Datenschutz im Smart Home: Strategien zur Verbesserung der Privatsphäre durch Entkopplung vom Hersteller

Studienarbeit im Modul SQF61

von

Patrick Langkau

Im Studiengang Künstliche Intelligenz M.Sc.
an der staatlich anerkannten AKAD Hochschule Stuttgart

5. April 2024

Bearbeitungszeit	10.02.2024 - 06.04.2024
Betreuer	Dr. Sebastian Bauer
Matrikelnummer	8150203
E-Mail	patrick.langkau@stud.akad.de
Adresse	Schneeglöckleweg 17 70374 Stuttgart

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Einführung in das Thema

Im Zuge der Digitalisierung haben Smart Home Technologien Einzug in den Alltag vieler Menschen gefunden. Diese Technologien können Komfort und Effizienz bieten, jedoch bergen sie auch Risiken für den Datenschutz. Die Verarbeitung und Speicherung persönlicher Daten durch Smart Home Geräte und deren Hersteller werfen Fragen hinsichtlich der Privatsphäre und des Schutzes dieser Informationen auf. Dies kann vor allem zum Problem werden, wenn die Hersteller die Daten nicht auf Servern in Deutschland oder der Europäische Union (EU) speichern, sondern wenn diese Daten im Ausland gespeichert werden. Angesichts dieser Entwicklungen ist es entscheidend, sich mit Strategien zur Verbesserung der Privatsphäre durch technische und organisatorische Maßnahmen auseinanderzusetzen. Dies beinhaltet unter anderem die Überlegung, die Geräte vom Hersteller zu entkoppeln, um so die Abhängigkeit zu verringern.

1.2 Relevanz des Datenschutzes für Smart Home Nutzer

Da durch die Benutzung von Smart Home Geräten viele persönliche Daten und Informationen über den Alltag und die Gewohnheiten der Bewohner anfallen, welche auch verarbeitet und an Dritte weitergegeben werden können, spielt der Datenschutz eine entscheidende Rolle für die Nutzer von Smart Home Technologien. Die Privatsphäre der Nutzer kann von einer solchen Datensammlung und der eventuellen Weitergabe erheblich beeinträchtigt werden. Ein angemessener Schutz dieser Daten ist daher essentiell, um Missbrauch zu verhindern und das Vertrauen in Smart Home Technologien zu stärken. Nutzer sollten sich potenzieller Risiken bewusst sein und Möglichkeiten haben, ihre Daten und Privatsphäre effektiv zu schützen.

1.3 Zielsetzung dieser Arbeit und Forschungsfrage

Das Ziel dieser Arbeit ist es, Strategien zur Verbesserung des Datenschutzes in Smart Home Systemen zu untersuchen, insbesondere durch die Reduzierung von Abhängigkeiten zu den Geräteherstellern. Der wesentliche Fokus liegt auf der Entkopplung dieser Smart Home Geräte vom Hersteller, um dem Nutzer zu ermöglichen, die Kontrolle über ihre Daten zu erhöhen und deren Privatsphäre zu schützen. Die zentrale Forschungsfrage lautet

daher: „Kann durch eine Entkopplung von Smart Home Geräten von ihren Herstellern eine Verbesserung des Datenschutzes und der Privatsphäre erzielt werden?“

2 Grundlagen

2.1 Definition von Smart Home Technologien

Ein Smart Home bezeichnet privat genutzte Räumlichkeiten, wie Eigenheime oder Mietwohnungen, in denen Geräte der Hausautomation, Haushaltstechnik und Kommunikationseinrichtungen vernetzt sind, um sich an die Bedürfnisse der Bewohner anzupassen. Durch diese intelligente Vernetzung wird es ermöglicht Assistenzfunktionen und Dienste zu nutzen, welche den alltäglichen Komfort gegenüber der normalen Nutzung hinaus steigern. Beim Smart Home wird eine Abgrenzung zu Smart Buildings gemacht, welche sich auf kommerziell verwaltete, größere Gebäudekomplexe bezieht. Im Zentrum steht die Integration und Vernetzung von Teilsystemen für Heizung, Beleuchtung, Sicherheit und Haushaltsgeräte. Dies kann eine autonome Steuerung und Effizienzsteigerung ermöglichen.[1]

2.2 Überblick über Datenschutzprobleme

Die Einführung von Smart Home Technologien birgt erhebliche Datenschutzprobleme, hauptsächlich aufgrund der umfangreichen Sammlung und Nutzung persönlicher Daten. Oftmals umfassen diese Daten sensible Informationen über Lebensweise und Vorlieben der Nutzer. Dies bringt das Risiko unbefugten Zugriffs, Datenlecks und der Nutzung der Informationen für nicht genehmigte Zwecke mit sich.[2] Ein zentrales Problem ist die Durchsetzung von Datenschutz in Internet of Things (IoT)-Umgebungen, welches als eines der Hauptbarrieren für die Verwirklichung des Smart Home Vision gilt.[3]
Eine Studie betonte die erheblichen Auswirkungen von Datenschutzproblemen auf die Absicht der Nutzer, Smart Home Technologien zu nutzen. Außerdem hob sie die Notwendigkeit hervor, diese Bedenken zu adressieren, wenn die Akzeptanz dieser Technologien verbessert werden sollte [4]. Des weiteren wurde festgestellt, dass die Privatsphäre und das Vertrauen der Nutzer durch Aspekte wie Datensicherheit, Kontrolle über die Weitergabe persönlicher Informationen sowie auch das Vertrauen in den Systemanbieter beeinflusst werden.[5]

[1] Strese u. a. 2010, vgl.
[2] Guhr u. a. 2020, vgl.
[3] Jacobsson und Davidsson 2015, vgl.
[4] Guhr u. a. 2020, vgl.
[5] Schomakers, Biermann und Ziefle 2021, vgl.

2.3 HomeAssistant

Home Assistant ist eine Open Source Lösung für die Heimautomatisierung. Diese Software kann zur zentralen Steuerung und Verwaltung von Smart Home-Geräten verwendet werden. Da diese Open Source Software auf einer Vielzahl von Hardwaregeräten ausgeführt werden kann, bietet diese Plattform eine umfassende Kompatibilität mit zahlreichen Smart Home Produkten. Home Assistant legt den Schwerpunkt auf Datenschutz sowie lokale Datenverarbeitung, hierdurch werden Daten hauptsächlich im lokalen Netzwerk des Benutzers statt in der Cloud verarbeitet und gespeichert. Dies erhöhte die Kontrolle und kann auch eine höhere Sicherheit gewährleisten.[6] [7]

2.4 ZigBee

ZigBee ermöglicht als offener und weltweit anerkannter Standard die drahtlose Kommunikation zwischen Smart Home Geräten über kurze Distanzen durch energieeffiziente Funkübertragungen. Diese Technologie ist besonders für ihre Fähigkeit bekannt, ein sicheres, zuverlässiges und energieeffizientes Netzwerk aufzubauen. ZigBee unterstützt darüber hinaus die Bildung von Mesh Netzwerken, was die Netzwerkabdeckung und Zuverlässigkeit innerhalb des Smart Home Ökosystems signifikant verbessert.[8] [9] Ein beispielhafter Aufbau eines ZigBee Netzwerks ist in Abbildung 2.1 zu erkennen.

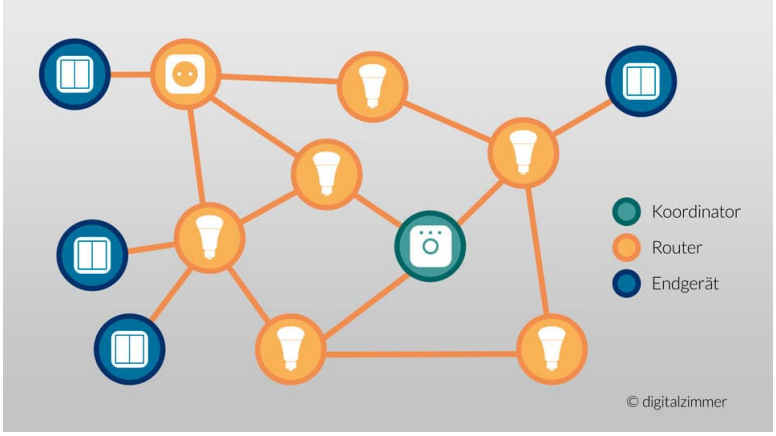

Abb. 2.1: Quelle: https://www.digitalzimmer.de/artikel/wissen/philips-hue-das-zigbee-netz-optimal-einrichten/

[6] Schomakers, Biermann und Ziefle 2021, vgl.
[7] Kraemer 2018, vgl.
[8] Guhr u. a. 2020, vgl.
[9] Schomakers, Biermann und Ziefle 2021, vgl.

2.5 Thread und Matter

Thread ist ein fortschrittliches Protokoll, welches auf dem Internet Protocol (IP) basiert. Dieses Protokoll dient zur Vernetzung von Smart Home Geräten. Es zeichnet sich durch die Schaffung von selbst heilenden und sicheren Mesh Netzwerken aus. Dies verbessert die direkte Kommunikation zwischen den einzelnen Geräten, was die Zuverlässigkeit sowie Effizienz im Smart Home erhöht. Ergänzend dazu ist Matter (zuvor bekannt als Project Connected Home over IP (IP)), als universelles Anwendungsschicht-Protokoll konzipiert, welches durch seine breite Kompatibilität und verschiedene Sicherheitsfeatures Vorteile bietet. Matter fördert die einheitliche Interaktion und Kommunikation zwischen Geräten verschiedener Hersteller und trägt somit zu einer einfacheren Integration sowie einer verbesserten Benutzererfahrung bei. Durch die Kombination von Thread und Matter bildet sich eine robuste Basis für interoperable und sichere Smart Home Lösungen.[10] [11]
Außerdem erlaubt Matter im Vergleich zu ZigBee mehrere Boarder Router, also Netzwerk Router, welche auch Internetzugriff haben können, zu erstellen. Somit kann das Netzwerk gegen einen Ausfall der Zentrale abgesichert werden. Ein beispielhafter Aufbau eines Thread Netzwerks ist in Abbildung 2.2 zu erkennen.

Abb. 2.2: Quelle: https://matter-smarthome.de/entwicklung/die-baustellen-im-matter-standard/

[10] Mocrii, Chen und Musilek 2018, vgl.
[11] Chalhoub 2020, vgl.

3 Hauptteil

3.1 Datenschutzherausforderungen in Smart Homes

3.1.1 Analyse spezifischer Datenschutzrisiken

Die Einführung von Smart Home Technologien in den privaten Lebensraum birgt eine Reihe spezifischer Datenschutzrisiken. Diese Risiken resultieren vorrangig aus der umfangreichen Datenerfassung und -verarbeitung, die für die Funktionalität dieser Geräte notwendig ist. Zu den sensiblen Daten, die von Smart Home Geräten gesammelt werden, gehören nicht nur Steuerungsbefehle und Gerätestatusinformationen, sondern auch personenbezogene Daten, die Einblicke in die Gewohnheiten und Lebensweisen der Bewohner geben können. [1]

Eines der Hauptprobleme ist die unerwünschte Datenweitergabe, sei es durch unsichere Datenübertragung, unzureichend gesicherte Speicherung oder den Verkauf von Daten an Dritte ohne explizite Zustimmung der Nutzer. Darüber hinaus besteht das Risiko von Datenlecks und Hackerangriffen, die durch Sicherheitslücken in den Smart Home Geräten oder deren Kommunikationsinfrastruktur ermöglicht werden. [2]

Ein weiteres Datenschutzrisiko ist die Möglichkeit der Erstellung detaillierter Nutzerprofile. Durch die Analyse der gesammelten Daten können nicht nur Verhaltensmuster erkannt, sondern auch persönliche Präferenzen und sogar emotionale Zustände der Bewohner abgeleitet werden. Dies birgt die Gefahr einer unbewussten Einflussnahme auf die Bewohner oder einer gezielten Werbung, die auf den gesammelten Daten basiert. [3]

3.1.2 Fallstudien von Datenschutzverletzungen

Die zunehmende Vernetzung von Haushalten durch Smart Home Technologien bringt nicht nur Komfort und Effizienzsteigerungen mit sich, sondern eröffnet auch neue Angriffsvektoren für Datenschutzverletzungen. Ein bemerkenswertes Beispiel ist der Vorfall mit dem Mirai Botnetz, der die Schwachstellen vernetzter Geräte deutlich macht. Mirai ist dafür bekannt, breitflächig IoT Geräte, einschließlich Heimrouter, zu infizieren und diese in ein Botnetz einzubinden, um massive Distributed Denial of Service Angriffe durchzuführen. Dieser Vorfall verdeutlicht nicht nur die potenziellen Risiken der Vernetzung, sondern auch die spezifischen Gefahren, die sich aus der Kompromittierung von Geräten ergeben, welche auf den ersten Blick als harmlos erscheinen mögen. Die Tatsache, dass Angreifer potenziell die Interaktion

[1] Jacobsson und Davidsson 2015; Guhr u. a. 2020, vgl.
[2] Schomakers, Biermann und Ziefle 2021; Mocrii, Chen und Musilek 2018, vgl.
[3] Chalhoub 2020; Ardito, Barbato und Andrea Saracino 2022, vgl.

mit Smart Speakern aufzeichnen können, offenbart ein erhebliches Risiko für die Privatsphäre der Nutzer. [4]

Neben der unmittelbaren Gefahr durch Malware wie Mirai existieren weitere Beispiele, die die Verletzlichkeit von Smart Homes gegenüber Datenschutzverletzungen aufzeigen. Ein Szenario, welches für viele beunruhigend sein sollte, ist der unbefugte Zugriff auf IoT Geräte, wie smarte Waschmaschinen und Heimsicherheitssysteme. Diese Vorfälle können dazu führen, dass persönliche Daten unautorisiert abgerufen und manipuliert werden, was die Privatsphäre der Nutzer direkt untergräbt und die Sicherheit ihres Zuhauses gefährdet[5]. Der Zugriff auf solche Geräte kann es Angreifern ermöglichen, sensible Informationen zu entwenden oder die Kontrolle über physische Sicherheitssysteme zu erlangen, was die Bewohner erheblichen Sicherheitsrisiken aussetzt.

Die Schwachstellen, die der Mirai Vorfall aufzeigt, unterstreichen die dringende Notwendigkeit, Benutzer vor seitlichen Verkehrsdatenbedrohungen in IoT Geräten zu schützen, die ihre Privatsphäre gefährden könnten. Die Analyse von Netzwerkverkehr, um Anomalien zu identifizieren, die auf eine Kompromittierung hinweisen, ist ein Ansatz, um solche Bedrohungen abzuwehren. Die Entwicklung und Implementierung von Strategien zum Schutz der Privatsphäre in Smart Homes muss eine Priorität für Forscher, Entwickler und Regulierungsbehörden sein, um die Sicherheit und das Vertrauen der Nutzer in diese Technologien zu gewährleisten. [6]

Diese Beispiele verdeutlichen die komplexen Herausforderungen, die sich im Kontext von Smart Homes für den Datenschutz stellen. Es ist evident, dass die Sicherung der Privatsphäre in vernetzten Haushalten eine umfassende Strategie erfordert, die sowohl technologische Lösungen als auch rechtliche und regulatorische Maßnahmen umfasst, um die Sicherheit und das Vertrauen der Nutzer in diese Technologien zu stärken.

[4] Huang u. a. 2023, vgl.
[5] Davenport 2016, vgl.
[6] Apthorpe, Reisman und Feamster 2017, vgl.

3.2 Strategien zur Verbesserung des Datenschutzes

3.2.1 Verwendung einer Open Source Smart Home Zentrale

Open Source Smart Home Zentralen stellen einen Paradigmenwechsel in der Art und Weise dar, wie Benutzer ihre intelligenten Geräte verwalten und kontrollieren. Diese Systeme, oft durch eine aktive Gemeinschaft unterstützt, bieten eine Plattform, die nicht nur für ihre Anpassungsfähigkeit, sondern auch für ihre Transparenz und Sicherheit bekannt sind. In diesem Beispiel soll Home Assistant als Smart Home Zentrale betrachtet werden, die hier aufgeführten Punkte treffen jedoch für alle, beziehungsweise die meisten Open Source Smart Home Zentralen zu. Benutzer profitieren von der Möglichkeit, ihre Systeme nach Belieben anzupassen, was eine präzise Kontrolle über die gesammelten Daten und deren Verwendung ermöglicht. Ein Schlüsselaspekt dabei ist, dass Open Source Systeme keine verborgenen Backdoors enthalten, die externe Parteien nutzen können, um unbefugten Zugriff auf Benutzerdaten zu erhalten. Dies erhöht das Vertrauen und die Sicherheit, indem es sicherstellt, dass alle Datenflüsse innerhalb des Systems nachvollziehbar und unter der Kontrolle des Benutzers bleiben. [7]

Technisch versierte Nutzer können Features, welche sie sich wünschen, aber aktuell noch nicht implementiert sind, auch einfach selbst implementieren. Dies Lösung können Sie dann den Entwicklern zur Verfügung stellen, welche daraufhin entscheiden können, ob sie diese Features in die Software für alle Nutzer integrieren wollen.

Ein weiterer Vorteil dieser Systeme ist ihre Unabhängigkeit von kommerziellen Anbietern. Dies reduziert die Wahrscheinlichkeit, dass Benutzerdaten für unbekannte Zwecke gesammelt oder missbraucht werden. Darüber hinaus fördert die Open Source Natur einen kontinuierlichen Verbbesserungsprozess durch die Gemeinschaft, was zu schnelleren Updates und Patches führt und das System gegenüber neuen Bedrohungen resilienter macht. [8]

Die Verwendung von einer vertrauenswürdigen Zentrale, an welcher Informationen von Geräten verschiedener Hersteller zusammenkommen, verhindert, dass ein Hersteller auch Informationen von Geräten anderer Hersteller abrufen kann. Die Verwendung einer solchen Zentrale kann jedoch nicht allgemein eine komplette Entkopplung zum Hersteller gewährleisten. Je nach Anschlussart können auch Geräte über die Application Programming Interface (API) des Herstellers angeschlossen werden. Dies ist oft der Fall, wenn die Geräte über Wireless Local Area Network (WLAN) angeschlossen werden. Ein reiner Anschluss eines IoT Gerätes über WLAN gibt keine Standardisierung vor. Ohne eine Veränderung der Gerätesoftware kann so in vielen Fällen nur auf die API des Herstellers zugegriffen werden.

[7] Hussain und Qi 2018, vgl.
[8] Panwar u. a. 2019, vgl.

3.2.2 Entkopplung der Geräte vom Hersteller

Indem Smart Home Geräte von den Herstellern entkoppelt werden, gewinnen Benutzer eine größere Kontrolle über ihre persönlichen Informationen. Durch diese Entkopplung kann komplett auf die Hersteller API verzichtet werden. Hierfür stellen einige Geräte eine sogenannte Lokale API zur Verfügung. Wichtig ist zu wissen, dass insofern den Geräten weiterhin erlaubt wird mit dem Internet zu kommunizieren, nicht sichergestellt werden kann, dass keine Informationen des Gerätes zum Hersteller fließen. Hierfür kann bei WLAN Geräten mithilfe von Firewall Regeln die Kommunikation zum Internet eingeschränkt oder untersagt werden. Eine Alternative ist es, Protokolle zu verwenden, bei welchem die Geräte generell keinen Direkten Zugriff auf das Internet haben, sondern nur mit einer Zentrale kommunizieren. Wird in diesem Fall nun eine vertrauenswürdige Zentrale gewählt, so kann hier eine Verbesserung der Privatsphäre und Sicherheit generiert werden. Durch diese Unabhängigkeit wird es Benutzern ermöglicht, über die Verwendung und Weitergabe ihrer Daten zu entscheiden, ohne von den Datenschutzrichtlinien der Hersteller abhängig zu sein.

Entkopplung durch Verwendung des ZigBee Protokolls

Das ZigBee Protokoll, welches bekannt für seine niedrige Energieaufnahme und hohe Sicherheit ist, unterstützt die Bildung eines Mesh Netzwerken. Dies ermöglicht eine robuste und zuverlässige Kommunikation zwischen Geräten. Durch die Fähigkeit, Daten direkt zwischen Geräten zu übertragen, ohne durch externe Server zu gehen, hilft ZigBee, das Risiko von Datenlecks zu minimieren und die Privatsphäre der Benutzer zu schützen. Die Verwendung von End-to-End-Verschlüsselung sichert die Datenübertragung ab, sodass nur autorisierte Geräte Zugriff auf die übertragenen Informationen haben. [9]
Da ZigBee Geräte nur untereinander und mit dem Koordinator in einem eigenen Netzwerk kommunizieren, ist, insofern ein vertrauenswürdiger Koordinator, wie beispielsweise Home Assistant, verwendet wird, keine Kommunikation mit dem Internet der IoT Geräte möglich. Dies bedeutet jedoch auch, dass Geräte im ZigBee Netzwerk nicht direkt mit Updates versorgt werden können. Das Updaten solcher Geräte ist jedoch im ZigBee Netzwerken trotzdem möglich. Der Koordinator, welcher in der Regel Internetzugriff hat, kann nach Updates für die angeschlossenen Geräte suchen und diese dann verteilen. [10]

Entkopplung durch Verwendung des Thread Protokolls

Die Nutzung des Thread Protokolls in Smart Home Umgebungen bietet eine strategische Methode zur Verbesserung der Datensicherheit und Privatsphäre durch Entkopplung der

[9] Li u. a. 2023, vgl.
[10] Zigbee2MQTT 2024, vgl.

Geräte vom Hersteller. Im Kontext der Entkopplung ermöglicht das Thread Protokoll eine sichere und effiziente Kommunikation zwischen Geräten im lokalen Netzwerk, ohne dass eine ständige Verbindung zu den Servern des Herstellers erforderlich ist. Dies trägt signifikant zum Schutz der Nutzerdaten bei, da die Kommunikation innerhalb des Smart Homes bleibt und nicht externen Parteien zugänglich gemacht wird.

Thread ist speziell für das IoT entwickelt worden und unterstützt die Erstellung eines Mesh Netzwerks. Diese Netzwerkstruktur ermöglicht es Geräten, direkt miteinander zu kommunizieren, was die Notwendigkeit einer zentralen Steuereinheit eliminiert. Durch die direkte Kommunikation zwischen den Geräten können Daten effizienter übertragen und gleichzeitig die Latenzzeiten reduziert werden. Ein weiterer Vorteil des Thread Protokolls ist seine robuste Sicherheitsarchitektur, die eine sichere Authentifizierung, Verschlüsselung und Schlüsselverwaltung umfasst, um die Privatsphäre der Nutzer und die Integrität der Daten zu gewährleisten. [11]

Für die Entkopplung der Smart Home Geräte vom Hersteller mittels des Thread Protokolls bedeutet dies, dass Nutzer in der Lage sind, ihre Geräte unabhängig von den proprietären Ökosystemen der Hersteller zu betreiben. Dies ermöglicht eine größere Flexibilität bei der Auswahl und Integration von Geräten verschiedener Hersteller in ein einziges Smart Home System. Zudem kann die Nutzung einer Open Source Smart Home Zentrale, wie beispielsweise Home Assistant, als Border Router nicht nur die Privatsphäre und Sicherheit verbessern, sondern auch die Benutzererfahrung durch erhöhte Interoperabilität und Zuverlässigkeit optimieren.

In Bezug auf die technische Implementierung nutzt das Thread Protokoll IPv6 für die Adressierung der Geräte, was eine nahtlose Integration in bestehende Netzwerkinfrastrukturen und das Internet ermöglicht. Dies erleichtert die Fernsteuerung und -überwachung der Smart Home Geräte, ohne dabei Kompromisse bei der Sicherheit einzugehen. Die End-to-End-Verschlüsselung gewährleistet, dass alle über das Thread Netzwerk übertragenen Daten geschützt sind und nur von autorisierten Geräten und Nutzern eingesehen werden können. Diese Abbildung 3.1 filtern hier auch, welche Daten an das Internet übergeben werden sollen. [12]

[11] Panwar u. a. 2019, vgl.
[12] OpenThread 2023, vgl.

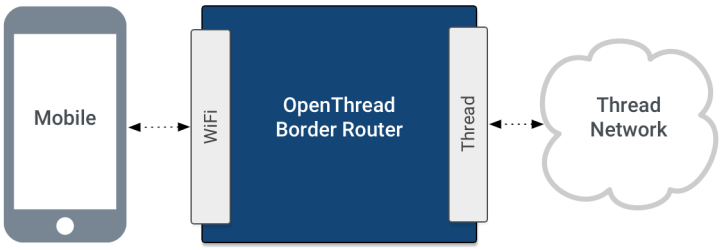

Abb. 3.1: Quelle: https://openthread.io/guides/border-router?hl=de

4 Bewertung

4.1 Zusammenfassung der Haupterkenntnisse

In dieser Arbeit wurden die vielschichtigen Datenschutzrisiken innerhalb des Smart Home Kontextes beleuchtet. Es wurde aufgezeigt, dass trotz der fortschrittlichen Möglichkeiten zur Verbesserung des Wohnkomforts durch Smart Home Technologien, diese auch erhebliche Risiken für die Privatsphäre der Nutzer bergen. Die Analyse hat gezeigt, dass Open Source Plattformen und sichere Kommunikationsprotokolle, wie ZigBee und Thread, wesentliche Bausteine für die Verbesserung der Privatsphäre darstellen können, indem sie die Kontrolle über die Daten den Nutzern zurückgeben und eine sichere Datenkommunikation gewährleisten. Des weiteren können lokale APIs verwendet werden, wenn zusätzlich den Geräten der Internetzugriff eingeschränkt oder untersagt wird. Im Bezug auf die Forschungsfrage kann festgehalten werden, dass durch die Entkopplung der Geräte von ihren Herstellern, Nutzern von Smart Home Systemen die Datenhoheit zurückgegeben wird und sich somit eine Verbesserung des Datenschutzes und der Privatsphäre erreichen lässt.

4.2 Bewertung der Effektivität der vorgestellten Ansätze

Die Effektivität der vorgestellten Datenschutzstrategien hängt von einer Reihe von Faktoren ab, einschließlich der technischen Umsetzung, der Benutzerfreundlichkeit und der gesetzlichen Rahmenbedingungen. Während Open Source Plattformen und verschlüsselte Kommunikation starke Werkzeuge zum Schutz der Privatsphäre bieten, sind sie allein keine Allheilmittel. Technische Herausforderungen, potenzielle Sicherheitslücken und die Dynamik der technologischen Entwicklung erfordern eine kontinuierliche Anpassung und Überprüfung der Datenschutzmaßnahmen. Zudem spielen die Akzeptanz und das Bewusstsein der Nutzer eine entscheidende Rolle für den Erfolg dieser Strategien. Für einige Nutzer wird das Installieren solcher Netzwerke und Open Source Systemen zudem eine zu große Hürde sein, vorallem wenn die technische Affinität fehlt. Sollten Nutzer sich jedoch die Zeit nehmen, um sich mit den hier behandelten Möglichkeiten auseinanderzusetzen, so können sie ihr Smart Home absichern und die Gerätehersteller aussperren.

4.3 Ausblick auf zukünftige Forschungen

Angesichts der rasanten Entwicklung im Bereich der Smart Home Technologien und der allgemeinen digitalen Vernetzung ist zu erwarten, dass sowohl die Datenschutzrisiken als auch die Möglichkeiten zu deren Bewältigung weiter zunehmen werden. Technologische Innovationen, etwa im Bereich der künstlichen Intelligenz können neue Wege eröffnen, um Datenschutz und Datensicherheit in Smart Homes zu stärken. Des weiteren sollte die Effektivität der in dieser Arbeit gezeigten Methoden noch einmal in einem Laborsystem untersucht werden. So lässt sich sicherstellen, dass tatsächlich keinen Daten abfließen können. Zusätzlich könnte es interessant sein, eine Erhebung durchzuführen, wie viele Hersteller von internetfähigen Smart Home Produkten, also beispielsweise weiße Produkte, welche über WLAN funktionieren, tatsächlich lokale APIs anbieten und ob diese eine tatsächliche Alternative darstellt.

Literaturverzeichnis

Apthorpe, Noah J., D. Reisman und N. Feamster (2017). „Closing the Blinds: Four Strategies for Protecting Smart Home Privacy from Network Observers“. In: URL: *https://arxiv.org/abs/1705.06809*.

Ardito, Luca, Luca Barbato und Paolo Mori amd Andrea Saracino (2022). „Preserving Privacy in the Globalized Smart Home: The SIFIS-Home Project“. In: *IEEE Security and Privacy* 20.1, S. 33–44. DOI: *10.1109/MSEC.2021.3118561*.

Chalhoub, george (2020). „The UX of Things: Exploring UX Principles to Inform Security and Privacy Design in the Smart Home“. In: CHI EA '20, S. 1–6. DOI: *10.1145/3334480.3381436*. URL: *https://doi.org/10.1145/3334480.3381436*.

Davenport, Nikole (2016). „Smart Washers May Clean Your Clothes, But Hacks Can Clean Out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on a Line, 32 J. Marshall J. Info. Tech. & Privacy L. 259“. In: URL: *https://repository.law.uic.edu/jitpl/vol32/iss4/2/*.

Guhr, Nadine u. a. (21. Jan. 2020). „Privacy concerns in the smart home context“. In: *SN Applied Sciences* 2.2, S. 247. ISSN: 2523-3971. DOI: *10.1007/s42452-020-2025-8*. URL: *https://doi.org/10.1007/s42452-020-2025-8*.

Huang, Xuping u. a. (März 2023). „Simulating and Estimating the Effectiveness of Security Notification by ISP to Malware-Infected Users“. In: *Journal of Information Processing* 31, S. 165–173. DOI: *10.2197/ipsjjip.31.165*.

Hussain, Fida und M. Qi (2018). „Integrated Privacy Preserving Framework for Smart Home“. In: *Proceedings of the 2018 15th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*. DOI: *10.1109/FSKD.2018.8687201*. URL: *https://dx.doi.org/10.1109/FSKD.2018.8687201*.

Jacobsson, Andreas und Paul Davidsson (2015). „Towards a model of privacy and security for smart homes“. In: S. 727–732. DOI: *10.1109/WF-IoT.2015.7389144*.

Kraemer, Martin J. (2018). „Preserving Privacy in Smart Homes: A Socio-Cultural Approach“. In: CHI EA '18, S. 1–4. DOI: *10.1145/3170427.3173018*. URL: *https://doi.org/10.1145/3170427.3173018*.

Li, Rong u. a. (2023). „ZPA: A Smart Home Privacy Analysis System Based on ZigBee Encrypted Traffic“. In: *IEEE Wireless Communications and Mobile Computing*. URL: *https://dx.doi.org/10.1155/2023/6731783*.

Mocrii, Dragos, Yuxiang Chen und Petr Musilek (2018). „IoT-based smart homes: A review of system architecture, software, communications, privacy and security“. In: *Internet of*

Things 1-2, S. 81–98. ISSN: 2542-6605. DOI: *https://doi.org/10.1016/j.iot.2018.08.009*. URL: *https://www.sciencedirect.com/science/article/pii/S2542660518300477*.

OpenThread (2023). „OpenThread Border Router“. In: URL: *https://openthread.io/guides/border-router?hl=de*.

Panwar, Nisha u. a. (2019). „Smart Home Survey on Security and Privacy“. In: *arXiv*. URL: *https://arxiv.org/abs/1904.05476*.

Schomakers, Eva-Maria, Hannah Biermann und Martina Ziefle (2021). „Users' Preferences for Smart Home Automation – Investigating Aspects of Privacy and Trust“. In: *Telematics and Informatics* 64, S. 101689. ISSN: 0736-5853. DOI: *https://doi.org/10.1016/j.tele.2021.101689*. URL: *https://www.sciencedirect.com/science/article/pii/S0736585321001283*.

Strese, Hartmut u. a. (Mai 2010). *Smart Home in Deutschland*. Berlin: Institut für Innovation und Technik (iit). ISBN: 978-3-89750-165-2.

Zigbee2MQTT (2024). „OTA updates“. In: URL: *https://www.zigbee2mqtt.io/guide/usage/ota_updates.html*.

Glossar

Cloud Die Cloud bezieht sich auf das Speichern und Zugreifen von Daten und Programmen über das Internet statt auf der eigenen Festplatte oder lokalen Servern. Es handelt sich um einen zentralen Online-Speicherort, der jederzeit und von überall aus zugänglich ist, sofern eine Internetverbindung besteht. Die Cloud ermöglicht es, Daten zu speichern, zu teilen und auf diese zuzugreifen, ohne physische Speichermedien nutzen zu müssen. Dies fördert die Mobilität und Zusammenarbeit, da Informationen leicht mit anderen geteilt und von verschiedenen Geräten aus abgerufen werden können. Während "Cloud" oft synonym mit "Cloud-Computing" verwendet wird, fokussiert sich der Begriff speziell auf die Speicher- und Zugriffsaspekte von Daten und Anwendungen im Internet.

Distributed Denial of Service Ein Distributed Denial of Service (DDoS) Angriff ist eine spezifische Form eines Denial of Service (DoS) Angriffs, bei dem viele kompromittierte Computersysteme - oft Teil eines Botnetzes - verwendet werden, um ein einzelnes Ziel, wie einen Server, eine Website oder ein Netzwerk, mit einer Flut von Internetverkehr zu überlasten. Ziel ist es, die normalen Funktionen des Ziels zu stören oder vollständig außer Betrieb zu setzen, indem seine Ressourcen bis zum Punkt der Überlastung beansprucht werden. Dies führt dazu, dass legitime Benutzeranfragen nicht mehr bearbeitet werden können. Im Gegensatz zu einfachen DoS-Angriffen, die von einem einzelnen System ausgehen, nutzen DDoS-Angriffe die erhöhte Angriffskraft vieler beteiligter Systeme, was sie schwieriger zu erkennen und abzuwehren macht. DDoS-Angriffe können verschiedene Formen annehmen und sich auf unterschiedliche Netzwerkschichten richten, was eine breite Palette von Abwehrstrategien erforderlich macht.

Firewall Eine Firewall ist ein Netzwerksicherheitssystem, das den ein- und ausgehenden Netzwerkverkehr überwacht und regelt, basierend auf vorher festgelegten Sicherheitsregeln. Ihr Hauptzweck ist es, unautorisierten Zugriff von außen auf ein privates Netzwerk oder einen Computer zu verhindern. Firewalls können sowohl als Hardware- als auch als Software-Lösungen implementiert werden, oder als eine Kombination von beidem, und sind ein wesentlicher Bestandteil der Netzwerksicherheit. Sie arbeiten, indem sie den Datenverkehr anhand von definierten Parametern wie IP-Adressen, Domain-Namen, Programmen, Ports und Protokollen filtern, wodurch nur befugter Datenverkehr das Netzwerk betreten oder verlassen kann. Moderne Firewalls bieten neben dem traditionellen Paketfiltern auch weiterführende Funktionen wie Intrusion Prevention Systeme (IPS), die Netzwerke proaktiv vor verschiedenen Arten von Angriffen schützen, und

VPN-Unterstützung für sichere Fernverbindungen. Firewalls sind ein grundlegender Schutzmechanismus, der dazu beiträgt, Netzwerke und Systeme vor einer Vielzahl von Bedrohungen zu schützen, einschließlich Viren, Würmern, Ransomware und DDoS-Angriffen.

Mesh Netzwerk Ein Mesh Netzwerk (englisch: Mesh Network) ist ein Netzwerktopologie-Konzept, bei dem einzelne Knotenpunkte (wie Computer, mobile Geräte, Router) direkt, dynamisch und nicht-hierarchisch miteinander verbunden sind, um eine effiziente Datenübertragung zu ermöglichen. Im Gegensatz zu traditionellen sternförmigen oder baumförmigen Netzwerken, bei denen Daten über zentrale Knotenpunkte (wie Switches oder Router) laufen, ermöglicht ein Mesh Netzwerk eine Punkt-zu-Punkt-Kommunikation zwischen den Geräten. Dies führt zu einer erhöhten Redundanz, da Daten über verschiedene Pfade weitergeleitet werden können, was die Ausfallsicherheit und Robustheit des Netzwerks verbessert.

Mesh Netzwerke sind besonders vorteilhaft in Umgebungen, wo die Netzabdeckung schwierig ist oder wo eine hohe Ausfallsicherheit erforderlich ist. Sie werden häufig in drahtlosen Netzwerken (Wireless Mesh Networks) eingesetzt, finden aber auch in verdrahteten Netzwerken Anwendung. Ein bekanntes Anwendungsbeispiel sind Smart Home-Systeme, in denen verschiedene Geräte wie Leuchten, Sensoren und Kameras miteinander vernetzt sind, um eine umfassende Steuerung und Überwachung zu ermöglichen.

Ein weiterer wichtiger Aspekt von Mesh Netzwerken ist ihre Skalierbarkeit. Da neue Geräte einfach hinzugefügt werden können, indem sie sich mit nahegelegenen Knoten verbinden, kann das Netzwerk flexibel erweitert werden, ohne dass eine umfassende Neukonfiguration erforderlich ist. Dies macht Mesh Netzwerke ideal für wachsende oder sich verändernde Umgebungen, wie beispielsweise städtische Gebiete, Veranstaltungsorte oder große Betriebsgelände.

Zu den Herausforderungen beim Einsatz von Mesh Netzwerken gehören die Netzwerkverwaltung und die Sicherstellung der Datenintegrität, da die dezentrale Struktur eine komplexe Koordination und fortgeschrittene Verschlüsselungstechniken erfordert, um Sicherheit und Privatsphäre zu gewährleisten.

Im Vergleich zu Smart Homes, die auf einfache Vernetzungsmodelle zurückgreifen können, bieten Mesh Netzwerke eine flexible und robuste Lösung für die Vernetzung einer großen Anzahl von Geräten, wobei sie durch ihre dynamische und selbstheilende Struktur die Zuverlässigkeit und Effizienz der Datenübertragung verbessern.

Open Source Open Source bezeichnet Software, deren Quellcode öffentlich zugänglich ist und von der Gemeinschaft genutzt, verändert und weiterverbreitet werden darf. Dieses

Konzept steht im Gegensatz zu proprietärer Software, bei der der Quellcode geheim gehalten und die Nutzung, Modifikation und Weitergabe durch Urheberrechte streng geregelt sind. Die Open-Source-Philosophie basiert auf der Idee der kollektiven Zusammenarbeit und dem freien Austausch von Wissen, um Softwareentwicklungen voranzutreiben und für eine breite Nutzerbasis verfügbar zu machen.
Die Vorteile von Open-Source-Software liegen in der Förderung von Innovation durch gemeinschaftliche Entwicklung, erhöhter Sicherheit durch transparente Überprüfungsmöglichkeiten des Codes, sowie in der Flexibilität, Software an spezifische Bedürfnisse anzupassen. Darüber hinaus können Kosten gesenkt werden, da Open-Source-Software oft kostenlos oder zu deutlich geringeren Kosten als proprietäre Lösungen angeboten wird. Es gibt zahlreiche bekannte Open-Source-Projekte, wie das Betriebssystem Linux, der Webbrowser Mozilla Firefox und das Bürosoftwarepaket LibreOffice. Die Verwaltung und Koordination von Open-Source-Projekten erfolgt häufig über Plattformen wie GitHub oder GitLab, wo Entwickler zusammenarbeiten, Code teilen und Feedback geben können.
Der Hauptunterschied zwischen Open Source und anderen Software-Lizenzmodellen liegt in der legalen und praktischen Möglichkeit für Endnutzer und Entwickler, Einblick in den Quellcode zu erhalten, diesen zu modifizieren und verbesserte Versionen innerhalb der Gemeinschaft zu teilen. Dies fördert nicht nur die technologische Entwicklung, sondern unterstützt auch die Schaffung von Gemeinschaften, die auf gegenseitigem Respekt, Zusammenarbeit und dem freien Austausch von Wissen basieren.

Smart Building Ein Smart Building, oder intelligentes Gebäude, bezeichnet eine erweiterte Anwendung des Smart Home-Konzepts, das sich auf gewerbliche, industrielle oder öffentliche Gebäude erstreckt. Wie bei einem Smart Home werden auch hier Geräte und Systeme vernetzt, um Prozesse wie Beleuchtung, Heizung, Lüftung, Klimatisierung (HLK), Sicherheit und weitere Gebäudebetriebssysteme effizient zu steuern und zu überwachen. Der Hauptunterschied zu Smart Homes liegt im Umfang und in der Komplexität der Automatisierung und Steuerung: Smart Buildings zielen darauf ab, den Betrieb, die Instandhaltung und die Nutzung des Gebäudes durch fortgeschrittene Automatisierungssysteme und Datenanalyse zu optimieren, um Energieeffizienz, Komfort, Gebäudesicherheit und Nachhaltigkeit zu maximieren. Darüber hinaus integrieren Smart Buildings oft Technologien zur Verbesserung der Raumnutzung und zur Unterstützung der Gesundheit und des Wohlbefindens der Nutzer.
Im Vergleich zu Smart Homes, die sich hauptsächlich auf die Verbesserung des Wohnkomforts und der persönlichen Effizienz in einem einzelnen Haushalt konzentrieren, decken Smart Buildings ein breiteres Spektrum an Funktionen und Zielen ab. Sie sind in der Regel mit fortschrittlicheren Systemen für das Energiemanagement, die

Raumbelegung, die Gebäudeinstandhaltung und -sicherheit ausgestattet und dienen der Optimierung der gesamten Gebäudeleistung. Während Smart Home-Systeme oft nachträglich in bestehende Wohnstrukturen integriert werden können, wird die Smart Building-Technologie häufig bereits in der Planungs- und Bauphase von Gebäuden berücksichtigt, um eine umfassende Integration und Maximierung der Gebäudeeffizienz zu ermöglichen.

Smart Home Ein Smart Home bezeichnet ein Wohnkonzept, bei dem Haushalts- und Multimedia-Geräte miteinander vernetzt sind und zentral gesteuert werden können. Dies ermöglicht eine Automatisierung von Prozessen im Haushalt und eine individuelle Programmierung von Abläufen, um den Wohnkomfort zu erhöhen, die Energieeffizienz zu verbessern und die Sicherheit zu erhöhen. Die Steuerung kann über verschiedene Schnittstellen erfolgen, darunter Sprachsteuerung, Smartphone-Apps, Tablets oder PCs. Typische Anwendungen eines Smart Homes umfassen die automatische Lichtsteuerung, die Temperaturregelung, die Steuerung von Unterhaltungselektronik, die Überwachung durch Sicherheitskameras und Alarm-Systeme, sowie die Haushaltsrobotik wie intelligente Staubsauger. Die Vernetzung der Geräte kann über verschiedene Standards und Protokolle wie WLAN, Bluetooth, ZigBee oder Z-Wave erfolgen. Smart Home-Systeme bieten Potenzial für mehr Lebensqualität und Energieeffizienz, werfen jedoch auch Fragen des Datenschutzes und der Sicherheit auf.

Abkürzungsverzeichnis

API Application Programming Interface

CHIP Connected Home over IP

EU Europäische Union

IoT Internet of Things

IP Internet Protocol

WLAN Wireless Local Area Network