inkluderingskrav 5 beskriver tycks forskningen relaterad till smarta hem öka kring 2015. Detta upptäcktes under när databaser valdes ut. ACM Digital Library och Science Direct ger en visuell illustration när filter för årtal appliceras, se figur 2 och figur 3.



Figur 2: Filter för årtal från ACM Digital Library



Figur 3: Filter för årtal från ACM Digital Library

Figur 2 och figur 3 visar sökresultat från sökfras 1 som beskrivs i kapitel *4.3 Litteratursökning och sökfraser*. Som figur 2 och figur 3 visar ökar antalet forskningsartiklar från år 2015. I korrelation att utvecklingen av IoT-enheter och smarta hem utvecklas i en snabb takt valdes det att undersöka från fem år tillbaka.

När kraven var bestämda för vad en forskningsartikel behövde uppnå för att användas i studien framställdes det en litteratursökningsfras för att hitta rätt forskningsartiklar. IoT är ett ämne som har undersökts i många olika fält och syften och omfattar ett brett område för både privat användning och användning i organisationer.

Sökfrasen behövde därför konstrueras för att stämma med frågeställningens syfte. Booth, et al. (2016) demonstrerar fem faser för sökprocessen som används, se figur 4.

Stage	Description	Steps
Stage 1	Initial search of the literature: scoping search	• Search for existing reviews and familiarise yourself with the topic and volume of literature by a scoping search on select databases (one or two key databases) • Determine which databases are to be included in the full search • Identify key search terms • Develop and document a search strategy
Stage 2	Conduct search	• Search all databases using the identified search terms and the key search principles where appropriate: free-text terms and tools, thesaurus terms, operators and limits • Conduct a search for unpublished or ***grey literature*** • Consider the appropriateness of a methodological search filter • Ensure if the search is modified, this is documented
Stage 3	Bibliography search	• Search the reference lists and bibliographies of all included studies for any additional relevant studies • Identify any key citations and conduct citation searches • Consider hand searching key journals
Stage 4	Verification	• Check indexing of any relevant papers that have apparently been missed by search strategies • Revise search strategies if necessary • Consider contact with experts to determine if all relevant papers have been retrieved
Stage 5	Documentation	Record details such as the sources searched, search strategies used, and number of references found for each source/method of searching (NB: although listed as Stage 5 here, it is helpful to document your searches and any additional techniques as you perform them)

Figur 4: Stegen i sökprocessen (Booth et al. 2016, s.110)

Strategier för varje steg utvärderades för att anpassas till studiens forskningsfråga, tidsram och resurser (Booth et al. 2016).

4.1.2 Databaser

En av inkluderingarna för studiens artiklar som dessvärre är begränsande är att arbetet måste anpassas efter de givna resurserna, se tabell 1. Databaser behöver därför vara kostnadsfria eller vara en tillgänglig resurs via Högskolan i Skövdes bibliotek. Booth, et al. (2016) rekommenderar att använda sig av en till två databaser relevanta till frågeställningen i den omfattande sökningen för att identifiera nyckelord som kan användas till den slutgiltiga söktermen.

En sökning på enbart *internet of things* med forskning från 2019–2020 via sökmotorn Google Scholar gav 47 500 träffar och behöver en tydlig strategi för att minimera antalet irrelevanta artiklar. Booth et al. (2016) listar olika databaser kategoriserade efter olika forskningsområden författare har valt att utforska. Utifrån Booth et al. (2016) rekommendationer valdes tre databaser relaterat till ämnet ut då dessa databaser även stödjer användandet av booleska operatorer som används för litteratursökning. De tre utvalda databaserna var IEEE Xplore, Applied Sciences och ACM Digital library. Databaserna valdes även ut då de underlättar litteratursökning efter studier som har blivit *peer-reviewed*, det är till exempel ett krav för att publicera studier på IEEE Xplore. Ytterligare filter på databaserna finns att använda för att anpassa sökningar ytterligare beroende på kraven. Databaserna har alla stöd för booleska och i kombination med det användes det snöbollsmetoden för att säkerställa att inga studier relaterade till ämnet missades. Slutligen användes snöbollsmetoden för att säkerställa att inga artiklar utöver dem som förekom i databaserna inte missades. Wohlin (2014) beskriver snöbollmetoden kan genomföras genom att undersöka referenser som används i de utvalda artiklarna för den här studien. Om studier ansågs vara av intresse för studien undersöktes det om den stämmer in på inkluderingarna som används för studierna som upptäcks via litteratursökningen. Snöbollsmetoden resulterade i artiklar från fem ytterligare databaser.

Följande är de databaser som dem slutgiltiga studierna utvanns från:

- IEEE Xplore
- Science Direct
- ACM Digital library
- USENIX
- Research Gate
- NTNU Open
- MDPI
- Springer Link

Eftersom hot mot *internet of things* och smarta hem är väldigt utforskade ämnen och för att besvara frågeställningen behöver söktermer kombineras för att utesluta irrelevanta artiklar. Brereton, Kitchenham, Budgen, Turner & Khalil (2007) rekommenderar användandet av booleska operatorer i kombination med databaser som är användbara för studier inom informationsteknologi.

Med hjälp av booleska kan en specifik sökterm arbetas fram för att finna artiklar som är relevanta för ämnet samtidigt som söktermen begränsar antalet artiklar som utvinns. Booleska operatorer är en metod som kan användas för att anpassa sin sökning efter litteratur genom att kombinera olika söktermer (Booth, et al. 2016). Vidare förklaring om den slutgiltiga söktermen diskuteras i kapitel *4.3 Litteratursökning och sökfraser*.

Användningen av booleska operatorer föll hand i hand med nästa steg i fas 1 som handlar om att konstruera och bestämma nyckelord som skall användas för söktermen, vilket kan göras med en *scoping search*.

4.2 Scoping search

För att få en uppfattning av söktermer för litteratursökningen används aspekter av en *scoping search* med mer generella sökningar om studiens forskningsämne (Booth, et al. 2016; Paré & Kitsiou, 2017).

Booth, et al. (2016) beskriver en *scoping search* som ett brett penseldrag då en mer omfattande sökning görs och granskning mot artiklar är grundlig med inte lika kritiskt som mot de slutgiltiga artiklarna. För att få en uppfattning av nyckelord som kan användas till dem slutgiltiga söktermerna utfördes följande sökningar på databasen IEEE Xplore:

- (”Smart home” OR Smart homes”)
- (“IoT” OR “internet of things”)

Från sökresultatet tittades det på artiklar som ansågs vara relevanta till ämnet beroende på titel. IEEE Xplore valdes ut för användarvänligheten i det här stadiet. Databasen gör det möjligt att enkelt se vilka nyckelord som förknippas till artiklarna. Nyckelorden dokumenterades och de som ansågs vara relevanta kunde sedan användas för att konstruera söktermer. Antalet artiklar var inte ett fokus då det var en mer generella sökningar för att utvinna nyckelord.

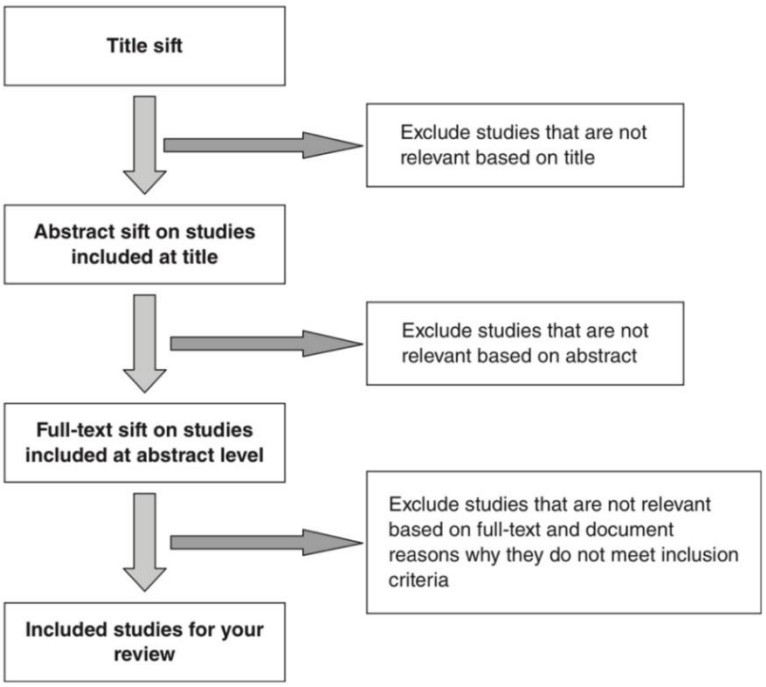
Det handlar mycket om att få en uppfattning om vilka databaser och söktermer som är relevanta och gynnar frågeställningen. En *scoping search* utfördes med fokus att nå ett urval av artiklar där smarta hem utsätts för någon form av manipulering. Syftet med det var att undersöka vilka nyckelord som används i artiklar som är relevant för frågeställningen. Då åtgärderna som används i studien baseras på befintliga åtgärder från Abdullah et al. (2019) var även ett fokus att identifiera nyckelord som förknippas åtgärder från deras studie.

Metoden som användes för urval av artiklar gjordes med hjälp av Booth, et al. (2016) metod för urval av artiklar, se figur 5.

Urvalet av de första artiklarna förhåller sig till fyra frågor som Booth, et al. (2016) hänvisar till när en kartläggande granskning utförs:

- Vart finns det tillräckligt med bevis?
- Vart finns det luckor i forskningen?
- Hur kan bevisen redovisas i den här studien?
- Finns det återkommande teman eller relationer i artiklarna?

Genom att utgå från både frågeställningen och sedan granska artiklar med de frågorna i åtanke kunde modellen från figur 5 utnyttjas mer tidseffektivt.



Figur 5: Modell för urval av artiklar (Booth, et al. 2016).

Under *scoping search* så användes de två första stegen från modellen från figur 5. Det första steget innebär att undersöka titlar från sökresultaten efter vad som anses vara relevant. Det är ett effektivt sätt att exkludera artiklar som tydligt inte förhåller sig till ämnet. Nästa steg innefattade att undersöka artiklars abstrakt och exkludera irrelevanta artiklar.

Om artiklarna ansågs förhålla sig till frågeställningen sparades dem och nyckelorden dokumenterades för att användas till den slutgiltiga sökfrasen.

4.3 Litteratursökning och sökfraser

När kraven var bestämda för vad en forskningsartikel behövde uppnå för att användas i den här studien framställdes litteratursökningsfraser för att hitta relevanta forskningsartiklar. Smarta hem är ett ämne som har undersökts i många olika syften och omfattar ett brett område då det innefattar både privat användning och användning i organisationer.

Sökfraserna som konstruerats i den här studien är baserade på åtgärderna från Abdullahs et al. (2019) studie. För att inte missa ytterligare åtgärder från tidigare forskning förhåller sig sökfraserna relativt breda. Detta resulterade i fyra sökfraser för varje databas, de letar efter samma form av artiklar men variationer skedde beroende på hur databasen hanterar booleska operatorer.

Boot et al. (2016) betonar att det inte anses finnas en magisk siffra på hur många artiklar eller sökträffar skall finnas. Dock bör det slutgiltiga resultatet leda till cirka fem till tolv studier för att litteraturstudien skall vara relevant (Boot et al. 2016). Tabell 3 visar grunden för sökfraserna innan de var anpassade för någon av databaserna:

Tabell 3: Grundläggande sökfraser innan anpassning per databas

Sökfras 1	(”smart home” OR ”smart homes”) AND secur* AND manipulat*
Sökfras 2	(“smart home” OR “smart homes”) AND eavesdrop*
Sökfras 3	(“smart home” OR “smart homes”) AND weakness*
Sökfras 4	(“smart home” OR “smart homes”) AND best practice

Grundsökfraserna från tabell 3 för varje databas men där det upplevdes som att någon form av ändring behövdes så gjordes det. Detta för att få relevanta artiklar till studien och en säkerhet att inga artiklar missades på grund av att sökfrasen inte var anpassad.

Att använda Smart home* testades för böjningar av termen vilket gav betydligt fler sökträffar. Dock avvek majoriteten av studier att fokusera på smarta hem och det räckte att termen smart i någon benämning användes i artikeln.

Istället används (”Smart home” or ”smart homes”) för att inte begränsa artiklar till endast en av termerna men fortfarande behålla fokuset på sökträffarna.

Sökfras 1 använder termen secur* vilket är en väldigt bred term då den resulterar även i böjningar som till exempel secure, security eller security threath. Sökningen är ämnad för att utvinna artiklar som undersöker säkerhet i smarta hem med fokus på manipulation. Nackdelen med att ha breda söktermer som secur* i sökfrasen är att undersökningsmomentet av studier blir mer tidskrävande men det försäkrar att inga studier överses. Många studier som undersöker säkerheten i det smarta hemmet inkluderade även åtgärdsförslag som kunde användas i studien.

Sökfras 2 använder eavesdrop* då med anledningen att nå artiklar som undersöker olika former av avlyssningstekniker då det är en vanlig och väldigt bred metod som har möjlighet att leda till någon form av övertagning och manipulering.

Sökfras 3 använder AND weakness* för att inkludera artiklar där svagheter i det smarta hemmet har identifierats. Trots mängden på sökresultatet resulterade dock inte sökfras 3 till några använda artiklar. Anledningen till det var att söktermen weakness* inte var specifik nog för att nå sökresultat för manipulation inom det smarta hemmet. De studier som ansågs relevanta i sökresultatet hade redan upptäckts genom sökfras 1 och sökfras 2. Sökfrasen behölls dock för att säkerställa att inga artiklar översågs.

Sökfras 4 använder AND ”best practice” vilket användes som en sista undersökning efter studier som kan ha framställs en egen *best practice*-lista. Dock, likt sökfras 3, ansågs det att de relevanta studierna redan hade utvunnits från sökfras 1 och 2.

Följande är tre tabeller som presenterar söktermer per databas. De visar vilka filter som användes, sökresultat, antalet artiklar utvalda på grund av titel och dess abstract och slutligen antalet utvalda artiklar baserat på dess fulla text.

Tabell 4: Litteratursökning för ACM Digital Library

Databas	Sökfras	Filter	Sökresultat	Titel & abstract	Baserad på full text
ACM Digital Library	("Smart home" or "smart homes") AND secur* AND manipulat* NOT energy	Past 5 Years	133	15	4
ACM Digital Library	(“smart home” or “Smart homes”) AND eavesdrop*	Past 5 years	151	6	2
ACM Digital Library	(“smart home” or “Smart homes”) AND Weakness*	Past 5 years	441	12	0
ACM Digital Library	(“smart home” or “Smart homes”) AND “best practice”	Past 5 years	48	2	0
			773	**35**	**6**

För ACM Digital Library behövde sökfras 1 modifieras. Sökresultatet var ursprungligen 330 men en betydligt stor mängd av resultaten fokuserade på energiförbrukning i smarta hem. Sökfras 1 ändrades då till att lägga till NOT energy för att avskärma den kategorin. Det användes bara ett sökfilter för att nå artiklar från år 2015 till 2020.

Tabell 5: Litteratursökning för IEEE Xplore

Databas	Sökfras	Filter	Sökresultat	Titel & abstract	Baserad på full text
IEEE Xplore	("Smart home" or "smart homes") AND secur*	2015-2020 Conferences, journals	402	20	5
IEEE Xplore	(“smart home” or “Smart homes”) AND eavesdrop*	2015-2020 Conferences, journals	24	8	3
IEEE Xplore	(“smart home” or “Smart homes”) AND Weakness*	2015-2020 Conferences, journals	29	5	0
IEEE Xplore	(“smart home” or “Smart homes”) AND “best practice”	2015-2019 Conferences, journals	23	4	0
			478	**46**	**9**

Ingen av sökfraserna behövde ändras för IEEE Xplore då de ansågs fungera väl. Dock eftersom IEEE Xplore bland annat har kurser som kan inkluderas i sökresultat så användes filter för att enbart få ut artiklar från konferenser och journaler.

Tabell 6: Litteratursökning för Science Direct

Databas	Sökfras	Filter	Sökresultat	Titel & abstract	Baserad på full text
Science Direct	("Smart home" or "smart homes") AND (Secure OR security OR security threat) AND manipulation	2015-2020 Review articles, Research articles	222	1	1
Science Direct	(“smart home” or “Smart homes”) AND eavesdropping	2015-2020 Review articles, Research articles	233	17	0
Science Direct	(“smart home” or “Smart homes”) AND (weakness OR weaknesses)	2015-2020 Review articles, Research articles	406	4	0
Science Direct	(“smart home” or “Smart homes”) AND “best practice”	2015-2020 Review articles, Research articles	192	2	0
			1 053	**24**	1

Science Direct var ett undantag i både söktermer och antal utvalda artiklar. Science direct är en databas som inte stödjer användningen en asterisk som boolesk operator. Som tabell 6 visar inkluderas hela ord i sökfrasen för att inkludera potentiella böjningar.

Science direct skiljer sig också i antalet utvalda artiklar. Sökresultaten resulterade i flest antal artiklar men i slutändan användes bara en artikel. Anledningen för det var ordningen databaserna användes i. Science Direct var den sista databasen i litteratursökningen vilket resulterade i att många artiklar hade förekommit i tidigare databaser och behövde inte användas på nytt. Urvalet av slutgiltiga studier är dock inte beroende av ordningen som databaserna används i eftersom studierna som förekommer på flera databaser skulle väljas ut oavsett ordningen.

Sökfraserna gör det möjligt att upptäcka artiklar med nyckelord som var förekommande under *scoping search* relaterat till åtgärderna från kapitel *2.1 Tidigare identifierade åtgärder* samtidigt som en tillräcklig mängd utifrån arbetets tidsplan kan undersökas.

Som det beskrevs i kapitel *4.1.2 Databaser* användes även snöbollsmetoden vilket resulterade i sex ytterligare studier vilket gjorde att det totala antalet utvalda studier blev 22, se bilaga 1 för en tabell med vilka slutgiltiga studier som blev utvalda.

4.4 Data extraktion

Scoping search utförs i samband med grundläggande frågor för data extraktion. En kartläggande granskning ska kategorisera och finna luckor potentiella i litteratur och behöver därför kategorisera data från den valda litteraturen (Grant & Booth, 2009). Det behöver fastställas en bas med bevis för studierna för att de skall kunna kartläggas och analyseras.

Därför ställs två primära frågor till artiklar i den här studien när dataextraktion först utförs:

1. Diskuterar studien manipuleringsmetoder mot smarta hem?

2. Diskuterar studien åtgärder för att hantera manipuleringsmetoder?

För att kunna extrahera relevant data för studien behöver svaret på dessa frågor vara ett ja. Efter det kan fyra ytterligare följdfrågor ställas för att få en mer djupgående analys:

3. Diskuteras ytterligare åtgärder utöver de tio åtgärderna från kapitel *2.3.1 Tidigare identifierade åtgärder?*

4. Vilka åtgärder rekommenderar studierna skall tas mot olika manipuleringstekniker?

När alla studier har analyserats utifrån de fyra första frågorna behöver två slutgiltiga frågor besvaras för att identifiera gemensamma nämnare och olikheter:

5. Vilka åtgärder kan användas av användare?

6. Vilka åtgärder kan användas av utvecklare?

De sex frågor som ställs används för att möjliggöra en kartläggande granskning för att kunna besvara frågeställningen för den här studien och tydligt extrahera vilka åtgärder kan appliceras av användare eller utvecklare. Frågorna är framtagna från Booths et al. (2016) rekommendationer för frågor att utgå ifrån med en anpassning för studiens frågeställning och område.

4.5 Studiers validitet

I samband med dataextraktionen utförs även en kvalitetsbedömning av studier för att bedöma studiers validitet. Då en kartläggande granskning inte skall fokusera på att bedöma utvalda studiers kvalité valdes det ändå att utföras en grundläggande kvalitetsbedömning. Detta på grund av att de utvalda studiernas kvalité behövde bedömas till hur väl de förhåller sig till den här studiens frågeställning och syfte. Varje studie har sina brister men för att utföra en systematisk kartläggande studie behöver bristerna i studierna värderas. Värderingen avgör om bristerna är så kritiska att studien blir oanvändbar eller om det är acceptabla och fortfarande kan användas till sammanställningen. En svaghet i en studie kan exempelvis bedömas som kritisk om resultaten från den skulle påverkas av att de som utförde den hade otillräckliga resurser för att genomföra eller om studien behövde avbrytas. Om en studies svaghet istället har en minimal inverkan på resultatet behöver den inte avfärdas (Booth, et al. 2016).

För att bemöta detta undersöks utvalda studiers fulla text för att säkerställa att de följer sin upplagda plan och inte är partiska till något utfall i deras studier. Studiernas validitet i korrelation till den här studien säkerställs även genom att försäkra att de sex frågor som ställs i kapitel *4.4 Data extraktion* är besvarade. Detta undersöks i samband med att läsa den fulla texten från dem utvalda studierna.

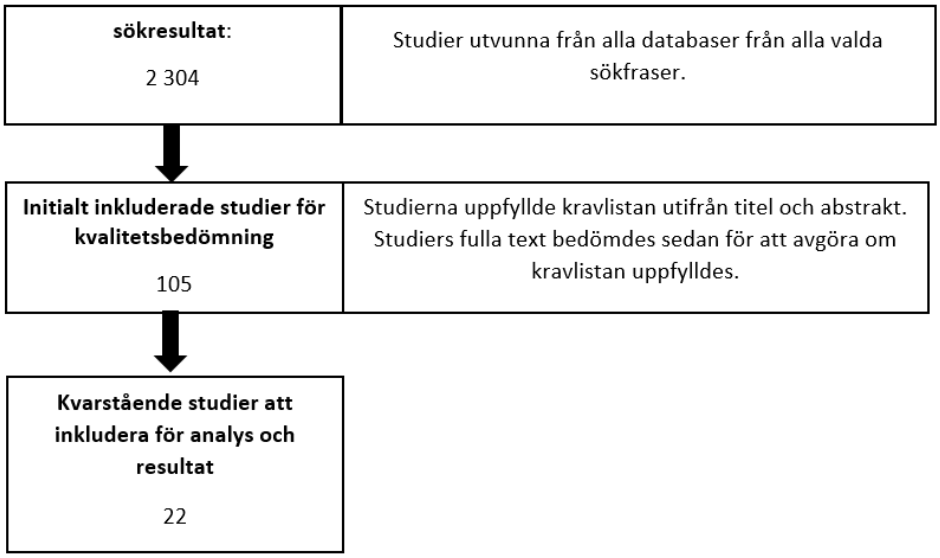
De tre utvalda databaserna, ACM Digital Library, IEEE Xplore & Science Direct, publicerar enbart studier som har blivit *peer-reviewed.* Detta säkerställer att studier därifrån har blivit granskade av experter inom området. Att även använda snöbollsmetoden försäkrar att inga artiklar från andra databaser uteblev. Artiklar utvunna från snöbollsmetoden granskades även manuellt för att försäkra att de tidigare hade blivit *peer-reviewed*, då det inte är ett kriterier för att artiklar skall publiceras på alla databaser.

5. Genomförande

Följande kapitel presenterar hur den valda metoden sätts i verk i med hjälp av dem framtagna sökfraserna. Det utvalda artiklarna blir sedan analyserade och data som är relevant till frågeställningen extraheras för att möjliggöra ett resultat för studien. Analysen och resultatet presenteras i form av kategorisering och tabeller. Slutligen presenteras en slutsats med ett ramverk baserat på studiens resultat.

5.1 Urval av studier

Studierna som valdes ut följde Booth et al. (2016) metod för att granska studier utifrån en sökfras, se figur 6.



Figur 6: Flödesschema för resultat av utvalda artiklar för studien (Författarens egen).

Sökresultatet för den valda sökfrasen var 2 304 olika studier som sedan bedömdes utifrån de inkluderingar och exkluderingar för studien, se kapitel *4.1.1 Inkluderingar & exkluderingar*. Som det presenteras i figur 6 exkluderades studier utifrån deras titel och abstrakt då i detta skede var möjligt att avgöra om studien gynnade frågeställningen. Till exempel exkluderades artiklar som enbart undersökte IoT och inte smarta hem. Även dubbletter och studier som inte var tillgängliga kostnadsfritt exkluderades här. 105 studier gick vidare för granskning där samtliga studier bedömdes i sin helhet. Frågeställning, metod och resultat granskades utifrån den här studiens forskningsmål. Om en artikel till exempel enbart identifierade sårbarheter och hot hos IoT i smarta hem utan att diskutera åtgärder eller metoder för hantering så exkluderades artikeln.

Detta på grund av att den i slutändan inte har möjlighet att bidra användbar data för den här studien. Studien behövde framföra förbättringsförslag eller åtgärder för IoT i det smarta hemmet. Åtgärderna kunde vara liknande eller andra åtgärder än vad Abdullah et al. (2019) presenterar. Vad som återstod var 22 studier som kunde analyseras då dessa ansågs uppfylla kriterierna som var utvalda för den här studien.

5.2 Analys och resultat

Följande kapitel presenterar analysen av de 22 studier som används för att besvara den här studiens frågeställning. Studierna granskades och presenteras med den kartläggande granskningens i form av en identifierad kategorisering från studierna (Booth et al. 2016). Se Bilaga 1 för en övergripande sammanfattning av vilka studier som valdes ut och vilka åtgärder de rekommenderar. De utvalda studiernas identifierade åtgärder kunde sedan kategoriseras i samband med Abdullahs et al. (2019) åtgärder.

Genom att utgå från åtgärderna från Abdullahs et al. (2019) studie kunde ytterligare kategorisering användas där det ansågs behövdas. Genom att kategorisera de utvalda artiklarnas åtgärder kunde analysen utföras för att möjliggöra en tydligare avgränsning för vilka åtgärder är lämpade för användare och utvecklare.

Det används sju huvudkategorier som innefattar åtgärder för antingen användare eller utvecklare eller båda parterna. Trots att åtgärderna utgår från Abdullah et al. (2019) som diskuteras i kapitel 2.3.1 *Tidigare identifierade åtgärder* skiljer dock en kategori, *Åtgärder för utvecklare av IoT-enheter*. Kategorin skiljer sig då den den är enbart ämnad för utvecklare, i den ingår tre underkategorier ämnade för utvecklare.

Flera av de utvalda studierna är inte begränsade till enbart en kategori utan kan befinna sig i fler. Åtgärdskategorierna härstammar från Abdullah et al. (2019) med förtydligande från de ursprungliga engelska titlarna och en anpassning för den här studien. Åtgärdskategorierna är följande:

- Riskbedömning.
- Övervakning av nätverkstrafik och enheter.
- Kryptering.
- Uppdatering av enheter i det smarta hemmet.
- Stark och förbättrad autentisering & auktorisering.
- Implementering och konfigurering av säkerhetsskydd.

- Åtgärder för utvecklare av IoT-enheter.
  - Utveckling av en universal standard.
  - Ökad kapacitet för enheters hårdvara.
  - Strängare krav på autentisering från utvecklare.
  - Utbildning av användare och intressenter.

5.2.1 Riskbedömning

Likt Abdullah et al. (2019) identifierar tre av de utvalda studierna riskbedömning som en förebyggande åtgärd mot manipuleringsmetoder. Detta genom att ha kunskapen om vad som kan ske och hur det bäst skall bemötas. Riskbedömning är när risker identifieras och bedöms för att avgöra hur allvarliga riskerna är. En riskbedömning i det här sammanhanget kan användas för att undersöka vilka risker kan drabba det smarta hemmet. På så sätt kan det i tidigt skede förebyggas att manipulation av IoT-enheter kan inträffa.

Den som kan nyttja av en riskbedömning kan bero mycket på kunskapsförmågan. En kvalificerad riskbedömning är nödvändigtvis inte något som utförs av en användare i vardagen och kan därför vara en metod som är bättre lämpad för utvecklare.

Osisiogu (2019) kategoriserar hot mot smarta hem i två kategorier, fysiska och cyberhot. Användandet av CIA-triaden, som står för konfidentialitet, riktighet och tillgänglighet, anses vara en metod för att få en uppskattning på hur hoten mot det smarta hemmet skall bemötas (Osisiogu, 2019; Park et al. 2019).

Park et al. (2019) och Pandey, Collen, Nijdam, Anagnostopoulos, Katsikas & Konstanstas (2019) presenterar båda åtgärder i form av mer automatiserade riskbedömning för övergripande hot mot smarta hem. Att förebygga attacker från utomstående angripare är inkluderade i dessa hot. Parks et al. (2019) studie fokuserar på hoten som kan uppstå på grund av sensorteknik i IoT-enheter som till exempel touchskärmar på smarttelefoner och AI-högtalare. Som det diskuterades i kapitel *2.3.3 Avlyssning & Imitering* kan angripare genom olika sensorattacker installera *malware* på IoT-enheter som i följd låter angriparen få någon grad av kontroll över enheterna. Attackerna mot sensorteknik kan vara en väg att få tag på användares inloggningsuppgifter (Park et al. 2019). För att möta och åtgärda hoten diskuterar ibid användandet av CIA-triaden men presenterar en egen riskbedömningsprocess. Denna riskbedömningsprocess skall vara anpassningsbar med realtidsrespons på grund av dem ständigt utvecklade hoten.

Även Pandey et al. (2019) presenterar en riskbedömningsprocess utvecklad för smarta hem som de förkortar till RAM. De använder *malware* som exempel där deras RAM avgör vilken den bästa åtgärden för problemet är för att minska eller åtgärda hot mot smarta hem. Det optimala resultatet för RAM är att förhindra hot från att ske från första början. Dock behöver Pandleys et al. (2019) RAM vara hårdkodad för att fungera per hotscenario. Detta i följd kan minska användarvänligheten för användare och vara mer inriktad för utvecklare.

5.2.2 Övervakning av nätverkstrafik och enheter

Den här åtgärdskategorin härstammar från Abdullahs et al. (2019) åtgärd *Monitoring the Network.* Nio av de utvalda studierna identifierar nätverksövervakning som en viktig del för att upptäcka avvikelser som kan uppstå när enheter kan ha blivit övertagna eller inte beter sig som de skall, vilket kan tyda på manipulation. Nätverksövervakning riktar in sig mot både användare och utvecklare men kräver dock att användare besitter ett tekniskt engagemang och kunskap över hur det fungerar. Detta kan göras genom att använda programvara som till exempel Wireshark. Genom att övervaka nätverket kan sårbarheter upptäckas och vissa program kan även bidra till att uppdatera IoT-enheterna (Abdullah et al. 2019).

Enligt Heartfield, Loukas, Budimir, Bezmeskij, Fontaine, Filippoupolitis& Roesch (2018) och Batalla, Vasilakos & Gajewski (2017) kan övervakning av IoT-enheterna i det smarta hemmet kan hjälpa mot att förhindra otillåten åtkomst. Detta i kombination med väl implementerat skydd för hemmanätverket för att förhindra olika former av manipuleringar som kan förekomma, som till exempel modifiering eller borttagning av meddelanden (ibid).

Likt Lin & Bergmann (2016) anser Serror et al. (2018) att själva nätverket är ett stort problemet som möjliggör attacker mot IoT-enheterna i det smarta hemmet. Både Park et al. (2019) och Serror et al. (2018) diskuterar bland annat användandet av avlyssningsattacker för att få åtkomst till root-rättigheter för att kunna manipulera systemet. Ibid föreslår kommunikationsregler som specificerar beteendet för varje IoT-enhet. “Communication rules specify the IP addresses (or hostnames) as well as port numbers and communication direction that need to be permitted to realize the intended functionality of a specific IoT device, similar to, e.g., rules for firewalls.” (Serror et al. 2018, s.4). Enligt ibid kan förbättrad *in-network* säkerhet behövas för att avlasta hemanvändare från komplicerade konfigurationer då det kan automatiskt anpassas till de anslutna enheterna och tjänsterna.

Detta skall enligt ibid ge varje IoT-enhet i hemmet en specifikation av den kommunikation som behövs för att utföra tjänsterna, genom att då ge hemmaroutern det ansvaret. Ibid anser att dessa regler kan implementeras av användaren i hemmet med hjälp av professionell hjälp, forum på internet eller egen kunskap. Nätverksövervakning baserad på maskinlärande kan enligt ibid hjälpa det smarta hemmet att identifiera och potentiellt isolera äventyrade IoT-enheter. Genom att använda maskinlärande tekniker kan övervakningen automatiseras med vetskapen att en automatisering kan vara för strikt. Ibid föreslår därför en kombination av kommunikationsregler och maskinlärande nätverksövervakning för att säkra nätverket mot utomstående attacker.

Även Ramapatruni, Narayanan, Mittal, Joshi & Joshi (2019) anser att nyttja maskinlärningstekniker för att motverka hackning vore effektivt. Detta genom att utnyttja maskinlärning för identifikation av dolda aktiviteter i det smarta hemmet. Deras artefakt kan användas för att lära sig det typiska beteendet av IoT-enheterna i det smarta hemmet för att upptäcka avvikelser. Om utvecklare erbjöd det skulle det underlätta arbetet för användare att hålla deras smarta hem säkert.

Likt Abdullah et al. (2019) beskriver Khawla & Tomader (2018) en form av imiteringsattack för att manipulera system, Sybil-attacker. Det är en form av attack för att manipulera system genom att angripare imiterar en verklig användare. Khawla & Tomader (2018) hänvisar till Demirbas & Song (2006) som föreslår att upptäcka en sybil-attack genom en övervakningsmetod genom att mäta signalstyrkan i korrelation med andra noder.

Sapalo Sicato et al. (2019) identifierar hot beroende på fyra lager som IoT-enheter primärt är uppbyggda på. Applikationslagret, mellanprogramvara-lagret, nätverkslagret och *perception*-lagret. Kategoriseringen för att identifiera hot beroende på lager skiljer sig från de tidigare studierna i metod för identifiering men de identifierade hoten går i linje med de andra utvalda studierna. Ibid presenterar ett ramverk för ett *Intrusion Detection and Prevention (*IDPS) för ett smart hem. Karimi & Krit (2018) anser att ett IDS-system är användbart för att även hjälpa användaren att inte behöva utföra övervakning manuellt. Deras lösning är fokuserad på att hantera hoten redan vid det smarta hemmets router. Lösningen skulle inte enbart hantera hoten från *malware*-typen VPNfilter utan också mot andra sortens *malware*-attacker (Sapalo Sicato et al. 2019). Systemet bygger på en IDPS-baserat maskinlärande algoritm för att förutspå och upptäcka avvikelser i nätverket. Osisiogu (2019) identifierar också en nödvändighet att använda system med självlärande algoritmer för att åtgärda hot mot IoT-enheter i det smarta hemmet. Enligt Osisiogu (2019) kan det i följd hjälpa utvecklingen av säkrare IoT-enheter mot cyberhot. Även om Sapalo Sicatos et al. (2019) använder sig av en artefakt som än inte är tillgänglig för

allmänheten finns det flera gratis IDS-system som användare i det smarta hemmet kan använda sig av.

5.2.2 Kryptering

Den här Åtgärdskategorin är en kombination av ibids åtgärder *Utilizing Effective Encryption* och *Using Private Network*. Kombinationen gjordes då separationen av åtgärderna inte ansågs nödvändig för identifiering av vem som bär ansvaret för uppgifterna. Likt Abdullah et al. (2019) identifierar tre ytterligare studier behovet av kryptering som en väsentlig del för att säkra det smarta hemmet mot yttre hot som avlyssnad trafik då det i följd kan leda till imitering och malware. Som Fouladi & Ghanoun (2013) skriver kan bristande kryptering leda till övertagning av enheter i det smarta hemmet, som till exempel smarta dörrlås. Karimi & Krit (2019) menar att kryptering kan hjälpa mot externa hot som man-in-the-middle attacker.

Användningen av krypteringsmetoder kan användas av både användare och utvecklare. Användare kan nyttja den kryptering som kommer med enheterna de implementerar i det smarta hemmet som till exempel medföljande kryptering i hemmaroutern. Utvecklare kan istället se till att deras produkter besitter bra krypteringsmetoder som bland annat (Batalla et al. (2017) rekommenderar. Batalla et al. (2017) identifierar hot som avlyssning, övertagning och kapning så angriparen kan få kontroll över enheter och eller göra att användare blir av med data. Enligt ibid skall användning av kryptering ge ett betydligt bättre skydd mot den formen av attacker. Ibid anser att AES-kryptering skall användas för dataöverföring, RSA för hantering av publika nycklar och digitala signaturer för delade nycklar. Ibid rekommenderar att antingen använda sig av statisk kryptering eller dynamisk kryptering.

En åtgärd i linje med kryptering som Abdullah et al. (2019) rekommenderar är att det smarta hemmet använder sig av krypterad VPN. Detta för att VPN gör att det finns en säker kommunikationskanal som blir svårare att få åtkomst till för angriparen. Likt det rekommenderar Oconnor, Ench & Reaves (2019) liknande åtgärd, Per-IoT VPN. Enligt Oconnor et al. (2019) hjälper VPN med att skydda mot manipulering från avlägsna attacker över internet men VPN skyddar dock inte mot lokalt övertagna routrar. Per-IoT VPN möjliggör att IoT-enheter kan själva upprätta VPN för att skydda sig. Per-IoT VPN är en åtgärd som också är möjlig som användare kan utnyttja.

5.2.3 Uppdatering av enheter i det smarta hemmet

Den här åtgärdskategorin baseras på Abdullahs et al. (2019) åtgärd *Updating the Software.* Utöver Abdullah et al. (2019) identifierar fem av de utvalda studierna behovet att uppdatera IoT-enheterna i det smarta hemmet. Kategorin är ämnad för både utvecklare och användare. Utvecklarna kan säkerställa att deras produkter har automatisk uppdatering eller påminner användare att uppdatera när tillgängliga finns. Användarna har i sin tur ansvaret att uppdatera enheterna manuellt om en automatisk uppdatering inte finns tillgänglig.

En hörnsten för att åtgärda manipulering av IoT-enheterna i det smarta hemmet är att se till att all firmware och programvara för IoT-enheterna som används i hemnätverket alltid har den senaste uppdateringen (Abdullah et al. 2019; Sapalo Sicato et al. 2019). Sapalo Sicato et al. (2019) betonar vikten av aktuella uppdateringar på enheterna då det anses vara en kritisk åtgärd för att motverka hot. Utvecklarna av enheten arbetar förhoppningsvis med att fortsatt säkra IoT-enheten genom att uppgradera mjukvaran med nya patch-versioner. Äldre versioner kan fortfarande ha sårbarheterna som en ny version har åtgärdat (Abdullah et al. 2019).

Enligt Khawla & Tomader (2018) skall firmware uppdateras regelbundet. För att utföra säkra uppdateringar rekommenderar Khawla & Tomader (2018) att göra det genom krypterade kommunikationsvägar och säkrade servrar för uppdatering av filer för att i följd motverka att enheter kan bli utsatta för kapning. En annan metod för uppdateringar rekommenderar Han, Jeon & Kim (2015) att använda sig av kontroller för att veta att uppdateringar av firmware är äkta. Detta med bra funktioner för autentisering och vem som har kontroll till vad samt krypteringsmetoder.

För att hantera besvären med redan infekterade enheter som kan manipuleras utvecklar Huth, Duplys & Güneysu (2016) ett protokoll för att bland annat möjliggöra en säker firmwareuppdatering på redan infekterade enheter. Om IoT-enheten är intrigerad i ett smart hem kan en skadegörande uppdatering av firmware vara sårbart för hemmet och användaren kan förlora kontroll. Då en manipulerande malware behöver tid på sig att gömma sig efter en skanning av en IoT-enhet vid uppdateringar kan protokollet upptäcka det. För att inte IoT-enheten skall kunna användas för imitering har Huth et al. (2016) implementerat fysiska funktioner som inte möjliggör kloning, imitering.

Ali, Dustgeer, Awais & Shah (2017) anser att attacker som avlyssning är passiva där information samlas men systemet förändras inte. Aktiva attacker är sedan när informationen kan modifieras och användas mot det smarta hemmet.

Ali et al. (2017) rekommenderar att enheter uppdaterade med hjälp av att enbart auktoriserade användare kan utföra uppdateringarna. I korrelation med det, och för att ha någon chans att skydda sig mot angripare, måste det finnas starka inloggnings och auktoriseringsuppgifter (Ali et al. 2017).

5.2.4 Stark och förbättrad autentisering & auktorisering

Den här kategorin baseras på Abdullah et al. (2019) åtgärd *Changing Credentials Regularly*. Genom den tidigare forskningen upptäcktes det att ibids kategori kunde delas upp i två kategorier för den här studien. Detta för att tydligare avgränsa vem åtgärden är applicerbar för, användare eller utvecklare. Fyra av studierna anser att starka autentiseringsmetoder och eller auktorisering kan säkra det smarta hemmets enheter mot olika former av manipulering. Som det diskuterades i kapitel *2.3.3 Avlyssning & imitering* blir imiteringstekniker svårare att genomföra om inloggningsuppgifter och rättigheter är starka. Som det skrevs i tidigare kapitel anser Ali et al. (2017) att för att det smarta hemmet skall ha någon chans att skydda sig mot angripare behöver starka inloggningsuppgifter och tydliga rättighetsregler finnas.

Kategorin drabbar både användare och utvecklare då användarna har möjligheten att själva ansvara över hur starka inloggningsuppgifter de har och enheternas autentiseringskrav.

Dock faller även ansvaret på utvecklare att implementera möjligheten att ha bra autentiseringsmetoder från början. Batalla et al. (2017) rekommenderar, likt Jia, Li, & Gao (2017) och Han et al. (2015), att använda bra metoder och följa befintliga riktlinjer för autentisering för att säkerställa att enbart behöriga kan få tillgång till det smarta hemmet.

5.2.5 Implementering och konfigurering av säkerhetsskydd

För att skydda sig mot olika manipuleringstekniker, som avlyssning och imitering identifierades anses den här åtgärdskategorin vara nödvändig. Den härstammar från Abdullahs et al. (2019) åtgärd *Backup Significant Information*. Den här åtgärdskategorin är bredare än ibids åtgärd för att inkludera fler befintliga metoder för att säkra det smarta hemmet som tidigare forskning identifierar.

Den här kategorin berör både utvecklare och användare i det smarta hemmet. Sex av de utvalda studierna rekommenderar och identifierar behovet av implementation av ytterligare säkerhetsskydd för det smarta hemmet. Då de befintliga skydd som finns behöver hanteras rekommenderas det att använda ytterligare för att säkra det smarta hemmet. Jia et al. (2017) föreslår en åtgärd i form av ett semi-automatiserad system som de själva har utvecklat som skall kunna upptäcka brister i IoT-enheter redan efter utveckling. Systemet undersöker om det förekommer bristande kryptering, öppna portar eller svaga lösenordshanteringar som kan utnyttjas av angripare. Om utvecklare nyttjar ibids system kan det hjälpa förebygga att osäkra produkter släpps på marknaden. Feng, Swaminathan & Wei (2017) föreslår användandet av hårdvaruisolering som åtgärd för att motverka manipuleringstekniker som replay-attacker. ” Hardware isolation provides the system and upper level applications with a lower level security mechanism by physically isolating the trusted system components from the untrusted ones.” (Feng et al. 2017, s.234).

Fyra andra studier fokuserar mer på att stärka skyddet mot manipuleringsmetoder över redan befintliga skyddsmetoder. Sapalo Sicato et al. (2019) rekommenderar en metod för att motverka manipulering som kan ske av *malware* och dataintrång via användarens router. Detta är att stänga av fjärrstyrning och ändra inloggningsuppgifterna till något säkrare än dem som medföljer. I samband är det viktigt att de säkerhetsåtgärder som finns implementerat är uppdaterade (Ibid). Det är även viktigt att de enheter som har möjlighet är säkrade med en uppdaterad brandvägg för att hantera yttre hot (Abdullah et al. 2019). För att motverka cyberattacker från angripare föreslår Ur Rehman & Gruhn (2018) Implementationen av ett sicher brandväggssystem som placeras mellan en central enhet som är bryggan till internet, som en router, och till enhet central till hemmet.

Jose et al. (2016) presenterar deras egen algoritm för *device fingerprinting* som bland annat gör listor för tillåtna och otillåtna enheter för att säkra hemmet. Detta med hjälp av presenterade inloggningsuppgifter gjorde att Jose et al. (2016) såg en tydlig förbättring i hemmets säkerhet för att förhindra otillåten åtkomst. Även Oconnor et al. (2019) diskuterar metoder för att stärka brandväggen så angripare inte kan ta kontroll över enheter. Oconnor et al. (2019) föreslår Traffic shaping för att förhindra manipulering av trafik, metoden bland annat implementeras med hjälp av brandväggskonfigurationer. Det är en metod för att se till att HTTPS trafik inte läcker känslig information vilket Ibid anser är nödvändigt om kryptering inte är tillräckligt för att skydda IoT-enheterna. Dock anser ibid att det behöver utföras ytterligare forskning för att metoden är fullt säker.

Som en slutgiltig säkerhetsåtgärd rekommenderar som sagt även Abdullah et al. (2019) att genomföra regelbundna säkerhetskopieringar av enheter i hemmet. Detta är väsentligt att ha om andra säkerhetsåtgärder inte var tillräckliga och data förlorades.

5.2.6 Åtgärder för utvecklare av IoT-enheter

I tidigare kapitel har det diskuterats åtgärder som både utvecklare och användare i det smarta hemmet kan använda sig av, beroende på deras tekniska förmåga. Dock finns det åtgärder som anses tydligt vara bortom användaren kontroll och kan eller bör nyttjas av enbart utvecklarna.

Följande kapitel kommer därför att diskutera åtgärder ämnade för utvecklare och då det anses vara bortom användarens kontroll för att skydda det smarta hemmet mot manipulering och övertagande av IoT-enheter.

5.2.6.1 Utveckling av en universal standard

Den här kategorin baseras på Abdullahs et al. (2019) åtgärd *Applying up-to-date Protocols*. Utöver ibid identifierar ytterligare två av de utvalda studierna att en stor utmaning för utvecklare är avsaknaden av en universal standard för IoT. Detta försvårar implementationen av genomgående bra säkerhet (Abdullah et al. 2019; Davis et al. 2020). En saknad homogenitet hos alla olika enheter som sammankopplas i hemmet försvårar utmaning att implementera säkerhet i det smarta hemmet. Det finns dock i nuläget dedikerade grupper som försöker bemöta problemet. Lin & Bergmann (2016) skriver om hur grupperna exempelvis har arbetat för en standard för att utmana det klassiska TCP/IP protokollet med ett protokoll för IoT, IETF IoT protokollet. Detta inkluderar bland annat IPv6 över trådlösa personliga nätverk med låg kapacitet. IETF standarder bidrar med säkra mekanismer för säker webbaserad kommunikation inom begränsade nätverk (Lin & Bergmann, 2016).

5.2.6.2 Ökad kapacitet för enheters hårdvara

Den här kategorin utgår från Abdullahs et al. (2019) identifierade sårbarhet *Limited Storage and CPU*. Utöver ibid var det tre ytterligare av de utvalda studierna som ansåg att enheters begränsade hårdvara var ett problem som behövde åtgärdas. Att öka kapaciteten för enheters hårdvara kan agera som en åtgärdskategori som möjliggör förbättrad säkerhet.

Karimi & Krit (2019) anser att hårdvarubegränsningarna som finns i ett smart hem behöver ses över trots att det i nuläget utvecklas nya algoritmer och enheter i försök att hantera det.

Många enheter i det smarta hemmets systemresurser anses vara en begränsning eftersom hårdvaran är begränsad och klassisk säkerhet som implementeras på traditionella datorer inte kan utföras (Lin & Bergmann, 2016; Oconnor et al. 2019). För att åtgärda IoT-enheters begränsade hårdvara så föreslår Lin & Bergmann (2016) att utnyttja möjligheten till att ha molnbaserade lösningar för IoT-enheter. På det sättet kan molntjänster avlasta IoT-enheterna genom att bidra till övervakning, lagring och hantering av data (Lin & Bergmann, 2016).

Lin & Bergmann (2016) skriver också att användandet av en IoT-gateway kan bidra till ett centraliserat hanteringsverktyg för anslutna IoT-enheter i det smarta hemmet som ansluts via det. En IoT-gateway kan ha mer prestanda och kan klara av mer säkerhet och kan agera som en brandvägg för att skydda IoT-enheterna ytterligare mot utomstående hot och minska attackytan (Lin & Bergmann, 2016).

5.2.6.3 Strängare krav på autentisering från utvecklare

Den här åtgärden är den andra uppdelningen av Abdullahs et al. (2019) åtgärd *Changing Credentials Regularly.* Som det beskrevs tidigare anses en uppdelning av ibids åtgärd ge en tydligare avgränsning för att undersöka om utvecklare eller användare har kontroll över åtgärden. Detta visade att två av de utvalda studierna identifierar behovet av strängare krav på autentisering från utvecklarna. Den autentiseringen som är tillgänglig på många IoT-enheter i hemmet är i många fall otillräcklig vilket kan vara en grundorsak till att enheter kan bli manipulerade.

Enligt Davis et al. (2020) behöver utvecklare ställa högre krav på enheters inloggningsuppgifter för att skydda enheterna. Till exempel kan utvecklare ha som krav att inloggningsuppgifter för en router ändras från standardinloggningen efter routerns första inloggning (Abdullah et al. 2019). Zhou, Jia, Yao, Zhu, Guan, Mao, Liu & Zhang (2019) anser att de nuvarande autentiseringsåtgärderna inte är tillräckliga för att hindra en angripare från att få åtkomst och ta kontroll över en enhet och manipulera den. Ibid föreslår därför att utvecklarna av IoT-enheterna implementerar ett unikt klientcertifikat i varje IoT-enhet. Genom att även säkra molnet som IoT-enheterna ansluter sig till hjälper till en konstant relation där enheter behöver tillstånd av molnet för varje inloggning. Detta kan åtgärda när angripares enheter försöker ta över en inloggningsprocess.

Zhou et al. (2019) framför också åtgärdsförslag för utvecklare hur enheter skulle bevisa sin validitet för att förhindra kapning. Även Abdullah et al. (2019) anser att en nödvändig åtgärd mot hoten är genom att utvecklare implementerar uppdaterade och aktuella kommunikationsprotokoll.

5.2.6.4 Utbildning för användare och intressenter

Den här åtgärdskategorin härstammar inte från Abdullahs et al. (2019) studie utan identifierades från två av de utvalda studierna, den anses dock vara användbar som en förebyggande åtgärd för det smarta hemmet.

Tabassum, Kosinski & Lipford, (2019) utförde en intervjustudie som identifierar vad för hot användare är rädda ska drabba dem och deras smarta hem. Att IoT-enheter i hemmet skall bli hackade och att användare förlorar kontroll över deras enheter var ett av hoten som skrämde användare men ur deras synvinkel var inte *malware* hotet. Övertagande och manipulering av enheterna ansågs istället kunna leda till spionage och inbrott för användare som använde övervakningssystem och digitala lås för ytterdörrar. Användare litar på att utvecklarna för produkten skall skydda deras data då det är för tungt ansvar för användaren att kontrollera all data som delas mellan de smarta enheterna. För att åtgärda den blinda tillit som kan leda till att deras enheter blir hackade diskuterar Tabassum et al. (2019) ett behov av någon centraliserad utbildningsplattform som användare kan ta del av. Det kan hjälpa användare och utvecklare att enklare ta del av information hur det smarta hemmet kan säkras. En centraliserad utbildningsplattform kan hjälpa med åtgärden *Stark och förbättrad autentisering & auktorisering* då användare och utvecklare enklare kan ta del av vilka säkerhetsåtgärder bör implementeras. Även Osisiogu (2019) anser att genom engagemang och utbildning av intressenter kan potentiella hackningsattacker förebyggas redan i utvecklingsfasen.

5.3 Slutsats

Följande kapitel diskuterar den slutsats som resulterade från analysen och kategoriseringen av åtgärder från de utvalda artiklarna. Genom att utgå från Abdullahs et al. (2019) åtgärder i kombination med att utföra litteratursökningen kunde ett ramverk skapas för att tydligt visa vilka åtgärder som kan användas av användare och utvecklare.

5.3.1 Ramverk med åtgärder för användare/utvecklare

Åtgärdskategoriseringen av analysen och resultatet från Abdullah et al. (2019) och den tidigare forskningen visar flera åtgärder som användare och utvecklare kan ta del av som anses vara effektiva åtgärder för att förebygga manipulation av IoT-enheter i det smarta hemmet. Följande kapitel presenterar vilken part kan nyttjas av de olika åtgärderna från kapitel *5.2 Analys och resultat.* Se tabell 7 för ett ramverk med detta. Tabell 7 visar de åtgärder som anses vara applicerbara med en ✓ för användare eller utvecklare. En ✓ inom parentestecken tyder på att åtgärden kan användas men har begränsningar för den parten som den förekommer i. Begränsningen förklaras i text efter tabell 7. Ordningen som tabell 7 presenterar åtgärdskategorierna är efter den ordningen som författaren av den här studien anser att ordningen bör utföras i, med start högst upp i tabellen.

Tabell 7: Ramverk som illustrerar vilken part, användare/utvecklare, kan använda en åtgärdskategori.

Åtgärdskategorier i en rekommenderad ordning för användning	Antal utvalda studier som rekommenderar åtgärd	Användare	Utvecklare	Studie som identifierade åtgärd
Ökad kapacitet för enheters hårdvara	3		✓	Lin & Bergmann (2016); Oconnor et al. (2016); Karimi & Krit (2019)
Utveckling av en universal standard	1		✓	Lin & Bergmann (2016)
Utbildning för användare och intressenter	2		✓	Tabassum et al. (2019); Osisiogu (2019)
Riskbedömning	3	(✓)	✓	Park et al. (2019); Osisiogu (2019); Pandey et al. (2019)
Strängare krav på autentisering från utvecklare	2		✓	Zhou et al. (2019); Davis et al. (2020)
Stark och förbättrad autentisering & auktorisering	4	✓	✓	Batalla et al. (2017); Jia et al. (2017); Han et al. (2015); Ali et al. (2017)
Kryptering	3	✓	✓	Batalla et al. (2017); Han et al. (2015); Fouladi et al. (2013)
Övervakning av nätverkstrafik och enheter	9	(✓)	✓	Serror et al. (2018); Batalla et al. (2017); Heartfield et al. (2018); Sapalo Sicato et al. (2019); Lin & Bergmann (2016); Park et al. (2019); Ramapatruni et al. (2019); Khawla & Tomader(2018); Osisiogu (2019)
Uppdatering av enheter i det smarta hemmet	5	✓	✓	Sapalo Sicato et al. (2019); Khawla & Tomader(2018); Han et al. (2015); Huth et al. (2016); Ali et al. (2017)
Implementering och konfiguration av säkerhetsskydd	6	✓	✓	Oconnor et al. (2019); Jia et al. (2017); Rehman et al. (2018); Jose et al. (2016); Feng et al. (2017); Sapalo Sicato et al. (2019)

Några åtgärdskategorier kan anses vara problematiska att införa i dagsläget, som utveckling av en universal standard. Åtgärdskategorierna är dock upplagda utefter vad författaren för den här studien anser ordningen de bör utföras i och inte nödvändigtvis vad som är omedelbart applicerbart.

5.3.2 Rekommenderad ordning och applicering för åtgärdskategorier

Följande kapitel beskriver varför den rekommenderade ordningen för åtgärdskategorierna valdes och hur den är applicerbar för användare och utvecklare.

Ordningen för åtgärdskategorierna börjar med tre åtgärder som är ämnade för utvecklarna. Utvecklare kan nyttja åtgärden *Ökad kapacitet för hårdvaran* då den i följd kan underlätta arbetet för *Utveckling av en universal standard* och *Stark och förbättrad autentisering & auktorisering*. Nästa steg vore för utvecklare att utveckla en universal standard i följd med att utbilda användare och intressenter för att bidra med kunskap hur åtgärder kan appliceras och användas i det smarta hemmet. Sedan kommer *Riskbedömning* vilket kan, till en vis mån, utföras av användare och utvecklare. Som det beskrevs tidigare är en kvalificerad riskbedömning möjlig att utföra beroende på kompetensnivån och intresset hos användare.

Utvecklarna kan i det stadiet bedöma hur förbättrad autentisering och auktorisering kan se ut på deras enheter då det i följd kan uppmana användare att stärka deras sätt att autentisera sig på enheter i hemmet.

När enheterna väl är implementerade i hemmet bör de vara försedda med bra kryptering. Detta är en åtgärdskategori som är primärt utvecklarens ansvar samtidigt som användare själva bör få möjligheten välja och förbättra vid behov. Enligt Abdullah et al. (2019) är användandet av VPN en metod bra för att stärka hemmet och det är en metod som användare själva kan utföra.

Implementerade enheter i det smarta hemmet bör genomgå regelbunden övervakning av nätverkstrafik och enheterna utföras för att upptäcka avvikelser som kan tyda på olika manipuleringstekniker från angripare. Denna åtgärdskategori kan användas av både användare och utvecklare. Dock som det beskrevs tidigare är nätverksövervakning en åtgärd som kräver en mer teknisk förmåga och är inte lämpad för alla användare i det smarta hemmet.

Både användare och utvecklare har möjligheten att använda åtgärdskategorin *Uppdatering av smarta enheter*. Utvecklarna har möjligheten att implementera automatiska uppdateringar på deras enheter medan användare kan själva utföra manuella uppdateringar. Enheter som är i bruk i det smarta hemmet bör också uppdateras när utvecklare gör en ny patch-version för enheter.

Slutligen kommer kategorin *Implementering och konfiguration av säkerhetsskydd* vilket är en kategori som egentligen kan placeras högre upp. Den befinner sig dock längst ner på listan då den kan anses som ett ytterligare skydd för det smarta hemmet och ger därför mer rörlighet när den kan appliceras, det är ett beslut som användare och utvecklare får ta efter eget behov.

5.3.3 Slutsats för åtgärdskategorierna utefter ramverket

Tabell 7 visar att sex av tio åtgärdskategorier är applicerbara för både användare och utvecklare och resterande fyra är alla kategorier med åtgärder bortom användares kontroll. I åtgärdskategorierna som både användare och utvecklare kan använda för att motverka manipulering kan de i flera fall även gynnas av varandra. Om en utvecklare till exempel ställer högre krav på autentisering för deras enheter kan det i följd tvinga användare att exempelvis använda bättre inloggningsuppgifter för en hemmarouter. En annat exempel kan vara att utvecklare skulle även kunna använda sig av Jia et al. (2017) system för att säkra deras produkter från *malware* innan de köps av användare.

Tabell 7 visar också två fall där användaren anses ha begränsningar för att åtgärder skall användas. Som det skrev tidigare i *5.2.1 Riskbedömning* är riskbedömning nödvändigtvis inte applicerbar för alla. Även om en användare besitter bra tekniska kunskaper är det inte en given förutsättning av användaren även kan utföra en riskbedömning baserad på CIA-triaden. Även Tabassum et al. (2019) argumenterar för att exempel IDS-system kan vara för tekniska och komplicerade åtgärder för det smarta hemmets breda sortiment av användare. Dock kan det inte uteslutas att möjligheten finns för användare, beroende på intresse och kunskapsnivåer för riskbedömning. För utvecklare som kan ha tillgångar för att utföra riskbedömningar i tidigt skede kan åtgärdskategorin vara bra lämpad för att förebygga manipulering av deras produkter.

Ett liknande scenario gäller för nätverksövervakning. Som nio studier presenterade har utvecklarna möjligheten att använda övervakning av IoT-enheter och förenkla övervakning för användare. Användare har även möjligheten att manuellt övervaka nätverk med hjälp av program som Wireshark för att upptäcka avvikelser i sitt nätverk eller IoT-enheters beteende.

Dock likt riskbedömning finns en begränsning till användares tekniska förmåga och förståelse kring hur nätverksprotokoll fungerar i grund. Det är inte begränsat till enbart utvecklare då det finns användare som besitter de kunskaperna och har engagemanget att utföra övervakning. Det samma gäller krypteringsmetoder som kan appliceras. Utvecklare har möjligheten att tillföra bra krypteringsmetoder till deras enheter men användare kan implementera ytterligare eller använda den befintliga krypteringen för att förhindra intrång. Många leverantörer har rekommendationer för hur deras produkter skall bäst hanteras av deras kunder. Det är dock upp till användaren själv om rekommendationerna för till exempel autentisering och auktorisering följs.

Vart åtgärdskategorierna skiljer sig är de som är ämnade för utvecklare. Som det beskrivs i kapitel *5.2.6 Åtgärder för utvecklare av IoT-enheter* finns det åtgärder som enbart utvecklarna har någon form av kontroll över. Åtgärderna skiljer sig då de är beroende av den faktiska tekniska utvecklingen för IoT och smarta hem. Ökad kapacitet för hårdvara och en universal standard är under ständig utveckling och är en åtgärd som de båda parterna måste acceptera att den inte är implementerbar idag. Som det beskrevs tidigare finns det enligt Lin & Bergmann (2016) grupper som arbetar för att lösa avsaknaden av en standard men det kräver fortfarande mycket arbete inom fältet IoT. Det två kategorierna är därför svåra även för utvecklare att implementera, trots behovet. Däremot kan *strängare krav på autentisering* och *utbildning av användare och intressenter* vara åtgärder som utvecklarna kan kontrollera. Strängare krav på autentisering kan direkt hjälpa mot att hantera manipulation av enheter i det smarta hemmet eftersom svaga inloggningsuppgifter för exempel en hemmarouter är en direkt väg in för en angripare.

6. Diskussion

Följande kapitel reflekterar över genomförandet och resultatet av studien och diskuterar även hur den kan användas för vidare forskning inom ämnet. Genom att utgå från Abdullahs et al. (2019) studie kunde en litteraturstudie utföras för att bryta ner säkerhetsrekommendationerna för smarta hem för att sedan identifiera vart användare eller utvecklare kan ta del av de olika åtgärderna. I de utvalda studierna är det inte alltid tydligt utskrivet för vem en åtgärd är ämnad för. Detta blev en bedömning som då behövde utgå från författarens egen förmåga för att nå en slutsats för ramverket i tabell 7. Se kapitel *5.3.2 Rekommenderad ordning och applicering för åtgärdskategorierna* för mer information kring bedömningen.

Genom att kombinera Abdullahs et al. (2019) åtgärder och sammanställa tidigare forskning bidrar den här studien med att presentera vilka åtgärder kan tas för att säkra det smarta hemmet, bara för användaren men även för utvecklare av IoT-enheter. Med hjälp av ett framställt ramverk försöker studien fylla en lucka i den tidigare forskningen angående vilka åtgärder användare har kontroll över. Samt vilka åtgärder som anses vara utvecklarnas ansvar för att säkra deras utrustning. Tidigare forskning har undersökt och visat att IoT-enheter, andra digitala medier samt det smarta hemmet är sårbara mot manipulationstekniker. Det har även framställs potentiella åtgärder som kan appliceras mot olika hot som avlyssning (Abdullah et al. 2019). Den här studien har med hjälp av den tidigare forskningen kunna fylla luckan som identifierades om vem som kan använda åtgärderna i det smarta hemmet, utvecklare eller användare. I samband med det identifieras det att det finns åtgärder som enbart utvecklare har möjligheten att implementera. Detta gör att användare behöver säkra det smarta hemmet mot manipulation till sin bästa förmåga tills det finns enheter med bättre implementerad säkerhet. Med hjälp av ramverket som presenteras i tabell 7 presenteras dock en rekommenderad ordning som åtgärderna kan/ska användas i. Detta kan förhoppningsvis hjälpa en användare att veta vart denne skall börja då det smarta hemmet kan vara mycket komplext.

De olika söktermerna uppfyllde sitt syfte för den här studien och med hjälp av snöbollsmetoden kunde även artiklar utöver de databaser som användes utvinnas. De inkluderingar och exkluderingar som används i studien anses ha varit nödvändiga för att de utvalda studierna skall kunna gynna frågeställningen. Kravlistan kan argumenteras för att ha varit för strikt och kan ha begränsat antalet utvalda studier. Trots att antalet artiklar var 22 hade alla de tidigare blivit kvalitetsgranskade och bedömts som representerande för forskningsfältet när de publicerades.

De utvalda artiklarna bedömdes sedan i den här studien för att undersöka om de bidrog till åtgärder som kunde användas för att besvara den här studiens forskningsfråga. Studien undersöker åtgärderna som bör tas för att bemöta manipulering av IoT-enheter i smarta hem men resultatet visade att det inte finns tydliga och enkla steg för att åtgärda det. Istället tyder resultatet på att en stor mängd åtgärder behöver tas för att säkra det smarta hemmet.
Åtgärderna som diskuteras kan användas för att säkra det smarta hemmet mot hoten men de är också applicerbara till flera andra hot som kan förekomma. Det finns flera hot som inte utforskats men är ett ständigt återkommande tema i de utvalda studierna för åtgärderna som rekommenderas.

Kategorin *Åtgärder för utvecklare av IoT-enheter* bidrar inte med praktiska åtgärder som användare kan applicera och möjligtvis inte heller utvecklare i dagsläget. Kategorin upplevdes dock nödvändig att inkludera då de presenterade åtgärdskategorierna behövs för att markant öka kapaciteten att kunna säkra det smarta hemmet mot övertagning och manipulation. Kategorin kan också anses vara extra viktigt då det finns en möjlighet att den kommer ha den största inverkan för att säkra smarta hem.

6.1 Hur ramverket i studien kan hjälpa användare och utvecklare

Med hjälp av ramverket kan utvecklare tydligt se vilka åtgärdskategorier de har ansvar över då användare inte har möjlighet att utföra alla åtgärder. Ordningen för ramverket illustrerar även för utvecklare vilka åtgärder behöver prioriteras för att skapa enheter för det smarta hemmet som kan bemöta olika manipulationstekniker mot hemmet.

Den rekommenderade ordningen gör det även möjligt för användare att se vart i processen att säkra det smarta hemmet de själva har kontroll över. Användare i det smarta hemmet kan ta hjälp av ramverket för att se vilka säkerhetsåtgärder är möjliga att utföra samt om de kräver en högre teknisk förmåga. Som det beskrevs tidigare är dock användarbasen för den här studien inriktad mot den användare som administrerar i hemmet. Ramverket då visar för användaren vart denna själv behöver ytterligare kunskap över åtgärdskategorier som kräver en mer teknisk förmåga, till exempel *Riskbedömning* och *Övervakning av nätverkstrafik och enheter*.

6.2 Samhälleliga och etiska aspekter

Den här studien kan förhoppningsvis bidra till ett förtydligande med vilka åtgärder behöver tas för att säkra det smarta hemmet, för både användare och utvecklare.

Ur en nätverk och systemadministratörs perspektiv kan detta ramverk agera som en checklista samt ge insikter med vilka steg bör tas för att säkra IoT-enheter.

Det diskuteras i den här studien flera sårbarheter och attackvektorer som möjliggör manipulation av IoT-enheter i det smarta hemmet. En potentiell etisk risk kan vara att den därför kan användas mot sitt syfte av till exempel en potentiell angripare. Dock diskuterar studien inte i detalj hur attackerna kan genomföras, istället diskuterar den mer generellt attackvektorer som med rätt kunskap kan användas för att angripa det smarta hemmet.

6.3 Framtida arbeten

Den här studien har möjliggjort en kartläggning av vilka åtgärder en användare och en utvecklare har kontroll över för att bemöta manipulering av IoT-enheter i det smarta hemmet. Det ramverk som presenteras i *kapitel 5.3 Slutsats* kan potentiellt användas som ett ramverk för framtida arbeten som vill undersöka vidare och djupare inom området vilka attackvektorer som kan angripa det smarta hemmet. Det kan även användas som en grund för arbeten som vill undersöka vad för konsekvenser kan uppstå från manipulering av nodbaserade enheter i det smarta hemmet.

Ett område som skulle kunna utforskas i kombination med den här studien är att utföra en kvalitativ intervjustudie för att fastställa vart gemene mans tekniska förmåga i det smarta hemmet ligger. En sådan studie skulle hjälpa för att fastställa en bas som utvecklare hade kunnat utgå från.

Referenser

Abdullah, A. A. T., Waleed, A., Sharaf, M., Abdullah, A.A. (2019) A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home. International Journal of Computer Science and Network Security, Uppl.19, no.9. ss. 139-146. Tillgänglig på internet: https://www.researchgate.net/publication/336717887_A_Review_of_Cyber_Security_Challenges_Attacks_and_Solutions_for_Internet_of_Things_Based_Smart_Home

Ali, W., Dustgeer, G., Awais, M. & Shah, M. A. (2017). IoT based smart home: Security challenges, security requirements and solutions. 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, 2017, ss. 1-6. Doi: 10.23919/IConAC.2017.8082057.

Ali, Y. & Hameed, A. (2019). Cloud Crypter for bypassing Antivirus. 2019 15th International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, 2019, ss. 1–6. Doi: 10.1109/ICET48972.2019.8994615

Al-Qaseemi, S. A., Almulhim, H. A., Almulhim, M. F. & Chaudhry, S. R. (2016) IoT architecture challenges and issues: Lack of standardization. 2016 Future Technologies Conference (FTC), San Francisco, CA, 2016, ss. 731-738. Doi: 10.1109/FTC.2016.7821686.

Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos G. & Burnap, P. (2019) A Supervised Intrusion Detection System for Smart Home IoT Devices. IEEE Internet of Things Journal, Uppl. 6, no. 5. ss. 9042-9053, Oktober. 2019, Doi: 10.1109/JIOT.2019.2926365.

Batalla, J.M., Vasilakos, A., & Gajewski, M. (2017). Secure Smart Homes: Opportunities and Challenges. ACM Comput. Surv. 50, 5, Artikel 75. Doi: 10.1145/3122816

Booth, A., Sutton, A. & Papaioannou, D. (2016). *Systematic approaches to a successful literature review*. (2: uppl.) Los Angeles: Sage.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M. & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software, volym 80, uppl 4, Elsevier, ss.571–583. Doi: 10.1016/j.jss.2006.07.009

Chu, G., Apthorpe, N. & Feamster, N. (2019). Security and Privacy Analyses of Internet of Things Children's Toys. 2019 IEEEInternet of Things Journal.Uppl.6, no 1. ss.978–985.

Clincy, V & Shahriar, H. (2019). IoT Malware Analysis. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 2019, ss. 920-921, Doi: 10.1109/COMPSAC.2019.00141.

Davis, B. D., Mason, J. C. & Anwar, M. (2020). Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. IEEE Internet of Things Journal. Doi: 10.1109/JIOT.2020.2983983.

Demirbas, M. & Song Y. (2006). An RSSI-based scheme for sybil attack detection in wireless sensor networks. 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06), Buffalo-Niagara Falls, NY, 2006 ss.-570, Doi: 10.1109/WOWMOM.2006.27.

Fakroon, M., Alshahrani, M., Gebali, F., Traore, I. (2020). Secure remote anonymous user authentication scheme for smart home environment. Internet of things, Uppl. 9. Doi: 10.1016/j.iot.2020.100158

Feng, X., Ye, M., Swaminathan, V., & Wei, S. (2017). Towards the Security of Motion Detection-based Video Surveillance on IoT Devices. Proceedings of the on Thematic Workshops of ACM Multimedia 2017 (Thematic Workshops '17). *Association for Computing Machinery, New York, NY, USA*, ss. 228–235. Doi: 10.1145/3126686.3126713

Fouladi, B. & Ghanoun, S. (2013). Security evaluation of the Z-wave wireless protocol. Black Hat USA, Uppl.1 ss. 1–6. Tillgänglig på internet: https://sensepost.com/cms/resources/conferences/2013/bh_zwave/Security%20Evaluation%20of%20Z-Wave_WP.pdf

Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G. & Baldini, G. (2017). Security and privacy issues for an IoT based smart home. 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Opatija, 2017, ss. 1292-1297, Doi: 10.23919/MIPRO.2017.7973622

Grant, M. & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, 26(2), ss.91–108. Doi: 10.1111/j.1471-1842.2009.00848.x

Han, J. Jeon, Y. & Kim, J. (2015). Security considerations for secure and trustworthy smart home system in the IoT environment, 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2015, ss. 1116-1118. Doi: 10.1109/ICTC.2015.7354752

Heartfield, R., Loukas, G., Budimir, S., Bezmeskij, A., Fontaine, J.R.J., Filippoupolitis, A. & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. Computers & Security, Uppl.78, ss. 398-428. Doi: 10.1016/j.cose.2018.07.011

Huth, C., Duplys, P. & Güneysu, T. (2016). Secure software update and IP protection for untrusted devices in the Internet of Things via physically unclonable functions. 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). Sydney, NSW, 2016, ss. 1–6. Doi: 10.1109/PERCOMW.2016.7457156.

Jia, X., Li, X. & Gao, Y. (2017). A Novel Semi-Automatic Vulnerability Detection System for Smart Home. Proceedings of the International Conference on Big Data and Internet of Thing (BDIOT2017). Association for Computing Machiner, *New York, NY, USA*, Ss.195–199. Doi: 10.1145/3175684.3175718

Jose, A. C., Malekian, R. & Ye, N. (2016). Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home. IEEE Access, Uppl. 4. ss. 5776-5787. Doi: 10.1109/ACCESS.2016.2606478

Karimi, K., Krit, S. (2019). Smart home-Smartphone Systems: Threats, Security Requirements and Open research Challenges. 2019 International Conference of Computer Science and Renewable Energies (ICCSRE), Agadir, Morocco, ss. 1-5. Doi: 10.1109/ICCSRE.2019.8807756

Kastner, M., Tricco, A., Soobiah, C., Lillie, E., Perrier, L., Horsley, T., Welch, V., Cogo, E., Antony, J. & Straus, S. (2012). What is the most appropriate knowledge synthesis method to conduct a review? Protocol for a scoping review. BMC Medical Research Methodology, 12(1). Doi: 10.1186/1471-2288-12-114

Khawla, M. & Tomader, M. (2018). A Survey on the Security of Smart Homes: Issues and Solutions. Proceedings of the 2nd International Conference on Smart Digital Environment (ICSDE'18). Association for Computing Machinery, New York, NY, USA, ss. 81–87. Doi: https://dl.acm.org/doi/10.1145/3289100.3289114

Kumar, S A. & Srivastava, T. V. (2016). Security in Internet of Things: Challenges, Solutions and Future Directions. 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, 2016, ss. 5772–5781.

Lin, H. & Bergmann, N.W. (2016). IoT Privacy and Security Challenges for Smart Home Environment. Information 2016, 7, 44. Doi: 10.3390/info7030044

Maayan, G. D. (2020). The Iot Rundown For 2020: Stats, Risks, And Solutions -- Security Today. [online] Security Today. Tillgänglig på: https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=1

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, RP. & Ni, W. (2018) Anatomy of Threats to the Internet of Things. 2018 IEEE Communications Surveys & Tutorials. Vol.21, utgåva 2. ss. 1636–1675. Doi: 10.1109/COMST.2018.2874978

Oconnor, T., Ench, W. & Reaves, B. (2019). Blinded and confused: uncovering systemic flaws in device telemetry for smart-home internet of things. Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19). Association for Computing Machinery, New York, NY, USA, ss. 140–150. Doi: 10.1145/3317549.3319724

Osisiogu, U. (2019). A Review on Cyber -Physical Security of Smart Buildings and Infrastructure. 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2019, Doi: 10.1109/ICECCO48375.2019.9043207

Pandey, P., Collen, A., Nijdam, N., Anagnostopolousos, M., Katsikas, S. & Konstanstas, D. (2019). Towards Automated Threat-Based Risk Assessment for Cyber Security in Smarthomes. Proceedings of the ... European conference on information warfare and security. ss.839-844. Tillgänglig på internet: http://hdl.handle.net/11250/2638515

Paré, G. & Kitsiou, S. (2017). Methods for Literature Reviews, Handbook of eHealth Evaluation: An Evidence-based Approach, University of Victoria. Tillgänglig på internet: https://www.ncbi.nlm.nih.gov/books/NBK481583/

Park, M., Oh, H. & Lee, K. (2019). Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. Sensors, 19(9). S. Doi: 10.3390/s19092148

Pascau, L. (2018). The IoT Threat Landscape and Top Smart Home Vulnerabilities in 2018. Bitdefender. Tillgänglig på internet: https://www.bitdefender.com/files/News/CaseStudies/study/229/Bitdefender-Whitepaper-The-IoT-Threat-Landscape-and-Top-Smart-Home-Vulnerabilities-in-2018.pdf

Ramapatruni, S., Narayanan, S. N., Mittal, S. Joshi A. & Joshi K. (2019). Anomaly Detection Models for Smart Home Security. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, ss. 19-24, Doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00015

Sapalo Sicato J.C., Sharma, P.K., Loia, V., Park, H.J. (2019). VPNFilter Malware Analysis on Cyber Threat in Smart Home Network. Applied Sciences, Uppl. 9, no. 13, p. 2763, Jul. 2019. Doi:10.3390/app9132763

Serror, M., Henze, M., Hack, S., Schuba, M. & Wehrle, K. (2018). Towards In-Network Security for Smart Homes. Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018). Association for Computing Machinery, New York, NY, USA, Article 18, ss.1–8. Doi: 10.1145/3230833.3232802

Shemshadi, A., Sheng, Q.Z., Qin, Y., Sun, A., Zhang, W.E. (2017). Searching for the internet of things: where it is and what it looks like. Pers Ubiquit Comput 21**,** ss.1097–1112 Doi:10.1007/s00779-017-1034-0

Suo, H., Wan, J., Zou, C., Liu, J. (2012) Security in the Internet of Things: A Review. International Conference on Computer Science and Electronics Engineering, Hangzhou, ss. 648-651. Doi: 10.1109/ICCSEE.2012.373

Tabassum, M., Kosinski, T., Lipford, H. R. (2019). ”I don’t own the data”: End Users Perception of Smart Home Device Data Practices and Risks. Fiftheenth Symposium on Usable Privacy and Security. USENIX Association, ss. 435-450. Tillgänglig på internet: https://www.usenix.org/system/files/soups2019-tabassum.pdf

Tanwar, S., Patel, P., Patel, K., Tyagi, S., Kumar, N., Obaidat, M. S. (2017) An advanced Internet of Thing based Security Alert System for Smart Home. International Conference on Computer, Information and Telecommunication Systems (CITS), Dalian, ss. 25-29. Doi: 10.1109/CITS.2017.8035326

Vojković, G., Milenković, M. and Katulić, T. (2019). IoT and Smart Home Data Breach Risks from the Perspective of Croatian Data Protection and Information Security Law. 2019 ENTRENOVA Conference Proceedings. Doi: 10.2139/ssrn.3490606

Whitter-Jones, J. (2018) Security Review On The Internet of Things. 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, 2018, ss.163-168. Doi: 10.1109/FMEC.2018.8364059

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE 14, Association for Computing Machinery, New York, NY, USA. Doi: 10.1145/2601248.2601268

Zhang, N., Sun, H., Sun, K. Lou, W. & Hou, Y. T. (2016). CacheKit: Evading Memory Introspection Using Cache Incoherence. 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, 2016, ss. 337-352, Doi: 10.1109/EuroSP.2016.34

Zhou, W., Jia, Y., Yao, Y., Zhu, L., Guan, Le., Mao, Y., Liu, P., Zhang Y. (2019). Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms. 28th USENIX Security Symposium, Santa Clara, CA. ss. 1133–1150. Tillgänglig på internet: https://www.usenix.org/conference/usenixsecurity19/presentation/zhou

Bilaga 1: Tabell och sammanfattning av utvalda studier

Utvalda studier	Sammanfattning för studien och dess identifiering av manipulation av enheter i smarta hemenheter.	Rekommenderade åtgärder mot manipulation i det smarta hemmet
Blinded and confused: uncovering systemic flaws in device telemetry for smart-home internet of things. (Oconnor et al. 2019)	Undersöker utvecklares designval för IoT-enheters meddelandeprotokoll och vad som sker när det förlorar anslutning. För att undersöka det använder de IoT-enheter för smarta hem. De upptäcker att 22 av 24 enheter som har undersökts har fel som möjliggör attacker som kan stoppa IoT-enheternas förmåga att sända ut alarm till användaren när de skall. De upptäcker även att felen kan förhindra IoT-enheternas förmåga att ladda upp information angående enheternas funktioner.	- Traffic shaping för att förhindra manipulering av trafik, metoden bland annat implementeras med hjälp av branväggskonfigurationer. En metod för att se till att HTTPS trafik inte läcker känslig information. -Per-IoT VPN: Per-IoT VPN möjliggör att IoT-enheter kan själva upprätta VPN för att skydda sig.
Towards the Security of Motion Detection-based Video Surveillance on IoT Devices (Feng et al. 2017)	Undersöker hur övervakningskameror i det smarta hemmet kan bli övertagna och manipulerade. Beskriver hur en angripare kan få åtkomst och kontroll av övervakningskameran genom replay attacker och andra malware infekteringar	Föreslår användandet av hårdvaruisolering som åtgärd för att motverka manipuleringstekniker som replay-attacker.
A Survey on the Security of Smart Homes: Issues and Solutions (Khawla et al. 2018)	En övergripande studie för hot och sårbarheter mot smarta hem med åtgärdsförslag. Beskriver imiteringsattacken Sybil för att manipulera system. Icke uppdaterade enheter kan medföra svag säkerhet som angripare kan nyttja för att ta över system.	Mäta signalstyrka i korrelation med andra noder för att bemöta sybil-attacker. Firmware skall uppdateras regelbundet genom krypterade kommunikationsvägar och säkrade servrar för uppdatering av filer för att i följd motverka att enheter kan bli utsatta för kapning
Towards In-Network Security for Smart Homes. (Serror et al. 2018)	Ser nätverket som det stora problemet som möjliggör attacker mot IoT-enheterna i hemmet. Användandet av avlyssningsattacker för att få åtkomst till	En kombination av kommunikationsregler och maskinlärande nätverksövervakning för att säkra

	root-rättigheter för att kunna manipulera systemet.	nätverket mot utomstående attacker.
Secure Smart Homes: Opportunities and Challenges. (Batalla et al. 2017)	Undersöker olika aspekter av smarta hem och vilka hot som kan förekomma i kombination med förslag för hur det kan åtgärdas. Säkerhetshot som avlyssning, övertagning och kapning används av angriparen så hen kan få kontroll över enheter och eller göra så användare blir av med data.	-AES-kryptering skall användas för dataöverföring, RSA för hantering av publika nycklar och digitala signaturer för delade nycklar. -Rekommenderar att antingen använda sig av statisk kryptering eller dynamisk kryptering. -Övervakning av IoT-enheterna i det smarta hemmet kan hjälpa mot att förhindra otillåten åtkomst. Detta i kombination med väl implementerad skydd för hemmanätverket -Även bra metoder för autentisering för att säkerställa att enbart behöriga kan få tillgång till det smarta hemmet.
A Novel Semi-Automatic Vulnerability Detection System for Smart Home. (Jia & Gao, 2017).	Studien diskuterar olika metoder för att få åtkomst och manipulera IoT-enheter i hemmet som till exempel avlyssning, imitering av användare, reply attacker, meddelande modifiering för att infektera med malware.	-Ett semi-automatiserad system som de själva har utvecklat som skall kunna upptäcka brister i IoT-enheter redan efter utveckling. Systemet undersöker om det förekommer bristande kryptering, öppna portar eller svaga lösenordshanteringar som kan utnyttjas av angripare
Security considerations for secure and trustworthy smart home system in the IoT environment (Han et al. 2015)	Identifierar att det smarta hemmet kan utsättas för många olika hot från angripare som kan ta över enheter i hemmet. Undersöker användningen av IoT-enheter id et smarta hemmet och vilka säkerhetskrav behövs i det smarta hemmet.	-Rekommenderar att ha uppdaterade säkerhetsversioner av enheterna. -kontroller för att veta att uppdateringar av firmware är äkta. -Bra funktioner för autentisering

		-Uppfattning om vem som har kontroll till vad samt krypteringsmetoder.
Anomaly Detection Models for Smart Home Security (Ramapatruni et al. 2019)	Identifierar att manga smarta hem-enheter har på senaste tiden blivit hackade och privat information läcker. Studien utför ett experiment med maskinlärande metoder för att upptäcka illvilliga aktiviteter i det smarta hemmet.	Maskinlärningsartefakt för att för identifikation av dolda aktiviteter i det smarta hemmet.
Smart home-Smartphone Systems: Threats, Security Requirements and Open research Challenges (Karimi & Krit, 2019)	Identifierar hot mot smarta hem och kategoriserar det som interna och externa hot. Manipulering av IoT-enheter i hemmet faller under externa hot.	- Bra krypteringsmetoder för nätverkstrafik. - Nätverksövervakning. - Se över hårdvarubegränsningar.
An approach to secure smart homes in cyber-physical systems/Internet-of-Things (Rehman et al. 2018)	Identifierar att det smarta hemmet är utsatt för hot från angripare och att sensorer är en stor faktor som används i det smarta hemmet. Många hemautomatiserande enheter i det smarta hemmet utgör en säkerhetsrisk som angripare kan utnyttja. En åtgärd presenteras för att bemöta det.	- Implementationen av ett sicher brandväggssystem som placeras mellan en central enhet som är bryggan till internet, som en router, och till enhet central till hemmet.
IoT based smart home: Security challenges, security requirements and solutions (Ali et al. 2017)	Identifierar passiva och aktiva hot. Anser att attacker som avlyssning är passiva där information samlas men systemet förändras inte. Aktiva attacker är sedan när informationen kan modifieras och användas mot det smarta hemmet.	- Hålla enheter uppdaterade med hjälp av att enbart auktoriserade användare kan utföra det. - Starka inloggnings och auktoriseringsuppgifte
Secure software update and IP protection for untrusted devices in the Internet of Things via physically unclonable functions (Huth et al. 2016)	För att hantera besvären med redan infekterade enheter som kan manipuleras utvecklar Huth, Duplys & Güneysu (2016) ett protokoll för att bland annat möjliggöra en säker firmwareuppdatering på redan infekterade enheter.	- Framtaget protokoll för att utföra säkra uppdateringar på enheter utan att manipulering kan ske. - Implementerade fysiska funktioner för att förhindra kloning & imitering med protokollet.
A taxonomy of cyber-physical threats and impact in the smart home (Heartfield et al. 2018)	Answer att anpassningen till internet of things och olika internettjänster är en attraktiv plats för cyberattacker i dagens läge. Klassificerar cyberhot och vilken	- Förebyggande åtgärder som åtgärder som stark autentisering och auktorisering.

	påverkan de kan ha på hemsystemet. Rekommenderar i samband åtgärder som bör implementeras.	- Aktiva metoder som övervakning & verifiering av användare och enheter.
VPNFilter Malware Analysis on Cyber Threat in Smart Home Network (Sapalo Sicato et al. 2019)	Identifierar hot beroende på fyra lager som IoT-enheter primärt är uppbyggda på. Kategoriserar olika hot beroende på lager. Undersöker *malware* VPNfilter.	-Användandet av ett IDPS av författarnas egen design för ett smart hem. Samt grundåtgärder för användare.
Towards Automated Threat-Based Risk Assessment for Cyber Security in Smarthomes (Pandey et al. 2019)	Diskuterar cyberhot mot smarta hem och hur hoten bäst bör åtgärdas.	-Presenterar en riskbedömningsprocess specifikt för smarta hem för att minska hot som *malware*.
I don't own the data": End Users Perception of Smart Home Device Data Practices and Risks (Tabassum et al. 2019)	Fokuserar på användarnas medvetenhet i det smarta hemmet och deras kunskap om hot. Hotet av hackade och manipulerade IoT-enheter diskuteras. Åtgärder för hur utvecklare bör agera framställs.	- I utveckling av implementerade säkerhetsåtgärder och policys behöver utvecklarna för enheterna ha användares tekniska förmåga i åtanke. Användare behöver utbildas.
A Review on Cyber -Physical Security of Smart Buildings and Infrastructure (Osisiogu, 2019).	Identifierar hot mot smarta hem i form av nätverksprotokoll, svag autentisering på enheter. Även möjligheten att produkter blir infekterade av *malware* innan de når användaren och manipulering av sensorer.	- Olika riskanalysmetoder för att bemöta och åtgärda hot. Till exempel CIA-triaden. - Ökad säkerhetsmedvetenheten hos användare och intressenter.
Discovering and Understanding the Security Hazards in the Interactions betweenIoT Devices, Mobile Apps, and Clouds on Smart Home Platforms (Zhou et al. 2019).	Angripare kan installera fantomenheter i det smarta hemmet för att lura IoT-molnet när användaren registrerar sig. Hotet möjliggör att angriparen tar över kontrollen av enheter i hemmet utan användarens vetskap.	- Förbättrade autentiseringsmetoder och protokoll för inloggningar av enheter mot IoT-moln.
Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective (Park et al. 2019)	Identifierar hot som kan uppstå via attacker mot IoT-enheternas sensorteknik. Exempelvis kan AI-högtalare användas för att införa angriparens kommandon. Även sensorer för touchskärmar kan användas för att komma över inloggningsuppgifter.	- Presenterar en riskbedömningsprocess för att ge användare en uppfattning om vilka IoT-enheter i hemmet kan drabbas och potentiellt åtgärdas.

Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study (Davis et al. 2020)	Manipulering av IoT-enheter på grund av fysisk tillgång och nätverkstillgång. Beroende på enheten kan flera IoT-enheter i hemmet också bli kapade i det scenariot.	- Högre krav på utvecklare och forskning mot en konsekvent standard för IoT-enheter.
IoT Privacy and Security Challenges for Smart Home Environment. (Lin & Bergman, 2016)	Studien anser att det största hotet mot det smarta hemmet är tillgång till systemet. Undersöker existerande lösningar för att förbättra säkerheten för IoT för det smarta hemmet.	- Användning av molnbaserade lösningar för IoT-enheter för att avlasta IoT-enheterna från mycket ansvar. - Användandet av en IoT-gateway för att bidra till ett centraliserad hanteringsverktyg för att ge mer prestanda och hantera säkerhet bättre.
Improving Home Automation Security; Integrating Device Fingerprinting (Jose et al. 2016)	Studien betonar betydelsen med tillgång till det smarta hemmet över internet men diskuterar säkerhetsproblem med det. På grund av att det smarta hemmet går att få tillgång till över internet kan även angripare få tillgång till det från sitt eget hem.	- Föreslår device fingerprinting för att lista tillåtna och otillåtna enheter för att säkra hemmet. - Förbättrade inloggningsuppgifter i korrelation med device fingerprinting.

Bilaga 1 – Övergripande sammanfattningar av de utvalda studierna och dess rekommenderade åtgärder mot manipulation av IoT-enheter för smarta hem (Författarens egen.)