HOCHSCHULE
MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Herr
Max Führer

Systematische Übersichtsarbeit für zukünftige Forschungsgegenstände forensischer Auswertungen von Hausautomatisierungen

Mittweida, März 2024

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Systematische Übersichtsarbeit für zukünftige Forschungsgegenstände forensischer Auswertungen von Hausautomatisierungen

Autor:
Max Führer

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO20w1-B

Erstprüfer:
Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
Felix Fischer, M.Sc.

Einreichung:
Mittweida, 10.03.2024

Verteidigung/Bewertung:
Mittweida, 2024

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

Systematic review for future research objects of forensic evaluations of home automation systems

Author:
Max Führer

Course of Study:
Applied Computer Science

Seminar Group:
FO20w1-B

First Examiner:
Prof. Dr. rer. nat. Dirk Labudde

Second Examiner:
Felix Fischer, M.Sc.

Submission:
Mittweida, 10.03.2024

Defense/Evaluation:
Mittweida, 2024

Bibliografische Beschreibung

Führer, Max:
Systematische Übersichtsarbeit für zukünftige Forschungsgegenstände forensischer Auswertungen von Hausautomatisierungen. – 2024. – 70 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2024.

Referat

Die Forschungsarbeit analysiert Hausautomatisierungstechnologien deutscher Hersteller im Kontext forensischer Untersuchungen mit Fokus auf die Entwicklung eines Verständnisses für Einsatzmöglichkeiten, Sicherheitsaspekte und die Erzeugung forensischer Daten. Eine umfassende Literaturanalyse aktueller deutscher und englischer Studien offenbart eine Forschungslücke bei Produkten deutscher Hersteller, während internationale Produkte, insbesondere Smart Speaker und Wearables, aufgrund ihrer persönlichen Interaktion mit dem Nutzer starkes forensisches Potenzial bieten. Die Analyse zeigt zudem eine Vernachlässigung der Betrachtung der Rechtskonformität bezogen auf die Datenspeicherung in vorhandenen Studien. Die Ergebnisse unterstreichen, dass die Smart Home Forensik ein wachsendes Forschungsfeld darstellt, welches signifikantes Entwicklungspotenzial aufweist. Es werden Herausforderungen wie die schnelle technologische Entwicklung, rechtliche Unsicherheiten, der Mangel an standardisierten Protokollen und die Veränderlichkeit der Daten durch Nutzereinfluss identifiziert. Die Arbeit betont die Notwendigkeit weiterer Forschung, um diese dynamische Disziplin voranzutreiben.

Abstract

The research analyzes home automation technologies from German manufacturers in the context of forensic investigations with a focus on developing an understanding of possible applications, security aspects and the generation of forensic data. A comprehensive literature review of current German and English studies reveals a research gap for products from German manufacturers, while international products, especially smart speakers and wearables, offer strong forensic potential due to their personal interaction with the user. The analysis also shows a neglect of the consideration of legal compliance in relation to data storage in existing studies. The results underline that smart home forensics is a growing field of research with significant development potential. Challenges such as rapid technological development, legal uncertainties, the lack of standardized protocols and the variability of data due to user influence are identified. The work emphasizes the need for further research to advance this dynamic discipline.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AES ..... Advanced Encryption Standard

AP ..... Wireless Access Point

API ..... Application Programming Interface

BLE ..... Bluetooth Low Energy

BSS ..... Basic Service Set

CBS ..... cloudbasierte Dienste

CCMP ..... Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CFIBD ..... Cloud-centric framework for isolating big data as forensic evidence from IoT infrastructures

CPS ..... cyber-physische Systeme

DFIF-IoT ..... Digital forensic investigation framework for IoT

DNS ..... Domain Name System

DSGVO ..... Datenschutz-Grundverordnung

DSSS ..... Direct Sequence Spread Spectrum

ESSID ..... Extended Service Set Identifier

FAIoT ..... Forensic-aware IoT

GPS ..... Global Positioning System

HEMS ..... Heim-Energiemanagementsystem

HTTPS ..... Hypertext Transfer Protocol Secure

IEEE ..... Institute of Electrical and Electronic Engineers

IO ..... Input/Output

IoT ..... Internet of Things

ISM ..... Industrial Scientific and Medical

JSON ..... JavaScript Object Notation

KML ..... Keyhole Markup Language

KRACK ..... Key Reinstallation Attack

NAS ..... Network Attached Storage

PoE ..... Power over Ethernet

SAE ..... Simultaneous Authentication of Equals

SIG . . . . . Bluetooth Special Interest Group

SPoF . . . . . Single Point of Failure

SSID . . . . . Service Set Identifier

SSL . . . . . Secure Sockets Layer

TCP/IP . . . . . Transmission Control Protocol/Internet Protocol

TFS . . . . . Tür- und Fenstersicherung

TKIP . . . . . Temporal Key Integrity Protocol

UART . . . . . Universal Asynchronous Receiver Transmitter

UPnP . . . . . Universal Plug and Play

USB . . . . . Universal Serial Bus

VOC . . . . . Volatile Organic Compounds

WEP . . . . . Wired Equivalent Privacy

WiFi . . . . . Wireless Fidelity

WLAN . . . . . Wireless Local Area Network

WPA . . . . . WLAN Protected Access

XML . . . . . Extensible Markup Language

1 Einleitung

1.1 Hintergrund und Relevanz des Themas

In den letzten Jahren wurden bedeutende Fortschritte in den Bereichen der Informations- und Kommunikationstechnologie verzeichnet. Technologien wie Kommunikationsnetzwerke, mobile Endgeräte, Lösungen für das Internet of Things (IoT), cloudbasierte Dienste (CBS) und cyber-physische Systeme (CPS) haben technologisch fortgeschrittenen Gesellschaften zahlreiche Vorteile gebracht [1–3]. Gleichzeitig bringen diese technologischen Fortschritte auch neue Herausforderungen in der Cybersicherheit mit sich, die tiefgreifende Einflüsse auf diverse Sektoren ausüben.

Ein Sektor, der eine signifikante Transformation erfahren hat, ist die Hausautomatisierung, auch bekannt als Smart Home. Ursprünglich ein Nischenmarkt, der hauptsächlich Technologieenthusiasten ansprach, hat sich dieser Bereich dank der Einführung von IoT-Technologien, Cloud-Computing, künstlicher Intelligenz sowie einem zunehmend breiteren Spektrum an Sensor- und Aktuatorfähigkeiten zu einem integralen Bestandteil moderner Haushalte entwickelt. Diese Entwicklung spiegelt die Konvergenz von Gebäudetechnik und Informations- und Kommunikationstechnologie mit dem Ziel wider, das Wohnen komfortabler, sicherer und energieeffizienter zu gestalten. In dieser Arbeit werden die Begriffe Hausautomatisierung und Smart Home synonym verwendet, um diese fortschrittlichen, vernetzten und automatisierten Wohnumgebungen zu beschreiben, die nicht nur praktische Lösungen bieten, sondern auch attraktive Ziele für Cyberangriffe darstellen. [4]

In diesem Kontext gewinnt die forensische Untersuchung von Hausautomatisierungssystemen, die in modernen Haushalten immer häufiger anzutreffen sind, zunehmend an Bedeutung. Es ist entscheidend, Systeme zu identifizieren, die forensisch relevant sind, um im Falle eines Sicherheitsvorfalls prioritäre Ermittlungen durchführen zu können. Solche Untersuchungen können entscheidend sein, um potenzielle Straftaten aufzudecken und nachzuweisen. Die Entwicklung von Standards und Richtlinien für die forensische Untersuchung dieser Systeme ist daher von großer Bedeutung, um eine effektive Reaktion auf Cyberbedrohungen in diesem sich schnell entwickelnden Bereich zu gewährleisten.

1.2 Zielsetzung

Die Forschungsarbeit zielt darauf ab, ein umfassendes Verständnis für verschiedene Aspekte der Hausautomatisierung und deren forensischer Relevanz zu entwickeln. Sie untersucht die vielfältigen Anwendungsgebiete und Einsatzszenarien der Hausautomatisierung, um deren Einfluss auf forensische Untersuchungen zu verstehen. Ein weiterer Schwerpunkt liegt auf der

Identifikation und Analyse der in Hausautomatisierungssystemen verwendeten Steuerungssoftwares, insbesondere in Bezug auf die von ihnen hinterlassenen forensischen Spuren. Des Weiteren werden spezifische Sicherheitsprobleme und Risiken, die sich aus der Nutzung von Geräten in der Hausautomatisierung ergeben, beleuchtet und Möglichkeiten ihrer forensischen Untersuchung erörtert. Von besonderem Interesse sind dabei jene Geräte und Technologien, die für forensische Analysen besonders relevant sind sowie Methoden, um deren Verhalten zu dokumentieren und zu analysieren. Schließlich bietet die Arbeit einen Ausblick auf zukünftige Trends und Forschungsfelder im Bereich der forensischen Auswertungen von Hausautomatisierungen, um neue Forschungsfelder in diesem dynamischen Forschungsbereich zu eröffnen.

1.3 Abgrenzung des Themas

Die vorliegende Forschungsarbeit konzentriert sich auf die Analyse und Bewertung von Hausautomatisierungssystemen im Kontext des Reallabors Telewerk in Mittweida, welches sich als Forschungsprojekt auf die Erforschung neuer Arbeitsformen und Technologien spezialisiert. Es bietet eine Plattform zur Untersuchung der Wechselwirkungen zwischen Menschen, Technik sowie Umwelt und fokussiert sich auf Themen wie Cybersicherheit, IoT-Vernetzung und nachhaltige Energie. Unter Beachtung der geografischen Eingrenzung liegt der Fokus primär auf Produkten und Technologien, die in Sachsen und, falls dort nicht verfügbar, in Deutschland entwickelt wurden. Internationale Produkte werden nur dann einbezogen, wenn sie auf dem deutschen Markt nicht erhältlich sind. Dieser Ansatz gewährleistet eine regionalspezifische Relevanz und Praxisnähe der Forschungsergebnisse.

Der zeitliche Rahmen für die Betrachtung von Forschungsarbeiten ist auf maximal fünf Jahre beschränkt, um die Relevanz und Aktualität der Informationen sicherzustellen. Dieser Ansatz reflektiert die schnelle Entwicklung und Dynamik im Bereich der Hausautomatisierung und stellt sicher, dass die Ergebnisse der Übersichtsarbeit die neuesten technologischen Fortschritte und Trends widerspiegeln.

Die Zielgruppe der Arbeit umfasst Experten aus den Bereichen Forensik und IT-Sicherheit sowie Forscher, die sich mit Hausautomatisierungssystemen beschäftigen. Dieser spezifische Fokus ermöglicht es, Inhalte zu liefern, die für diese Expertengruppen von direkter Relevanz sind und praktische Einblicke in zukünftige Forschungsfelder bieten. Die Arbeit nimmt dabei bewusst keine direkte Bezugnahme auf rechtliche Aspekte im Sinne der Datenschutz-Grundverordnung (DSGVO) oder des deutschen Rechts. Der Schwerpunkt liegt vielmehr auf der technischen Analyse und der Identifizierung offener Forschungslücken in den bestehenden Produkten der Hausautomatisierung. Diese fokussierte Betrachtung ermöglicht es, ein detailliertes Verständnis der technischen Herausforderungen und Potenziale in diesem Bereich zu entwickeln.

Letztendlich basiert die Arbeit auf einer umfassenden Literaturanalyse existierender Forschungsarbeiten. Diese methodische Vorgehensweise ermöglicht es, den aktuellen Stand der Forschung zu ermitteln und zukünftige Forschungsfelder systematisch zu identifizieren. Durch diese methodische Herangehensweise wird ein fundierter Überblick über den aktuellen Wissensstand im Bereich der Hausautomatisierung und dessen forensische Auswertung gewährleistet.

1.4 Aufbau der wissenschaftlichen Arbeit

Beginnend mit einer Einleitung, wird der Kontext und die Relevanz der Arbeit dargelegt. Das darauf folgende Kapitel Kapitel 2 bietet eine grundlegende Aufbereitung des Wissens, das für das Verständnis der Arbeit notwendig ist. Es behandelt die Hauptkomponenten eines Smart Home Systems, setzt sich mit verschiedenen Kommunikationsstandards auseinander und vergleicht verschiedene Lösungen hinsichtlich der Umsetzung eines Smart Homes. Zudem erfolgt ein Einblick in den aktuellen Stand der IoT-Forensik sowie der damit verbundenen Herausforderungen.

In Kapitel 3 erfolgt eine Kategorisierung der Hausautomatisierungstechnologien und die Vorstellung eines Bewertungsschemas zur Analyse ihrer forensischen Relevanz. Dieses Kapitel beinhaltet auch die Bewertung einzelner Geräte und diskutiert Herausforderungen und Limitationen im Kontext dieser Bewertungen.

Das Kapitel 4 diskutiert die Ergebnisse, identifiziert Muster und Trends bezüglich der forensischen Relevanz und zeigt Limitationen der Forschungsarbeit auf. Darüber hinaus erfolgt eine Auflistung aller Smart Home-Geräte, wobei in einem hypothetischen Kontext ihre potenzielle forensische Relevanz erörtert wird.

Zum Abschluss bietet Kapitel 5 eine Übersicht über die Inhalte dieser Arbeit, umreißt potenzielle zukünftige Entwicklungen sowie Forschungsfelder und evaluiert die Beantwortung der gestellten Forschungsfragen.

2 Grundlagen

Im Folgenden wird ein Überblick über die Hauptkomponenten und Technologien eines Hausautomatisierungssystems gegeben, um ein vertieftes Verständnis ihrer Funktionsweisen zu ermöglichen. Dabei wird vorausgesetzt, dass ein grundsätzliches Interesse und eine Basiskenntnis in Bezug auf IoT-Forensik vorhanden sind. Ziel ist es, spezifische Herausforderungen und Methoden, die besonders im Bereich der Forensik von IoT von Bedeutung sind, detailliert zu beleuchten.

2.1 Definition Hausautomatisierung

Smart Home, auch bekannt als Hausautomatisierung, bezieht sich auf die Integration von Technologie und Diensten in Wohngebäuden zur Verbesserung des Komforts, der Effizienz und der Energieverwaltung. In der akademischen Literatur gibt es verschiedene Ansätze zur Definition dieses Konzepts. Laut Darby [5] können zwei Hauptperspektiven unterschieden werden:

1. *haus- und nutzerzentriert*: Das Smart Home wird als ein hochautomatisiertes Wohngebäude mit integrierten Geräten betrachtet, das auf moderner Technologie, Komfort und häuslicher Effizienz basiert.
2. *gebäude- und systemorientiert:* Das Smart Home ist fokussiert auf die Energieeffizienz, Hilfsdienste und dezentraler Energieerzeugung, unterstützt durch Informations- und Kommunikationstechnologie.

Beide Definitionen betonen die Rolle der Kommunikationstechnologie bei der Vernetzung von Geräten und ermöglichen Fernzugriff sowie Steuerung zur Bereitstellung verschiedener Dienste [5]. Bei der Diskussion über Hausautomatisierung ist es essenziell, eine Reflexion darüber anzustellen, wie die Begriffe „smart“ oder „intelligent“ definiert werden könnten. Es gilt zu erforschen, welche spezifischen Merkmale ein intelligentes Haus von einem konventionellen Wohngebäude unterscheiden. Edwards und Grinter [6] identifizieren vier charakteristische Merkmale von Intelligenz im Kontext intelligenter Umgebungen:

1. Intelligente Systeme sind in der Lage, durch die Analyse von Sensordaten eine Bewertung des gegenwärtigen Umgebungszustandes vorzunehmen.
2. Intelligente Systeme sind in der Lage, den aktuellen Zustand der Umgebung anzunehmen, indem sie mehrere Faktoren auf einmal berücksichtigen.
3. Intelligente Systeme besitzen die Fähigkeit, basierend auf ihrer eigenen Einschätzung der gegebenen Umstände, Nutzerintentionen zu antizipieren.
4. Intelligente Systeme sind aufbauend auf diesen angenommenen Intentionen in der Lage, proaktive Maßnahmen zu ergreifen.

Schließlich sind die Leistungskennzahlen in einem intelligenten Haus darauf ausgerichtet, den Komfort und die Produktivität der Bewohner zu maximieren, während gleichzeitig die Betriebskosten, wie Energie und andere Versorgungsleistungen minimiert werden sollen [7]. Ein intelligentes System sollte anpassungsfähig, kontextbewusst, adaptiv und vorausschauend sein, um diese Ziele zu erreichen. [8, 9]

2.2 Hauptkomponenten im Smart Home

Im Smart Home-Sektor lassen sich fünf zentrale Komponenten identifizieren: Sensoren, Aktoren, Controller, Gateways und das Steuernetz. Nachfolgend werden diese Bestandteile erläutert.

Sensoren Im Kontext der Hausautomatisierung spielen Sensoren eine zentrale Rolle als technologische Schnittstellen, die spezifische physikalische oder technische Größen messen und diese Informationen für weitere Verarbeitungszwecke zur Verfügung stellen. Ein Sensor fungiert als eine Vorrichtung, die bestimmte Parameter wie beispielsweise Temperatur, Geschwindigkeit, Spannung oder Frequenz erfasst und diese in analoge oder digitale Werte umwandelt. Diese Umwandlung ermöglicht es, dass Sensoren als integraler Bestandteil eines Kommunikationsnetzwerkes agieren, indem sie generierte Daten an andere Geräte übermitteln. [10, 11]

Innerhalb von Smart Home Systemen finden sich vielfältige Anwendungen für Sensoren. Beispielsweise tragen Temperatursensoren in Raumthermostaten zur Klimaregulierung bei, während Bewegungsmelder, Türsensoren und Rauchmelder wichtige Sicherheitsfunktionen erfüllen. Jeder dieser Sensoren ist darauf spezialisiert, bestimmte Umgebungsvariablen zu erfassen und entsprechende Signale zu generieren. [11]

Aktoren Diese Elemente, die auch unter dem Begriff Aktuatoren bekannt sind, fungieren in der Hausautomatisierung als Schnittstellen zwischen der Informationsverarbeitung und der physischen Welt. Ein Aktor nimmt Stellinformationen in Form von geringer Leistung, die entweder analog oder digital von der Recheneinheit eines eingebetteten Systems ausgehen, auf und wandelt diese in leistungsbehaftete Signale um. Diese Signale werden in einer Energieform übertragen, die zur Beeinflussung des jeweiligen Prozesses erforderlich ist. Diese Energie kann in verschiedenen Formen wie elektrischer, thermischer, chemischer oder Strömungsenergie vorliegen. [10]

Diese Komponenten führen spezifische Aktionen wie Ein- oder Ausschalten, Dimmen, Aufladen oder Verriegeln aus, wodurch sie direkt auf die physischen Komponenten des Haussystems einwirken [11]. Beispielhafte Anwendungen für Aktoren in der Hausautomatisierung sind Fenstermotoren, die das Öffnen und Schließen von Fenstern steuern, Lichtschalter und -dimmer, die die Beleuchtung regulieren, sowie elektrische Türschlösser, die für Sicherheit und Komfort sorgen.

Controller Im Smart Home System spielt der Controller eine entscheidende Rolle, da er als zentrales Steuerelement agiert, der die Intelligenz des Steuerungsnetzwerks bündelt. Er ist dafür zuständig, Daten von Sensoren und Aktoren zu empfangen, zu verarbeiten und basierend darauf automatisierte Prozesse im intelligenten Heim umzusetzen. [11]

Darüber hinaus fungiert er als zentrale Schnittstelle, über die er Befehle von verschiedenen Benutzeroberflächen - darunter Smart Home-Apps, intelligente Fernbedienungen oder Universalschalter - sowie Sprachbefehle entgegennimmt. Diese Befehle werden anschließend via Funk an die entsprechenden Smart-Home-Geräte weitergeleitet, um bestimmte Aktionen oder Reaktionen zu initiieren. [12]

Gateways Das Gateway ist das Verbindungsglied zwischen dem internen Kommunikationsnetzwerk des Hauses und externen Netzwerken, wie dem Transmission Control Protocol/Internet Protocol (TCP/IP)-basierten Internet oder Mobilfunknetzwerken. Diese Funktion ist besonders im Bereich des IoT von Bedeutung, in dessen Funktionalität das Gateway als Vermittler zwischen einer Vielzahl von Sensornetzwerken und Cloud-Plattformen oder Datenzentren agiert, die über das Internet verbunden sind. [11, 13]

Ein Hauptziel des Gateways im IoT-Kontext ist es, die Heterogenität, die durch verschiedene Geräte entsteht und die eine immense Menge an Daten in unterschiedlichen Formaten sammeln, zu bewältigen. Dabei leitet es diese gesammelten Daten an höhere Instanzen, wie Cloud-Plattformen weiter. Für eine ordnungsgemäße Funktion und Verwaltung von IoT-Systemen ist es notwendig, dass die gesammelten Daten gereinigt, vorverarbeitet und gefiltert werden, bevor sie basierend auf den erforderlichen Anwendungen an Cloud-Plattformen gesendet werden. [13]

In Bezug auf die Funktionalität gibt es zwei Arten von Gateways: das Basic Gateway und das Smart Gateway. Das Basic Gateway fungiert als Proxy zwischen IoT-Geräten mit geringer Leistung und der Cloud-Plattform, indem es die eingehenden Daten einfach weiterleitet. Im Gegensatz dazu handhabt ein Smart Gateway die Daten effizienter, indem es diese vorverarbeitet, filtert, analysiert und nur die relevanten oder notwendigen Daten an die Cloud-Plattform übermittelt. Diese differenzierte Datenverarbeitung ermöglicht es dem Smart Gateway, eine entscheidende Rolle bei der Reduzierung der Datenmenge zu spielen, die zur weiteren Analyse an die Cloud-Plattform gesendet wird. [13]

Steuernetz Das Steuernetz basiert auf unterschiedlichen Übertragungsmedien, die je nach Anwendungsfall und Umgebungsbedingungen ausgewählt werden. Im Folgenden werden die verschiedenen Übertragungstechnologien und ihre spezifischen Eigenschaften im Kontext der Hausautomatisierung erläutert.

Ein häufig verwendetes Medium für die Datenübertragung in Smart Home Systemen ist das Bus-Kabel, speziell das J-Y(ST)Y 2x2x0,8 mm² Kabel. Dieses Kabel eignet sich besonders für niedrige Datenraten und wird oft in Neubauten integriert, da seine Installation in bestehenden Gebäuden aufgrund der notwendigen baulichen Eingriffe kostenintensiv sein kann. [14]

Eine Alternative hierzu bietet die Powerline-Technologie, bei der die Datenübertragung über das existierende 230 V Stromnetz erfolgt. Diese Methode erfordert keine zusätzlichen Datenleitungen, lediglich spezielle Steckdosenadapter und Vorschaltklemmen sind notwendig, was sie zu einer praktikablen Lösung für bestehende Strukturen macht. [14]

Das Flachkabelsystem ist eine weitere Option, die sich durch eine geringe Kabelstärke von nur 0,3 mm auszeichnet. Diese Beschaffenheit ermöglicht eine unkomplizierte Montage auf Wänden ohne invasive Eingriffe in die Bausubstanz. Ursprünglich aus dem Automobilbau stammend, zeichnen sich diese Kabel auch durch ihre Kosteneffizienz aus. [14]

Ethernet-Verbindungen sind hauptsächlich in lokalen Netzwerken verbreitet und dienen der Datenübertragung zwischen Computern und Druckern. Trotz ihrer höheren Kabelstärke im Vergleich zu Flachkabeln werden sie aufgrund ihrer Leistungsfähigkeit und Zuverlässigkeit geschätzt, allerdings ist ihre Installation aufwendiger. [14]

Abschließend bieten funkbasierte Systeme eine flexible Lösung, besonders in Anlagen mit einer großen Anzahl an Sensoren und Aktoren. Diese Systeme nutzen elektromagnetische Funkwellen zur Protokollübertragung und bestehen aus Komponenten wie Funksendern und -empfängern [14]. Zu diesen Technologien zählen unter anderem Wireless Local Area Network (WLAN), Bluetooth Low Energy (BLE), ZigBee und Z-Wave, welche im folgenden Abschnitt 2.3 näher erläutert werden.

2.3 Kommunikationsstandards in der Hausautomatisierung

Innerhalb des Smart Homes definieren Kommunikationsstandards die Modalitäten der Interaktion zwischen einzelnen Geräten im intelligenten Heimnetzwerk sowie deren Kommunikation mit den Nutzern. Im Folgenden werden die am Markt weitverbreitetsten drahtlosen Kommunikationsstandards vorgestellt und im Hinblick auf ihre historische Entwicklung, Datendurchsatz, Topologie, Sicherheit und Energieverbrauch untersucht.

2.3.1 Wireless Local Area Network

Historie Der Institute of Electrical and Electronic Engineers (IEEE) 802.11-Standard, auch als WLAN bekannt, bezeichnet eine Reihe von Funknetzwerkstandards, die vom IEEE herausgegeben werden. Die erste Version dieses Standards wurde im Jahr 1997 veröffentlicht und legte die Grundlagen für die drahtlose Kommunikation in verschiedenen Frequenzbändern, darunter 2,4 GHz, 5 GHz und 6 GHz. Im Jahr 1999 wurden zwei weitere Standards innerhalb

des 802.11-Frameworks eingeführt, nämlich 802.11a und 802.11b. Letzterer, auch als Wireless Fidelity (WiFi) bekannt, entwickelte sich zu einem der weitverbreitetsten Standards für drahtlose Kommunikation. Der 802.11b-Standard deckt ein breites Anwendungsspektrum von privaten Netzwerken über industrielle Anwendungen bis hin zu öffentlichen Hotspots ab. [15, 16]

Datendurchsatz Bei der Betrachtung von WLAN-Standards ist es wichtig zu verstehen, dass die vom IEEE ausgewiesenen maximalen Übertragungsgeschwindigkeiten theoretische Werte sind, die unter optimalen Bedingungen erzielt werden können. Diese Geschwindigkeiten werden jedoch in der Praxis meist nicht erreicht. Beispielsweise wird ein WLAN, das dem IEEE 802.11n-Standard entspricht und mit einer maximalen Rate von 600 MBit/s beworben wird, im Alltag oft nur Geschwindigkeiten um die 300 MBit/s liefern. Ähnlich verhält es sich mit dem IEEE 802.11ac-Standard, der zwar Raten von bis zu 7 GBit/s vorsieht, jedoch in Wirklichkeit selten mehr als 867 MBit/s realisiert. Der Funkstandard sieht sich mit der Realität konfrontiert, dass solche Zahlen aufgrund von Einschränkungen durch Funkkanalbreiten, Übertragungsarten und Antennenzahlen sowie anderen Umgebungsbedingungen nur theoretischer Natur sind. [17]

Tabelle 2.1: WLAN-Standards im Vergleich nach [17]

WLAN-Generation	**WiFi 4**	**WiFi 5**	**WiFi 6 / 6E**
Funkstandard	IEEE 802.11n	IEEE 802.11.ac	IEEE 802.11ax
Maximale Übertragungssrate	600 MBit/s	6.936 MBit/s	9.608 MBit/s
Theoretische Übertragungsrate	300 MBit/s	867 MBit/s	1.200 MBit/s
Maximale Reichweite	100 m	50 m	50 m
Frequenzbereich	2,4 + 5 GHz	nur für 5 GHz	2,4 + 5 + 6 GHz

Die maximale Übertragungsrate, die in den Spezifikationen der WLAN-Standards genannt wird, kann somit als Idealwert bezeichnet werden. Er beruht auf der Summe aller möglichen Leistungsmerkmale, die der Standard hergeben könnte. Daher ist es sinnvoller, sich an einer theoretischen Übertragungsrate zu orientieren, die eher dem Maß entspricht, das handelsübliche Geräte erreichen können. [17]

Topologie In WLAN-Netzwerken ist die Architektur häufig um eine Stern-Topologie zentriert, die sich um ein Basic Service Set (BSS) organisiert. Hierbei nimmt der Wireless Access Point (AP) eine zentrale Position ein, da er als Vermittler zwischen dem drahtgebundenen und dem drahtlosen Netzwerk dient. Diese Funktion erinnert an die einer Bridge im IT-Kontext, die eine Netzwerkkomponente darstellt, welche zwei unterschiedliche Netzwerksegmente miteinander verbindet. Im Falle des AP besteht seine „Bridge"-Funktion darin, die Übertragungsprotokolle zu filtern und so eine Überlastung des WLANs zu verhindern, indem er nur relevante Datenpakete passieren lässt und den Netzwerkverkehr effizient steuert. Innerhalb seiner Funkzelle garantiert der AP eine bestimmte Übertragungsrate, die jedoch von allen angeschlossenen Teilnehmern geteilt wird. Faktoren wie die Positionierung des AP und Umgebungseinflüsse wie Luftfeuchtigkeit und bauliche Gegebenheiten beeinflussen die Übertragungsrate. Für eine optimale Leistung ist es ratsam, den AP so zu positionieren, dass

keine Hindernisse zwischen ihm und den WLAN-Clients bestehen. Die Identifikation einzelner WLAN-Netze erfolgt über Extended Service Set Identifier (ESSID) bzw. Service Set Identifier (SSID). [18]

Sicherheit Die Sicherheitsmaßnahmen in WLAN-Netzen haben sich stetig weiterentwickelt, um aufkommende Bedrohungen und Schwachstellen zu adressieren. Ursprüngliche Protokolle wie Wired Equivalent Privacy (WEP) waren aufgrund fundamentaler Schwachstellen im Design und der Implementierung anfällig für diverse Angriffsarten, wie zum Beispiel der Verwendung eines kurzen Initialisierungsvektors und die Vorhersagbarkeit von Schlüsselströmen. WLAN Protected Access (WPA) verbesserte die Sicherheit durch die Einführung von Temporal Key Integrity Protocol (TKIP), das dynamische Schlüssel generiert, aber immer noch von der Sicherheit der verwendeten Passwörter abhängig war. [15]

Mit WPA2 wurde ein signifikanter Fortschritt erzielt, insbesondere durch die Einführung des Advanced Encryption Standard (AES)-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)-Verfahrens, das eine stärkere Verschlüsselung und Authentifizierung bietet. Dies erschwerte zwar viele der einfachen Angriffsmethoden, aber es blieben weiterhin Anfälligkeiten, insbesondere in der Implementierung der Protokolle, die durch fortgeschrittene Angriffstechniken wie Key Reinstallation Attack (KRACK) ausgenutzt werden konnten. [15]

WPA3, das aktuellste Sicherheitsprotokoll, adressiert bekannte Schwachstellen durch die Implementierung fortgeschrittener Authentifizierungsmechanismen wie Simultaneous Authentication of Equals (SAE). Ein wesentlicher Bestandteil dieses Protokolls ist der Schutz von Management-Frames. Management-Frames sind Steuernachrichten innerhalb eines WLAN-Netzwerks, die für Aufgaben wie die Verbindungsaufnahme, -verwaltung und -trennung zwischen Geräten verantwortlich sind. Durch den Schutz dieser Frames wird das Netzwerk gegen Deauthentifizierungsangriffe abgesichert, bei denen Angreifer versuchen, Geräte gewaltsam aus dem Netzwerk zu entfernen. Trotz dieser Verbesserungen bleibt die Sicherheit in WLAN-Netzwerken eine stetige Herausforderung, die kontinuierliche Wachsamkeit und Updates erfordert, um gegen neu entstehende Bedrohungen gewappnet zu sein. [15]

Energieverbrauch Zu Beginn hat sich WLAN aufgrund seines signifikanten Energiebedarfs, der durch die ursprüngliche Konzeption für die Übertragung umfangreicher Datenmengen bedingt ist, nicht als vorherrschendes Kommunikationsnetzwerk in Smart Homes durchsetzen können. Der Einsatz von WLAN beschränkte sich auf Geräte, die direkt mit dem Stromnetz verbunden sind, da es für batteriebetriebene Geräte oder solche, die auf Energy Harvesting basieren, nicht geeignet ist. Energy Harvesting-Geräte sind innovative Komponenten, die Energie aus ihrer Umgebung sammeln, beispielsweise durch die Nutzung von Licht, Temperaturunterschieden oder Vibrationen, um ihren Betrieb zu ermöglichen. Diese Technologie ermöglicht es Geräten, autonom zu funktionieren und minimiert die Abhängigkeit von externen Energiequellen oder dem häufigen Austausch von Batterien. Obwohl WLAN-Netzwerke die Anbindung von Automatisierungsgeräten an mobile Endgeräte erlauben, ist für die Kom-

munikation mit Sensoren und Aktoren, die energieeffizientere Technologien nutzen, ein Gateway erforderlich. Die Herausforderungen für WLAN in der Hausautomatisierung liegen in der Notwendigkeit, den Energieverbrauch zu senken, um eine längere Batterielebensdauer zu erreichen, und der zunehmenden Netzwerküberlastung, die durch die gesättigten Frequenzbänder bei 2,4 GHz und 5 GHz verursacht wird. [11]

2.3.2 Bluetooth Low Energy

Historie Im Jahr 1994 begannen Ericsson und Nokia mit der Entwicklung einer Technologie für drahtlose Kurzstreckenkommunikation, die später als Bluetooth bekannt wurde, benannt nach dem Wikingerkönig Harald Gormson Blaatand. Diese Technologie zielte darauf ab, kleinere Geräte einfach zu vernetzen. 1998 bildete sich die Bluetooth Special Interest Group (SIG), zu der heute tausende Unternehmen gehören. Ericsson, Nokia, IBM, Toshiba und Intel trugen maßgeblich zur Entwicklung des Bluetooth-Standards bei, als die SIG 1999 die ersten Spezifikationen veröffentlichte. Bluetooth entwickelte sich rasch zu einem wichtigen Funkstandard für die drahtlose Kommunikation, insbesondere seit der Einführung von BLE in Version 4.0, die die Energieeffizienz erheblich verbesserte. [19, 20]

Datendurchsatz Beim Datendurchsatz von Bluetooth hängt die Übertragungsgeschwindigkeit wesentlich vom verwendeten Modulationsverfahren ab. Bei Einsatz des 8DPSK-Modulationsverfahrens, das mit Bluetooth 2.0/2.1 eingeführt wurde, ist eine maximale Übertragungsrate von 3 MBit/s möglich. [20]

Tabelle 2.2: BLE Spezifikationen nach [20, 21]

Bluetooth-Generation	**BLE 4.0 / 4.1 / 4.2**
Funkstandard	IEEE 802.15
Maximale Übertragungsrate	3 MBit/s
Theoretische Übertragungsrate	2.169,9 kBit/s
Maximale Reichweite	10 m
Frequenzbereich	2,4 GHz

Topologie BLE operiert mit spezialisierten Low-Energy-Geräten in der Stern-Topologie und ist primär für Anwendungen konzipiert, die in größeren Intervallen kleine Datenmengen bis zu 220 kBit/s übertragen. Für höhere Datenraten sind Bluetooth Classic oder Bluetooth 5 erforderlich, wobei dann die Energieeffizienzvorteile von BLE nicht genutzt werden können. Es ist zu beachten, dass trotz der theoretischen Fähigkeit des BLE-Protokolls, hohe Sendeleistungen zu erreichen, die Verwendung von Low-Energy-Chips die Datenrate begrenzt, um eine längere Batterielaufzeit zu gewährleisten. [21]

Sicherheit Die Sicherheitsmechanismen von Bluetooth-Verbindungen lassen sich in drei Hauptkategorien unterteilen, die auf unterschiedlichen Ebenen der Authentifizierung basieren. Auf der niedrigsten Stufe ist es möglich, dass Geräte einander identifizieren und Verbindungen ohne vorherige Authentifizierung etablieren. Die mittlere Sicherheitsstufe erfordert,

dass Geräte sich zwar erkennen, jedoch eine Dienste-Authentifizierung für die Herstellung einer Verbindung notwendig ist. Die höchste Sicherheitsebene verhindert, dass Geräte einander erkennen und macht eine Verbindungs-Authentifizierung für jegliche Kommunikation erforderlich. [20]

Energieverbrauch Bluetooth in seiner ursprünglichen Form ohne die BLE Spezifikation zeigt einen hohen Energieverbrauch, ähnlich dem von WLAN. Im Gegensatz dazu zeichnet sich BLE, insbesondere in Kombination mit Low-Energy-Chips, durch eine erhebliche Energieeinsparung aus. Diese Chips benötigen nur minimale Batterieleistung und können über mehrere Jahre hinweg funktionieren. Der geringere Energieverbrauch von BLE resultiert vor allem aus der Verlagerung bestimmter Funktionen vom Hauptprozessor (Host) zum Controller. Dieser Ansatz ermöglicht es dem Host, längere Zeiträume im Schlafmodus zu verbringen, während der Controller die Hintergrundkommunikation autonom abwickelt. Ein weiterer Faktor für die Energieeffizienz ist der schnelle Verbindungsaufbau, der den Gesamtstrombedarf reduziert. [21]

2.3.3 ZigBee

Historie ZigBee, entwickelt von der ZigBee Alliance, ist ein Funkstandard, der ursprünglich darauf abzielte, proprietäre Funktechniken im Nahbereich für Mess- und Steuerungszwecke zu ersetzen. Der Funkstandard beruht auf dem IEEE-802.15.4-Standard und umfasst mehrere Schichten, darunter die Funk- und Zugriffsschicht sowie Netz- und Sicherheitsschichten, ergänzt durch eine Anwendungs-Application Programming Interface (API) mit herstellerunabhängigen Profilen. Trotz seiner lizenzfreien Nutzung für Softwareentwickler und Unterstützung durch namhafte Hersteller ist die Verbreitung von ZigBee eingeschränkt geblieben, teilweise aufgrund mangelnder Interoperabilität und der Entwicklung proprietärer Funktionen durch einige Hersteller. [22, 23]

Datendurchsatz ZigBee nutzt die lizenzfreien Industrial Scientific and Medical (ISM)-Bänder für seine Operationen, wobei der 2,4 GHz-Bereich weltweit verfügbar ist. Zusätzlich gibt es regionalspezifische Frequenzen: 915 MHz in den USA und 868 MHz in Europa. Die Datenübertragungsraten variieren je nach Frequenzbereich: Die Technologie erreicht eine Datenübertragungsgeschwindigkeit von bis zu 250 kBit/s in einem Frequenzband von 2,4 GHz verteilt über zehn Kanäle, während im Frequenzbereich von 915 MHz Geschwindigkeiten von bis zu 40 kBit/s über sechs Kanäle und bei 868 MHz bis zu 20 kBit/s über einen Kanal realisiert werden können. Diese Übertragungskapazität erlaubt es, Entfernungen zwischen Zehn und 100 Metern zu überwinden. Im Bereich von 2,4 GHz nutzt die Technologie eine Kombination aus Phasenmodulation und Direct Sequence Spread Spectrum (DSSS), was die Widerstandsfähigkeit der Übertragung gegen Störungen verbessert. [22]

Sicherheit ZigBee implementiert ein dreistufiges Sicherheitskonzept, um unterschiedlichen Sicherheitsanforderungen gerecht zu werden. Die erste Ebene bietet keine Sicherheitsmaßnahmen, während die zweite Ebene grundlegende Zugangskontrollen beinhaltet. Die dritte

Tabelle 2.3: ZigBee Spezifikationen nach [22]

Kommunikationsstandard	**ZigBee**
Funkstandard	IEEE 802.15.4
Maximale Übertragungsrate	250 kBit/s
Theoretische Übertragungsrate	250 kBit/s
Maximale Reichweite	10-100 m
Frequenzbereich	2,4 GHz

und gleichzeitig höchste Sicherheitsstufe umfasst fortgeschrittene Schutzmaßnahme durch die Verwendung einer symmetrischen Verschlüsselung. Diese basiert auf dem AES mit einer Schlüssellänge von 128 Bit, um eine robuste Sicherheit in ZigBee-Netzwerken zu gewährleisten. [22]

Topologie ZigBee nutzt eine Mesh-Netzwerktechnologie, die es ermöglicht, ein Netzwerk aus Geräten aufzubauen, in dem jedes Gerät als Router fungieren kann. Diese Struktur bietet zuverlässige und redundante Kommunikationswege, selbst in anspruchsvollen Umgebungen. Mit einem Aktionsradius von bis zu 100 Metern kann ZigBee bis zu 65.000 Geräte in einem Netzwerk unterstützen. [24]

Energieverbrauch ZigBee ist in der Hausautomatisierung besonders wegen seines niedrigen Energieverbrauchs geschätzt, was es ideal für den Einsatz in batteriebetriebenen Geräten macht. Diese Effizienz in Kombination mit geringer Funkabstrahlung trägt zur Attraktivität von ZigBee in umweltbewussten und energieeffizienten Anwendungen bei. [11, 24]

2.3.4 Z-Wave

Historie Die Geschichte von Z-Wave beginnt mit der Gründung des Unternehmens Zensys Ende der 1990er Jahre durch zwei dänische Ingenieure. Ursprünglich lag der Fokus von Zensys auf der Entwicklung und dem Vertrieb eigener Smart Home Lösungen. Jedoch erkannte das Unternehmen bald das Potenzial, seine Funktechnologie anderen Firmen zu lizenzieren und die dafür notwendigen integrierten Schaltungen zu verkaufen. In den USA fand Zensys seine ersten großen Kunden und in Europa war der deutsche Schalterhersteller Merten, der nun Teil von Schneider Electric GmbH ist, der erste bedeutende Hersteller, der Z-Wave einsetzte. Ein wichtiger Meilenstein in der Entwicklung von Z-Wave war die Gründung der Z-Wave Alliance, einer Industrieallianz, die Hersteller von Z-Wave-kompatiblen Produkten zusammenbringt. [11]

Datendurchsatz Z-Wave ist eine bidirektionale, drahtlose Kommunikationstechnologie, die sich durch die Rückbestätigung von Nachrichten vom Empfänger zum Sender auszeichnet, wodurch die Übertragungszuverlässigkeit gesteigert wird. Diese Technik nutzt den Frequenzbereich um 868 MHz, was ihr im Vergleich zu herkömmlichen 2,4-GHz-Systemen eine um 30 bis 50 Prozent höhere Reichweite verleiht. Die Übertragungsgeschwindigkeit liegt bei 90 kBit/s. [25]

Tabelle 2.4: Z-Wave Spezifikationen nach [26, 27]

Kommunikationsstandard	**Z-Wave**
Funkstandard	kein Standard
Maximale Übertragungsrate	90 kBit/s
Theoretische Übertragungsrate	90 kBit/s
Maximale Reichweite	30m
Frequenzbereich	868 MHz

Sicherheit Z-Wave gewährleistet eine sichere und zuverlässige bidirektionale Kommunikation, indem es eine Kombination aus Empfangsbestätigungen und einem Mesh-Netzwerk einsetzt, was zur Effizienz des Systems beiträgt. Mit der neuesten Generation, Z-Wave Gen7, erreicht das System einen höheren Sicherheitsstandard, indem es die AES 128 implementiert, was die Datensicherheit erheblich verbessert. [11, 26]

Topologie Z-Wave besitzt ähnlich wie ZigBee eine Mesh-Netzwerk-Fähigkeit, wobei jedes Gerät im Netzwerk Daten weiterleiten kann, was zu einer dynamischen und selbst konfigurierenden Netzwerkstruktur führt. Ein einzelnes Z-Wave-Netz unterstützt bis zu 232 Geräte, für größere Anwendungen können mehrere Netze über Universal Plug and Play (UPnP)- und TCP/IP-basierte Gateways verbunden werden. [25]

Energieverbrauch Z-Wave zeichnet sich als eine auf Wohngebäude zugeschnittene drahtlose Kommunikationstechnik aus, die sich durch die Verwendung eines speziell für den Industrie- und Medizinbereich reservierten 868-MHz-Frequenzbands hervorhebt [11]. Diese Frequenzwahl ist strategisch, um gängige Überlastungen, die in häufiger genutzten Frequenzbereichen auftreten, zu vermeiden. Durch die geringe Übertragungsgeschwindigkeit im Vergleich zu anderen Kommunikationsstandards, kann ein niedriger Energieverbrauch erzielt werden.

2.3.5 Vergleich

Tabelle 2.5 präsentiert einen vergleichenden Überblick über die vorgestellten Kommunikationsprotokolle im Bereich Smart Home. Diese Übersicht enthält die untersuchten Attribute zu den entsprechenden Kommunikationsstandards.

Tabelle 2.5: Vergleich der Kommunikationsstandards in Smart Home Systemen

Systemart	**WLAN/WiFi**	**BLE**	**ZigBee**	**Z-Wave**
Funkstandard	IEEE 802.11	IEEE 802.15.4	IEEE 802.15.4	kein Standard
Sicherheit	Hoch	Hoch	Hoch	Hoch
Datendurchsatz	300-1200 MBit/s	1-3 MBit/s	250 kBit/s	90 kBit/s
Energieverbrauch	Hoch	Niedrig	Niedrig	Niedrig
Frequenzbereich	2,4 + 5 + 6 GHz	2,4 GHz	2,4 GHz	868 MHz
Topologie	Stern	Stern	Mesh	Mesh

2.4 Zentrales und dezentrales Smart Home

Nachdem die grundlegenden Konzepte und Technologien hinter Smart Homes beleuchtet wurden, werden nun die zentralen Architekturen betrachtet, die die Funktionsweise und das Management dieser intelligenten Systeme prägen: zentrale und dezentrale Smart Homes. Diese Unterkapitelkapitel beleuchten, wie die jeweilige Architektur die Interaktion zwischen Geräten, die Datenverarbeitung und die Systemeffizienz beeinflusst und legen dar, welche Vor- und Nachteile sich daraus für Nutzer und Netzwerkmanagement ergeben.

2.4.1 Zentrales Smart Home

Zentrale Smart Home-Systeme sind dadurch charakterisiert, dass die Integration und Steuerung von Sensoren und Aktoren durch eine zentrale Einheit ermöglicht wird. In solchen Systemen sind die einzelnen Sensoren und Aktoren über einen zentralen Controller miteinander verbunden, was die Grundlage für ein effizientes und koordiniertes Netzwerk bildet. Diese Verbindungen können entweder über Funktechnologie oder Kabeltechnologie realisiert werden, wobei jede Komponente direkt an den zentralen Controller angeschlossen ist. [14]

Abbildung 2.1 zeigt den zentralen Controller als das Herzstück des Systems, indem er die eingehenden Daten von den Sensoren empfängt, verarbeitet und entsprechende Befehle an die Aktoren weiterleitet. Diese zentrale Steuerungseinheit ermöglicht eine hohe Benutzerfreundlichkeit, da sie die Verwaltung und Kontrolle aller angeschlossenen Geräte von einem einzigen Punkt aus erlaubt. Dieses Konzept vereinfacht die Handhabung des Systems erheblich, da Nutzer nicht mehrere separate Geräte oder Anwendungen bedienen müssen, sondern eine zentrale Schnittstelle für alle ihre Smart Home-Anforderungen haben. [28]

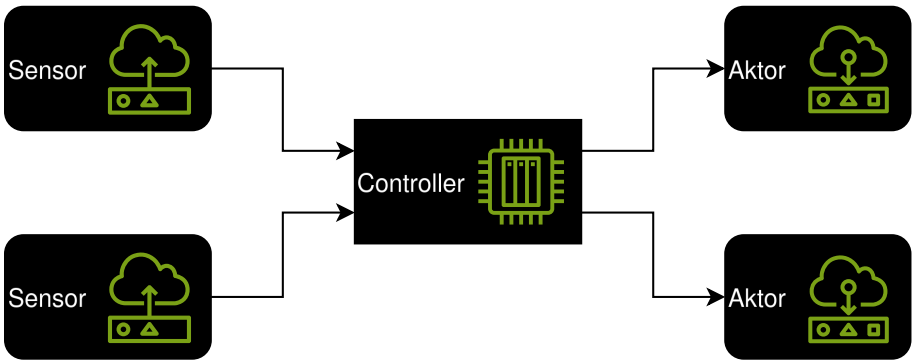

Abbildung 2.1: Funktionsweise eines zentralen Smart Homes in Anlehnung an [28]

Die im zentralen Smart Home gewonnene Zentralisierung birgt auch gewisse Risiken, was bedeutet, dass der zentrale Controller einen sogenannten Single Point of Failure (SPoF) darstellt. Das bedeutet, dass im Falle eines Ausfalls oder einer Fehlfunktion des Controllers die gesamte Kommunikation innerhalb des Netzwerks unterbrochen wird. Dies kann dazu führen, dass sämtliche verbundenen Geräte und Systeme nicht mehr funktionsfähig sind und das gesamte Smart Home-System vorübergehend außer Betrieb gesetzt wird. [14]

Ein zentrales Smart Home-System ist für viele Benutzer attraktiv, da es eine einfache Bedienung bietet, die kein umfassendes technisches Wissen voraussetzt. Diese Zugänglichkeit macht es zu einer bevorzugten Wahl für Privatanwender. Zudem sind die Kosten für solche Systeme oft geringer, und es gibt vertrauenswürdige Ansprechpartner bei Problemen oder Fragen, da große und namhafte Unternehmen wie Robert Bosch Smart Home GmbH, Telekom Deutschland GmbH oder RWE AG oft hinter diesen Produkten stehen. [28]

Zu den Nachteilen eines zentralen Smart Homes zählen die Abhängigkeit von herstellerspezifischer Software, die die Kompatibilität mit Geräten anderer Hersteller einschränken kann. Das kann dazu führen, dass Nutzer an die Produktpalette eines bestimmten Herstellers gebunden sind, was sowohl die Auswahl als auch die Erweiterbarkeit des Systems begrenzt. Die Möglichkeit, das System zu erweitern und anzupassen hängt stark vom Angebot des Herstellers ab, was in einer weniger flexiblen und möglicherweise teureren Langzeitnutzung resultieren kann. [28]

2.4.2 Dezentrales Smart Home

Ein dezentrales Smart Home System zeichnet sich durch das Fehlen eines zentralen Controllers aus. In einem solchen System sind die einzelnen Geräte entweder durch Kabelverbindungen oder drahtlose Kommunikation miteinander verbunden und führen ihre Kommunikation direkt untereinander durch. Diese Art der Vernetzung ermöglicht einen flexibleren und potenziell robusteren Ansatz im Vergleich zu Systemen mit einer zentralen Steuerungseinheit. [14, 28]

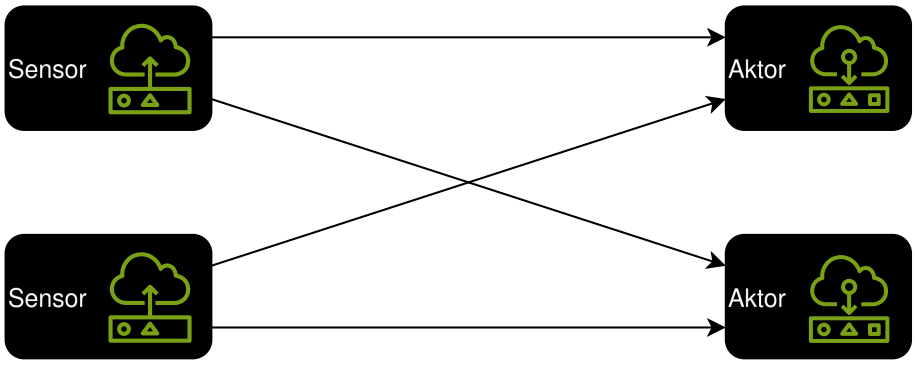

Abbildung 2.2: Funktionsweise eines dezentralen Smart Homes in Anlehnung an [28]

Abbildung 2.2 bildet die Interaktion zwischen den verschiedenen Geräten in einem dezentralen Smart Home System basierend auf vordefinierten Parametern ab. Diese Parameter werden durch spezialisierte Software festgelegt und steuern, wie und wann Geräte Informationen austauschen und aufeinander reagieren. [14]

Ein dezentrales Smart Home bietet den Vorteil, dass die Technologie direkt in den einzelnen Geräten integriert ist, was eine zentrale Steuereinheit überflüssig macht. Diese Struktur erlaubt eine hohe Flexibilität und Erweiterbarkeit des Systems, da es nicht auf herstellerspezifische Funktionen beschränkt ist. [28]

Allerdings sind dezentrale Systeme in der Regel kostenintensiver und erfordern ein höheres Maß an technischem Verständnis oder professioneller Beratung für die Installation und Wartung. Diese Art von System kann besonders für Nutzer attraktiv sein, die individuelle Lösungen bevorzugen und bereit sind, in die Technologie und das erforderliche Wissen zu investieren. [28]

2.4.3 Vergleich beider Systeme

Tabelle 2.6 präsentiert einen vergleichenden Überblick über die Vor- und Nachteile von zentralen und dezentralen Smart Home Systemen.

Tabelle 2.6: Vor- und Nachteile von zentralen und dezentralen Smart Home Systemen

Systemart	Vorteile	Nachteile
Zentrales Smart Home	Benutzerfreundlich Niedriger Preis Für Privatpersonen Direkte Ansprechpartner	Proprietäre Software Vendor Lock-in bei Ausbau Controller ist SPoF
Dezentrales Smart Home	Kein Controller als SPoF Technik integriert in Geräte Beliebig erweiterbar	Kostenintensiv Technikaffinität erforderlich

2.5 Open Source Lösungen zur Softwaresteuerung in der Hausautomatisierung

Unter dem Begriff „Lösungen zur Softwaresteuerung in der Hausautomatisierung“ versteht man Systeme, die es ermöglichen, verschiedene Aspekte des häuslichen Umfelds – von der Beleuchtung über die Heizung bis hin zur Sicherheitstechnik – zentral und oft auch ferngesteuert zu verwalten und zu kontrollieren. Diese Softwarelösungen fungieren als Schnittstelle zwischen dem Benutzer und den technischen Komponenten des Hauses, wobei sie jedoch nicht die Hardwareelemente selbst, sondern vielmehr deren Koordination und Steuerung umfassen.

Auf dem Markt existieren zahlreiche Ansätze zur Softwaresteuerung in der Hausautomatisierung, die sich grob in zwei Kategorien einteilen lassen: proprietäre und Open-Source-Lösungen. Proprietäre Systeme werden von Unternehmen entwickelt und vertrieben; sie sind oft durch Urheberrechte geschützt und bieten eine kommerzielle, oft benutzerfreundliche Paketlösung. Im Gegensatz dazu stehen Open-Source-Lösungen, die durch ihre frei zugänglichen und modifizierbaren Quellcodes eine hohe Anpassungsfähigkeit und eine starke Gemeinschaft von Entwicklern und Anwendern aufweisen.

2.5.1 openHAB

openHAB, ein Projekt mit dem Titel Open Home Automation Bus, wurde 2010 von dem Java-Entwickler Kai Kreuzer initiiert [29]. Als eine Open-Source-Softwarelösung für Smart Homes, die in Java implementiert und auf dem Eclipse SmartHome-Framework aufbaut, zeichnet sich openHAB durch seine Herstellerneutralität sowie seine Unabhängigkeit von spezifischer Hardware und Protokollen aus [30].

Die Flexibilität von openHAB zeigt sich in seiner Fähigkeit, auf jedem Gerät eingesetzt zu werden, das eine Java Virtual Machine unterstützt. Dieses Merkmal unterstreicht Kreuzers Ziel, mit openHAB eine robuste, stabile und offene Softwarelösung für die Heimautomatisierung zu entwickeln, was in Abbildung 2.3 durch eine Darstellung der Benutzeroberfläche der Softwaresteuerung veranschaulicht wird. [29]

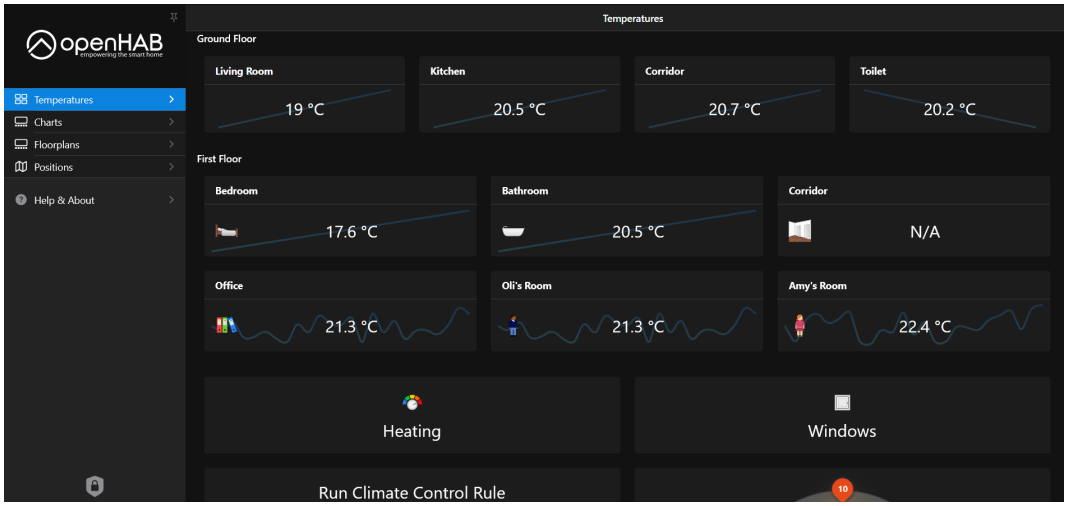

Abbildung 2.3: openHAB Benutzeroberfläche [31]

Zentral für das Verständnis von openHAB sind die sogenannten „Things“, die als Entitäten innerhalb des Systems fungieren und die Möglichkeit bieten, physische Geräte oder Dienste in das System zu integrieren. Diese „Things“ können mehrere Funktionen bereitstellen. Beispielsweise kann ein Multi-Sensor im Z-Wave-System sowohl als Bewegungsmelder als auch zur Messung der Raumtemperatur dienen. Interessant ist, dass „Things“ nicht ausschließlich physische Objekte sein müssen, sondern auch Webdienste oder andere informations- und funktionsreiche Quellen repräsentieren können. [30]

Die Fähigkeiten der Things werden durch sogenannte „Channels“ offenbart. „Channels“ sind Schnittstellen, durch die die Fähigkeiten der Things zugänglich gemacht werden. Hierbei ist es wichtig zu verstehen, dass die Nutzung bestimmter Fähigkeiten, die ein „Channel“ bietet, von der individuellen Konfiguration des Systems abhängt. Bei der Konfiguration eines openHAB-Systems ist es nicht notwendig, jede von einem „Thing“ angebotene Fähigkeit zu verwenden. Welche „Channels“ für ein „Thing“ verfügbar sind, kann durch die Dokumentation des entsprechenden „Bindings“ eingesehen werden. [30]

„Bindings“ sind als Softwareadapter zu verstehen, die es ermöglichen, „Things“ in das Smart Home System einzubinden. Sie fungieren als Add-ons, die eine Verbindung zwischen physischen Geräten und den „Items“ herstellen und abstrahieren die spezifischen Kommunikationsanforderungen des Geräts, sodass es vom Framework allgemeiner behandelt werden kann. [30]

Die „Items“ in openHAB repräsentieren die nutzbaren Fähigkeiten innerhalb von Anwendungen, sei es in Benutzeroberflächen oder in der Automatisierungslogik. Sie verfügen über einen Zustand (State) und können Befehle empfangen. [30]

Eine entscheidende Komponente im openHAB-System sind die „Links“, die als Verbindungsstücke zwischen „Things“ und „Items“ dienen. Ein „Link“ stellt eine Assoziation zwischen genau einem „Channel“ und einem „Item“ dar. Wenn ein „Channel“ mit einem „Item“ verknüpft ist, wird er als „aktiviert“ betrachtet, was bedeutet, dass die durch das „Item“ repräsentierte Fähigkeit über diesen „Channel“ zugänglich ist. Es ist möglich, dass „Channels“ mit mehreren „Items“ verknüpft werden und „Items“ an mehrere „Channels“ angebunden sein können. [30]

2.5.2 ioBroker

ioBroker ist ein modulares System, wobei jedes Modul innerhalb von ioBroker eine spezifische Aufgabe erfüllt. Um eine Übersicht über diese Vielzahl von Modulen zu bewahren, verfügt ioBroker über einen zentralen Koordinator, der alle Module überwacht. Dieser Koordinator, bekannt als der „js-controller“, arbeitet im Hintergrund und ist verantwortlich für die zentrale Datenspeicherung sowie das Management und die Kommunikation zwischen allen Modulen. Die einzelnen Module werden als Adapter bezeichnet und vom Benutzer nur bei Bedarf installiert. Das webbasierte Verwaltungsinterface, bekannt als Admin-Adapter oder kurz „Admin“, ist selbst ein Adapter und dient als Management-Schnittstelle eines ioBroker-Systems. Der Admin wird normalerweise über die Adresse `http://localhost:8081` aufgerufen. [32]

Wenn ein neuer Adapter mit dem Admin installiert wird, werden zunächst die Adapterdateien aus dem Internet geladen und in den Serverspeicher geschrieben. Soll ein Adapter gestartet werden, wird zuerst eine Instanz des Adapters erstellt. Jede Adapterinstanz kann individuell konfiguriert und über den Admin unabhängig gestartet und gestoppt werden. Daher läuft jede Instanz in ihrem eigenen Prozess, der im Hintergrund mit dem ioBroker js-controller kommuniziert. [32]

In einem Multihost-System mit mehreren ioBroker-Servern können Instanzen von Adaptern auch auf verschiedene Server verteilt werden. Dies ermöglicht es, die Last zu verteilen oder zusätzliche Hardware direkt vor Ort anzuschließen. (Input/Output (IO)-Ports, Universal Serial Bus (USB), etc.) [32]

Die Kommunikation zwischen den Adaptern, dem js-controller, Datenbanken und Web-Frontends erfolgt über mehrere TCP/IP-Verbindungen. Je nach gewählter Einstellung werden Daten entweder im Klartext oder verschlüsselt ausgetauscht. [32]

ioBroker und die Adapter sind hauptsächlich in der Programmiersprache JavaScript geschrieben, welche zum Ausführen eine entsprechende Laufzeitumgebung benötigt. Daher setzt ioBroker auf Node.js, eine Laufzeitumgebung, die für eine Vielzahl von Softwareplattformen wie Linux, Windows und macOS verfügbar ist. [32]

Zur Installation von ioBroker und den Adaptern wird der Node Package Manager benötigt, welcher das Suchen, Installieren, Entfernen, Kompilieren und Aktualisieren von Modulen und deren Abhängigkeiten ermöglicht. Ohne Node.js funktioniert ioBroker nicht. Eine manuelle Installation von Node.js ist dabei allerdings nicht notwendig, da diese direkt durch den ioBroker-Installer erfolgt. [32]

Diese Prozessvereinfachung spiegelt sich auch in der Benutzerfreundlichkeit der Software wider, wie in Abbildung 2.4 dargestellt, die eine Benutzeroberfläche der Softwaresteuerung zeigt.

Abbildung 2.4: ioBroker Benutzeroberfläche [33]

2.5.3 Home Assistant

Die Funktionsweise von Home Assistant basiert auf einer strukturierten Konfiguration mittels spezifischer Dateien. Eine zentrale Rolle spielt dabei die Datei „configuration.yaml“, die sich standardmäßig im Verzeichnis `~/.homeassistant/` befindet. Diese Datei ist das Herzstück

der Konfiguration, in der grundlegende Einstellungen vorgenommen werden, wie etwa die Definition des geografischen Standorts. Zudem werden in dieser Datei auch die verschiedenen Smart Home-Geräte und Web-Services, die als „Components“ bezeichnet werden, integriert. [34]

Eine umfangreiche Liste der kompatiblen Components, welche über 900 verschiedene Geräte und Dienste umfasst, ist auf der Webseite `https://home-assistant.io/components/` verfügbar. Diese Webseite dient als zentrale Informationsquelle für die Nutzer, um die jeweils benötigten Einträge für die „configuration.yaml“-Datei zu finden und so gewünschte Geräte oder Services in das eigene Smart Home System zu integrieren. [35]

Ein weiteres entscheidendes Element von Home Assistant ist die Datei „automations.yaml“, in der automatisierte Prozesse zwischen den einzelnen Components definiert werden. Jede Automatisierung setzt sich aus drei Hauptkomponenten zusammen: Trigger, Condition und Action. Der Trigger beschreibt das Ereignis, das den Automatisierungsprozess initiiert. Conditions, die optional sind, legen fest, unter welchen spezifischen Bedingungen eine Automatisierung durchgeführt wird. Letztendlich wird die Aktion ausgeführt, sobald der Auslöser aktiviert ist und alle definierten Bedingungen erfüllt sind. [36]

Dieses Prinzip der Automatisierung verdeutlicht die Flexibilität und Benutzerfreundlichkeit von Home Assistant, was durch Abbildung 2.5 unterstrichen wird, die einen Einblick in die Benutzeroberfläche der Softwaresteuerung gibt.

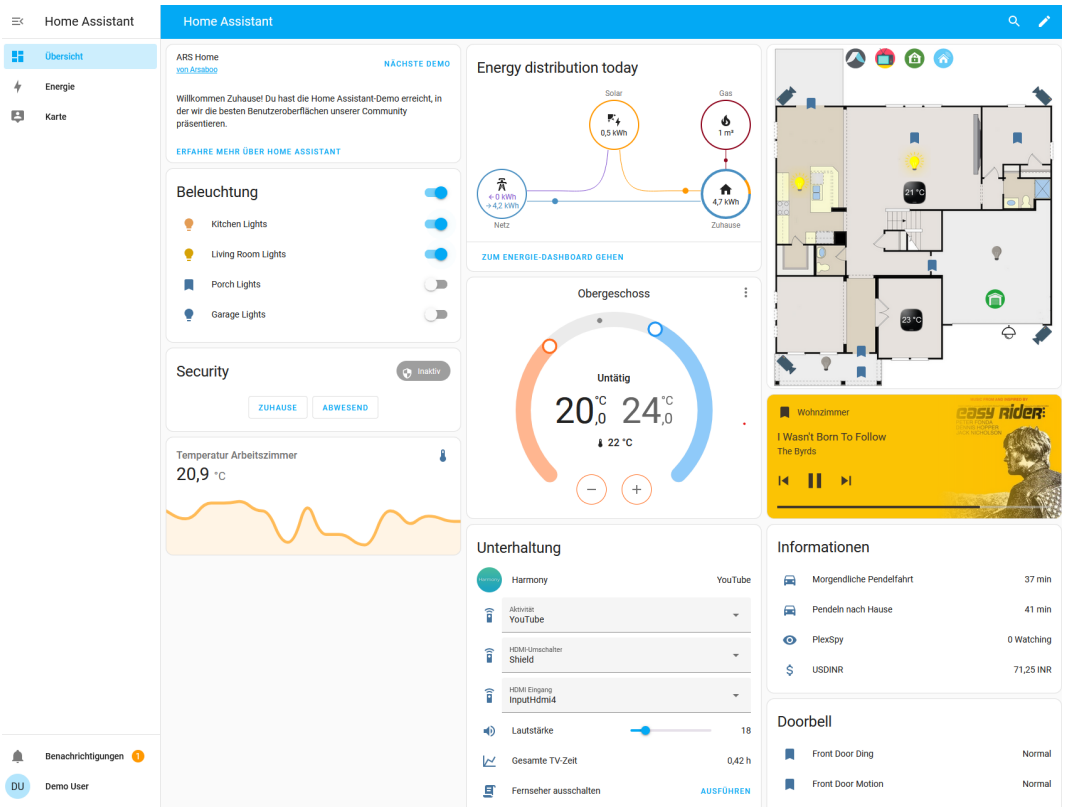

Abbildung 2.5: Home Assistant Benutzeroberfläche [37]

2.5.4 Kommerzielle Lösungen

Gegenstücke zu Open-Source-Lösungen für Smart Home-Systeme sind kommerzielle oder proprietäre Plattformen, die oft als Teil eines geschlossenen Ökosystems von einem Unternehmen angeboten werden. Diese Systeme bieten häufig eine benutzerfreundliche Oberfläche, Integrationssupport für eine breite Palette von Geräten und gegebenenfalls Abonnements für erweiterte Funktionen oder Services.

Google Nest Ursprünglich als Nest Labs bekannt, bietet Google Nest eine Reihe von Smart Home-Produkten, die sich auf die Verbesserung der Heimsicherheit, den Komfort und die Energieeffizienz konzentrieren. Die Plattform erlaubt die Steuerung über die Google Home App und ist eng mit anderen Google-Diensten integriert. [38]

Amazon Echo Amazon bieten in ihrem Smart Speaker Amazon Alexa eine weit verbreitete cloudbasierte Sprachassistentin an, die sich in zahlreiche Smart Home-Geräte integrieren lässt. Über die Alexa-App können Nutzer ihre Geräte steuern und Automatisierungen einrichten. Alexa ist besonders bekannt für ihre Fähigkeiten im Bereich der Sprachsteuerung. [39]

Apple HomeKit Apples Smart Home-Plattform ermöglicht die Steuerung von kompatiblen Geräten über iOS-Geräte wie iPhones und iPads oder per Sprachbefehl über den eigenen Sprachassistenten Siri. HomeKit legt einen starken Fokus auf Sicherheit und Datenschutz und unterstützt die Erstellung von Szenen und Automatisierungen. [40]

Samsung SmartThings SmartThings ist eine vielseitige Smart Home-Plattform, die eine breite Palette von Geräten unterstützt und Nutzern ermöglicht, diese über eine einzige App zu verwalten. Samsung legt Wert auf die Integration verschiedener Marken und Gerätetypen, um ein umfassendes Smart Home-Erlebnis zu bieten. [41]

Philips Hue Bekannt für ihre intelligente Beleuchtung, bietet Philips Hue auch eine Reihe von Schaltern und Sensoren an, die über die Hue Bridge miteinander vernetzt werden. Die Plattform ermöglicht umfangreiche Automatisierungsmöglichkeiten und Integrationen mit anderen Smart Home-Systemen. [42]

Bosch Smart Home Das Bosch Smart Home-System bietet eine Vielzahl von Produkten und Lösungen für die Heimautomatisierung, die auf Sicherheit, Komfort und Energieeffizienz abzielen. Bosch legt einen starken Fokus auf die Interoperabilität seiner Geräte und die Sicherheit der Nutzerdaten. [43]

Diese kommerziellen Plattformen unterscheiden sich von Open-Source-Lösungen durch ihre Geschäftsmodelle, die Integration proprietärer Technologien und oft durch eine stärkere Betonung auf Benutzerfreundlichkeit und Kundensupport. Während Open-Source-Plattformen mehr Flexibilität und Anpassungsfähigkeit bieten können, ziehen viele Nutzer die Einfachheit und den Komfort kommerzieller Lösungen vor.

2.6 Internet of Things Forensik

In diesem Kapitel erfolgt eine Darstellung des aktuellen Forschungsstandes im Bereich der IoT-Forensik. Anschließend wird eine Aufzählung gegenwärtiger Herausforderungen vorgenommen, die das Feld derzeit konfrontiert.

2.6.1 Stand der Forschung

Das Internet der Dinge eröffnet nicht nur neue Möglichkeiten in der Vernetzung und Automatisierung unseres täglichen Lebens, sondern stellt auch eine Reihe einzigartiger und komplexer Herausforderungen für den Bereich der digitalen Forensik dar. Die rasante Zunahme vernetzter Geräte führt zu einer exponentiellen Zunahme der Datenmengen, die in Datenzentren verarbeitet werden müssen. Dies bringt neue Herausforderungen in Bezug auf Kapazität, Sicherheit und Datenanalyse mit sich. Die IoT-Forensik ist ein interdisziplinäres Feld, das Cloud-Forensik, Geräteebenen-Forensik und Netzwerk-Forensik umfasst, um eine umfassende Untersuchung und Beweissicherung in diesem komplexen Umfeld zu ermöglichen. [44]

Trotz der Vielzahl von Prozessmodellen und Rahmenwerken, die entwickelt wurden, um die Herausforderungen in der IoT-Forensik anzugehen, wurden signifikante Lücken und Einschränkungen in den bestehenden Ansätzen identifiziert. Es wird die Notwendigkeit für ein verbessertes, proaktives Modells definiert, das speziell für die Handhabung von Verbrechensszenarien im IoT-Kontext konzipiert ist. [45]

Einige innovative Ansätze, wie das Next Big Thing Prozessmodell, zielen darauf ab, die Identifizierung potenzieller Beweisquellen durch einen strukturierten 1-2-3-Zonenansatz zu erleichtern. Der 1-2-3-Zonenansatz teilt den Untersuchungsraum in drei spezifische Bereiche auf, um die systematische Erfassung und Analyse von Beweismaterial zu erleichtern: Zone 1 konzentriert sich auf persönliche Geräte wie Smartphones und Computer, die direkt vom Nutzer kontrolliert und leicht zugänglich sind. Zone 2 bezieht sich auf lokale Netzwerke und IoT-Geräte, die nicht unmittelbar unter Nutzerkontrolle stehen, aber physisch erreichbar sind. Zone 3 erstreckt sich auf externe und Cloud-basierte Ressourcen, die wichtige Daten fernab des direkten Zugriffs speichern oder verarbeiten. Trotz seines Potenzials weist dieses Modell Herausforderungen in Bezug auf die praktische Implementierung auf, da nicht immer gewährleistet werden kann, dass Ermittler direkten Zugriff auf alle relevanten Geräte oder Cloud-Server haben. Ähnlich verhält es sich mit dem Forensic-aware IoT (FAIoT)-Modell und dem Digital forensic investigation framework for IoT (DFIF-IoT), die beide darauf abzielen, die Beweiskette aufrechtzuerhalten und eine forensische Untersuchung durch Prozessparallelität zu ermöglichen. Jedoch fehlt auch bei diesen Modellen eine praktische Implementierung, was ihre Anwendbarkeit in realen forensischen Szenarien einschränkt. [45]

Die Entwicklung spezifischer Frameworks, wie das Cloud-centric framework for isolating big data as forensic evidence from IoT infrastructures (CFIBD), zeigt innovative Ansätze zur Bewältigung der Herausforderungen in der IoT-Forensik. Diese Frameworks befassen sich mit spezifischen Aspekten wie der Mobilitätsforensik und der Isolation von Beweisen in großen Datenmengen. Trotz der theoretischen Natur vieler dieser Modelle illustrieren sie die Komplexität der IoT-Forensik und die Notwendigkeit, kontinuierlich innovative Lösungen zu entwickeln. Diese Lösungen müssen sowohl die technischen Herausforderungen als auch die rechtlichen Aspekte berücksichtigen, um die Zulässigkeit von Beweisen in Gerichtsverfahren zu gewährleisten. [45]

Zusammenfassend erfordert die Bewältigung der vielfältigen Herausforderungen in der IoT-Forensik eine kontinuierliche Entwicklung von Modellen und Rahmenwerken, die nicht nur auf theoretischen Überlegungen basieren, sondern auch praktisch implementierbar und in realen forensischen Untersuchungen anwendbar sind. Die Integration von proaktiven, szenariobasierten Aktivitäten und die Sicherstellung einer forensisch fundierten Beweissicherung und -analyse sind entscheidend, um die forensische Untersuchung im IoT-Bereich effektiv zu gestalten und die Rechtsprechung in einer zunehmend vernetzten Welt zu unterstützen. [44, 45]

2.6.2 Herausforderungen

Die Forensik im Bereich des IoT konfrontiert Ermittler mit einer Vielzahl spezifischer Herausforderungen, die hauptsächlich aus der Vielfalt und Komplexität der beteiligten Systeme resultieren. Diese Herausforderungen reichen von der Heterogenität und den Sicherheitsfragen der Geräte bis hin zu den Schwierigkeiten bei der Datenerhebung und -analyse, insbesondere wenn es um proprietäre Systeme und Cloud-Dienste geht.

Die Komplexität und Vielfalt von IoT-Geräten, die unterschiedliche, oft proprietäre Dateisysteme und Formate verwenden, verlangt ein tiefgehendes Verständnis ihrer einzigartigen Merkmale und Betriebsweisen. Diese Situation wird durch die Integration von Drittanbieterdiensten für Überwachung und Sicherheit weiter erschwert. Sicherheitsfragen, insbesondere im Kontext der Hausautomation, sind ein weiteres signifikantes Problem, da viele Smart Home Systeme ohne einen starken Fokus auf Sicherheitsaspekte entwickelt wurden, was potenzielle Sicherheitslücken nach sich zieht. [46]

Die Cloud-Forensik stellt eine weitere Herausforderung dar, da die Mehrheit der IoT-Daten in der Cloud gespeichert wird und der Zugriff auf forensische Beweise oft von der Kooperationsbereitschaft der Dienstanbieter abhängt. Die Unterschiede in den Cloud-Plattformen komplizieren die Beweiserhebung zusätzlich. [44]

Die Speicherbegrenzungen von IoT-Geräten bedeuten, dass die Lebensdauer der Daten kurz ist und Beweise schnell überschrieben werden können. Das macht es schwer den Beweis zu sichern und unterstreicht die Notwendigkeit, forensische Methoden in die Entwicklung von IoT-Systemen zu integrieren, um die Verlässlichkeit digitaler Beweise sicherzustellen. [44, 46, 47]

Datenschutz und Privatsphäre bilden eine zusätzliche Barriere in der IoT-Forensik, da die umfangreichen, oft sensiblen Datenmengen, die von IoT-Geräten generiert werden, unter strenge Datenschutzbestimmungen fallen. Probleme wie unklare Datenlokalisierung, Datenkorruption und die begrenzte Speicherkapazität erschweren die Beweissicherung zusätzlich. [47, 48]

Es wird deutlich, dass spezifische Schulungsprogramme für Ersthelfer essenziell sind, um zu gewährleisten, dass Beweise nicht durch Sicherheitslücken verändert oder gelöscht werden. Der Einsatz von Cloud-Diensten verkompliziert die Herausforderungen weiter, da oft eine unzureichende Identifikationspflicht bei der Registrierung die Zuweisung von Beweisen zu spezifischen Personen erschwert. [47, 48]

Die Zuverlässigkeit und unzureichende Dokumentation sowie Wartung forensischer Werkzeuge, das Fehlen einheitlicher internationaler Standards für digitale Forensik-Tools, und die stetige Weiterentwicklung der IoT-Architektur erschweren den Einsatz dieser Werkzeuge in rechtlichen Zusammenhängen und beeinträchtigen sowohl die Forschung als auch die praktische Anwendung in diesem Bereich. [49, 50]

Zusammenfassend stellen die vielschichtigen Herausforderungen in der IoT-Forensik hohe Anforderungen. Innovative Ansätze und die Entwicklung neuer forensischer Werkzeuge und Methoden sind unerlässlich. Ebenso sind spezifische Schulungen für Ersthelfer von großer Bedeutung. Darüber hinaus ist eine engere Integration forensischer Überlegungen in die Entwicklung von IoT-Systemen erforderlich. All diese Maßnahmen sind entscheidend, um die Verlässlichkeit und Sicherheit digitaler Beweise in der sich ständig weiterentwickelnden technologischen Landschaft zu gewährleisten.

3 Bewertung der forensischen Relevanz von Smart Home Technologien

Das folgende Kapitel untersucht einen zentralen Aspekt der digitalen Forensik im Kontext des IoT: die forensische Relevanz von Smart Home Geräten. Zu Beginn wird die Methodik erläutert, die das Bewertungsframework sowie die zugrunde liegenden Kriterien umfasst. Anschließend erfolgt eine Übersicht über die Produktabdeckung von Smart Home Geräten im deutschen Markt. Der Fokus liegt hier auf den deutschen Herstellern, um die regionalspezifische Relevanz dieser Arbeit zu wahren. Abschließend werden zu jeder Smart Home Kategorie Forschungsarbeiten untersucht, die sich mit der forensischen Relevanz dieser Geräte auseinandersetzen.

3.1 Methodik

Die Bewertung der forensischen Relevanz von Smart Home Geräten erfolgt durch ein speziell entwickeltes Bewertungsframework. Dieses Framework stützt sich auf fünf präzise definierte Kriterien, die dazu dienen, die forensische Bedeutung der jeweils untersuchten Geräte exakt zu bestimmen.

3.1.1 Bewertungsframework

Das primäre Ziel des Bewertungsframeworks ist es, eine objektive und systematische Methode zur Bewertung der forensischen Relevanz von Smart Home Technologien bereitzustellen. Hierfür wird ein mehrdimensionaler Ansatz verfolgt, der unterschiedliche Aspekte der jeweiligen Technologie berücksichtigt. Dies beinhaltet die Entwicklung spezifischer Bewertungskriterien und einer Skala zur Quantifizierung dieser Kriterien, die durch die numerischen Werte von 1 bis 5 realisiert wird. Dabei entspricht der Wert 1 einer niedrigen und der Wert 5 einer hohen forensischen Wertigkeit.

Zur praktischen Anwendung dieses Schemas wird jedes Gerät anhand der definierten Kriterien evaluiert. Beispielsweise wird ein Smart Speaker der Marke „XYZ“ in folgenden Kategorien wie folgt bewertet:

- Datenzugänglichkeit: 3
- Homogenität der Daten: 2
- Informationsgehalt: 3
- Datenintegrität: 5
- Rechtskonformität: 4

Aus diesen Einzelbewertungen resultiert ein Gesamtscore von $\frac{3+2+3+5+4}{5} = 3,4$, was auf die forensische Relevanz des Geräts hinweist. Es ist zu beachten, dass die Bewertung der einzelnen Kategorien ausschließlich auf einer Literaturanalyse und der subjektiven Wahrnehmung des Autors basiert. Sollten in bestimmten Bereichen noch keine Forschungsarbeiten vorhanden sein, wird dies entsprechend mit „-“ gekennzeichnet.

Das Bewertungsschema ist so konzipiert, dass es flexibel genug ist, um neue Entwicklungen und Technologien zu integrieren. Ein regelmäßiger Review-Prozess zur Anpassung und Aktualisierung des Bewertungsschemas ist vorgesehen, um die Relevanz und Genauigkeit des Frameworks kontinuierlich zu gewährleisten.

3.1.2 Kriterien für die forensische Relevanz

In der forensischen Analyse digitaler Geräte sind verschiedene Kriterien ausschlaggebend, um die Relevanz der Daten für Untersuchungen zu bewerten. Diese Kriterien ermöglichen es, die Nützlichkeit und Verlässlichkeit der gesammelten Daten einzuschätzen und sicherzustellen, dass sie den rechtlichen Anforderungen entsprechen.

Datenzugänglichkeit Ein zentrales Kriterium ist die Zugänglichkeit der Daten. Hierbei wird bewertet, wie leicht oder schwer es ist, auf die Daten eines Geräts zuzugreifen. Faktoren wie Verschlüsselung, Netzwerksicherheit und die Notwendigkeit physischen Zugriffs spielen eine entscheidende Rolle. Wenn beispielsweise der Datenzugriff ohne spezialisierte Werkzeuge möglich ist, dann ist die forensische Wertigkeit hoch.

Homogenität der Daten Die Homogenität der Daten bezieht sich auf das Ausmaß, in dem gesammelte Daten aus verschiedenen Smart Home Geräten in Struktur, Format und Typ übereinstimmen oder vergleichbar sind. Eine hohe Homogenität erleichtert die Verarbeitung und Auswertung der Daten und erhöht somit ihre forensische Wertigkeit.

Informationsgehalt Beim Informationsgehalt der Daten geht es um die Qualität und Quantität der von einem Gerät erfassten Daten. Sind die Daten detailliert und bieten sie einen reichen Kontext, ist ihre forensische Wertigkeit hoch.

Datenintegrität Die Integrität beurteilt, wie anfällig Daten für Veränderungen oder Manipulationen sind. Sind die Daten leicht manipulierbar, verringert sich ihre forensische Wertigkeit. Eine hohe Datenintegrität gewährleistet, dass die Daten als verlässliche Beweismittel dienen können.

Rechtskonformität Die Rechtskonformität bezieht sich auf die Einhaltung gesetzlicher Vorschriften und Datenschutzbestimmungen bei der Sammlung, Übermittlung und Verarbeitung von persönlichen Daten durch diese Geräte. Dies umfasst die Beachtung von Datenschutzgesetzen, insbesondere in Bezug auf die Speicherung von Nutzerdaten in der Cloud, sowie die Berücksichtigung von Sicherheitsrisiken wie externe Angriffe und unautorisierte Zugriffe.

Wenn die Rechtskonformität bei der Verarbeitung und Analyse von Daten aus Smart Home Systemen niedrig ist, dann ist die forensische Wertigkeit dieser Daten ebenfalls niedrig. Dies liegt daran, dass die Verwendung dieser Daten in rechtlichen Verfahren angefochten werden könnte, besonders wenn sie unter Verletzung von Datenschutzgesetzen und Sicherheitsstandards gesammelt wurden.

Zusammengefasst stellen diese Kriterien sicher, dass die in der forensischen Analyse verwendeten Daten nicht nur technisch aussagekräftig, sondern auch rechtlich vertretbar sind.

3.2 Energieverwaltung

Zur Kategorie Energieverwaltung im Bereich Smart Home gehören verschiedene Geräte und Systeme, die darauf abzielen, den Energieverbrauch im Haushalt effizienter zu gestalten.

3.2.1 Hersteller deutscher Smart-Home-Lösungen für Energieverwaltung

Tabelle 3.1 führt einige der wichtigsten Geräte und deren Hersteller auf, die auf dem deutschen Markt in dieser Kategorie zu finden sind.

Tabelle 3.1: Hersteller deutscher Smart Home Lösungen für Energieverwaltung

Hersteller	Heizkörperthermostat	Raumthermostat	HEMS	Smart Plug	Photovoltaik	Photovoltaik-Steuerung	Innenbeleuchtung	Außenbeleuchtung	Lichtsteuerung	Rolladen	Rolladensteuerung
Robert Bosch Smart Home GmbH	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓
tado GmbH	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
eQ-3 AG	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓
devolo GmbH	✓	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓
DELTA DORE RADEMACHER GmbH	✓	✓	✗	✓	✗	✗	✗	✗	✓	✓	✓
AVM Computersysteme Vertriebs GmbH	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✓
Schneider Electric GmbH	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓
SMA Solar Technology AG	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗
Solarwatt GmbH	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗
Gira - Giersiepen GmbH & Co. KG	✗	✓	✓	✓	✗	✗	✗	✓	✓	✗	✓
Busch-Jaeger Elektro GmbH	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓
Alfred Schellenberg GmbH	✓	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓
Albrecht JUNG GmbH & Co. KG	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✓

Robert Bosch Smart Home GmbH Im Produktportfolio befinden sich Heizkörperthermostate, Raumthermostate, ein Heim-Energiemanagementsystem (HEMS), Smart Plugs sowie Lösungen für Licht- und Rolladensteuerung. Nicht angeboten werden Photovoltaik-Anlagen und -Steuerungen, Innen- und Außenbeleuchtung sowie Rollläden. [51–56]

tado GmbH Im Produktportfolio befinden sich Heizkörperthermostate, Raumthermostate und HEMS. Nicht angeboten werden Smart Plugs, Photovoltaik-Lösungen, Innen- und Außenbeleuchtungen, Licht- und Rollladensteuerungen. [57–59]

eQ-3 AG Im Produktportfolio befinden sich Heizkörperthermostate, Raumthermostate, HEMS, Smart Plugs, Licht- und Rollladensteuerungen. Nicht angeboten werden Photovoltaik-Anlagen und -Steuerungen sowie Innen- und Außenbeleuchtungen und Rollläden. [60–65]

devolo GmbH Im Produktportfolio befinden sich Heizkörper- und Raumthermostaten, HEMS, Smart Plugs, Photovoltaik-Steuerungen sowie Licht- und Rollladensteuerungen. Nicht angeboten werden Photovoltaik-Anlagen, Innen- und Außenbeleuchtungen sowie Rollläden. [66–71]

DELTA DORE RADEMACHER GmbH Im Produktportfolio befinden sich Heizkörperthermostaten, Raumthermostaten, Smart Plugs, Lichtsteuerungen, Rollläden und Rollladensteuerungen. Nicht angeboten werden HEMS, Photovoltaik-Lösungen sowie Innen- und Außenbeleuchtungen. [72–77]

AVM Computersysteme Vertriebs GmbH Im Produktportfolio befinden sich Heizkörperthermostate, Raumthermostate, Smart Plugs, Innenbeleuchtung, Lichtsteuerungen und Rollladensteuerungen. Nicht angeboten werden HEMS, Photovoltaik, Photovoltaik-Steuerungen, Außenbeleuchtungen sowie Rollläden. [78–83]

Schneider Electric GmbH Im Produktportfolio befinden sich Heizkörperthermostate, Raumthermostate, HEMS, Smart Plugs, Licht- und Rollladensteuerungen. Nicht angeboten werden Photovoltaik-Lösungen, Innen- und Außenbeleuchtungen sowie Rollläden. [84–89]

SMA Solar Technology AG Im Produktportfolio befinden sich HEMS, das speziell auf die von Photovoltaik-Anlagen erzeugte Energie ausgerichtet ist, sowie auf Wechselrichter und Steuerungssoftware. Es werden keine Solarpanels und keine anderen Smart Home Geräte im Bereich der Energieverwaltung angeboten. [90, 91]

Solarwatt GmbH Im Produktportfolio befinden sich Solarpanels, Solarspeicher sowie HEMS. Andere Smart Home Geräte im Energieverwaltungsbereich sind jedoch nicht im Angebot. [92–94]

Gira - Giersiepen GmbH & Co. KG Im Produktportfolio befinden sich Raumthermostate, HEMS, Smart Plugs, Außenbeleuchtungen, Licht- und Rollladensteuerungen. Nicht angeboten werden Heizkörperthermostate, Photovoltaik und deren Steuerungen, Innenbeleuchtungen und Rollläden. [95–99]

Busch-Jaeger Elektro GmbH Im Produktportfolio befinden sich Heizkörper- und Raumthermostate, HEMS sowie Licht- und Rollladensteuerungen. Zudem sind Photovoltaik-Lösungen über eine Partnerkooperation mit wibutler erhältlich. Nicht angeboten werden Smart Plugs, Innen- und Außenbeleuchtungen und Rollläden. [100–105]

Alfred Schellenberg GmbH Im Produktportfolio befinden sich Heizkörperthermostate, Smart Plugs, Lichtsteuerungen, Rollläden und Rollladensteuerungen. Für Photovoltaik-Anlagen greift das Unternehmen auf Produkte der Marke QCELLS zurück. Raumthermostate, HEMS sowie Innen- und Außenbeleuchtungen sind nicht im Angebot. [106–111]

Albrecht JUNG GmbH & Co. KG Im Produktportfolio befinden sich Smart Plugs sowie Licht- und Rollladensteuerungen. Nicht angeboten werden Heizkörperthermostate, HEMS, Photovoltaik-Lösungen sowie Innen- und Außenbeleuchtungen und Rollläden. [112–115]

3.2.2 Forensische Relevanz von Energieverwaltungssystemen

In dieser Forschungsarbeit konnten forensische Analysen für drei der in Unterabschnitt 3.2.1 aufgeführten Geräte identifiziert werden, welche in dem definierten Zeitraum von 2019 bis 2023 untersucht wurden. Es ist anzumerken, dass die betrachteten Produkte nicht von deutschen Unternehmen stammen. Konkret umfassen die Forschungsarbeiten einerseits das Google Nest Thermostat und die Kasa Smart Light Bulb, andererseits verschiedene Smart Plugs, nämlich den Plug Edimax SP-2101W, D-Link DSP-W115, den TP-Link HS100, den Telldus TZWP-102 und den Amazon HD34Bx.

Smartes Raumthermostat - Google Nest Thermostat Smarte Raumthermostate, wie das Google Nest, haben die Fähigkeit, umfangreiche Nutzungsstatistiken und Umgebungsdaten zu erfassen und zu speichern. Diese Daten werden häufig an Cloud-Dienste, darunter die Nest Cloud, übertragen, was ihre Bedeutung für forensische Untersuchungen unterstreicht. [116]

Die Sicherheit der Daten wird durch Verschlüsselungsmethoden wie AES-128 während der Netzwerkkommunikation sichergestellt. Der Zugang zu detaillierten Geräteinformationen setzt außerdem die Verwendung von Benutzeranmeldeinformationen voraus. [117]

In Bezug auf die Homogenität der Daten bleibt in den vorliegenden forensischen Arbeiten ein Mangel an spezifischen Angaben bestehen. Die intelligenten Thermostate erfassen eine Vielzahl von Daten, darunter Nutzungsstatistiken, Systemprotokolle, Nutzereinstellungen, Nutzungsverhalten und den Wohnort des Nutzers. Darüber hinaus enthalten die gesammelten Daten Informationen über Heizmuster und die Heiztechnologie des Hauses, welche durch

den Zugriff auf Benutzerdaten erschlossen werden können. Statische Informationen wie Seriennummer, MAC-Adresse und Softwareversion sind ebenfalls Teil der gespeicherten Daten und spielen eine wichtige Rolle bei der Identifizierung und Analyse des Geräts. [116, 117]

Eine identifizierte Schwachstelle im Bootprozess der Thermostate birgt jedoch potenziell das Risiko einer Firmware-Manipulation, was die Datenintegrität gefährden könnte. Obwohl Firmware-Updates signiert werden, bestehen zudem Mängel in der Hardware-Sicherheitsinfrastruktur, die forensische Untersuchungen erschweren könnten. [116]

Die Sammlung und Übertragung persönlicher Daten durch diese Geräte wirft in der Forschungsliteratur Datenschutzbedenken auf. Sicherheitsrisiken wie externe Angriffe und unautorisierte Zugriffe stellen eine Herausforderung für die Einhaltung rechtlicher Vorschriften in forensischen Kontexten dar [116]. Die Speicherung von Nutzerdaten in der Cloud erfordert besondere Aufmerksamkeit im Hinblick auf Datenschutzgesetze. Zudem unterstreicht die Nutzung von privat gesammelten Heimnutzungsdaten die Notwendigkeit einer sorgfältigen Bewertung der Rechtskonformität in solchen forensischen Untersuchungen [117].

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.2 die forensische Relevanz vom Google Nest Raumthermostat anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 3,5 von 5 möglichen Bewertungspunkten.

Tabelle 3.2: Forensische Relevanz vom Google Nest Raumthermostat

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	3
Homogenität der Daten	-
Informationsgehalt	5
Datenintegrität	3
Rechtskonformität	3

Smart Plug - Verschiedene Geräte Ling et al. wiesen nach, dass Angreifer den Netzwerkverkehr von Smart Plugs erfassen und deren Kommunikationsprotokolle entschlüsseln könnten. Der Grund hierfür ist die Verwendung einfacher, unverschlüsselter Kommunikationsprotokolle, die den Datenverkehr leicht abfangbar und analysierbar machen. Diese Sicherheitslücke könnte es potenziellen Angreifern ermöglichen, sensible Informationen zu erlangen oder Manipulationen durchzuführen. [118]

Eine herausfordernde Problematik in diesem Bereich ist die Variation in Datenstruktur und -typen zwischen verschiedenen Modellen von Smart Plugs. Diese Unterschiede sind signifikant und beinhalten diverse Protokolle sowie Formate, was die Schaffung einer einheitlichen Datenbasis erschwert, da die Konsistenz und Vergleichbarkeit der Daten über unterschiedliche Modelle hinweg nicht gewährleistet ist. Somit stellt die Heterogenität der Datenstrukturen und -typen ein wesentliches Hindernis für die Homogenität der von Smart Plugs generierten Daten dar. [119]

Smart Plugs sind in der Lage, detaillierte Aktivitätsdaten zu erfassen, einschließlich der Zeiten, zu denen Geräte ein- und ausgeschaltet werden [119]. Neben Aktivitätsdaten enthalten Smart Plugs auch spezifische Geräteinformationen, darunter Modell, MAC-Adresse, IP-Adresse und Firmware-Version des angeschlossenen Geräts, sowie Daten über dessen Status und Energieverbrauch [118].

In Bezug auf die Datenintegrität von Smart Plugs spielt die Anfälligkeit für Netzwerkangriffe eine zentrale Rolle. Die Integrität der übertragenen Daten kann signifikant beeinträchtigt werden, wenn Angreifer in der Lage sind, in die Netzwerkkommunikation einzudringen [119]. Ein wesentlicher Faktor, der diese Schwachstellen bedingt, sind die oft verwendeten einfachen Kodierungs- und Authentifizierungsverfahren, welche die Datenintegrität vulnerabel gegenüber verschiedenartigen Angriffen machen, da sie nicht ausreichend robust gegenüber fortgeschrittenen Infiltrationsmethoden konzipiert sind [118].

Abschließend lässt sich feststellen, dass keine spezifischen Informationen gefunden wurden, die die Rechtskonformität im forensischen Kontext von Smart Plugs belegen.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.3 die forensische Relevanz von diversen Smart Plugs anhand der definierten Bewertungskriterien bewertet und erhalten einen Durchschnittsscore von 3,25 von 5 möglichen Bewertungspunkten.

Tabelle 3.3: Forensische Relevanz vom Plug Edimax SP-2101W, D-Link DSP-W115, den TP-Link HS100, Telldus TZWP-102 und Amazon HD34Bx Smart Plug

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	4
Homogenität der Daten	2
Informationsgehalt	5
Datenintegrität	2
Rechtskonformität	-

Innenbleuchtung - Kasa Smart Light Bulb Bei der forensischen Analyse der Kasa Smart Light Bulb ergaben sich Einblicke in die Datenstruktur und -verfügbarkeit, die für die Untersuchung von Bedeutung sind. Durch die Analyse der zugehörigen mobilen App konnte eine Datenbankdatei namens „iot.db“ identifiziert werden, die in fünf Tabellen organisiert ist: accounts, devices, locations, scenes und device groups [120]. Diese Strukturierung deutet auf eine systematische Erfassung und Organisation der Daten hin, was auf eine Homogenität der Daten schließen lässt. Die Datenbank umfasst eine Vielzahl von Informationen, darunter Geräte-IDs, Zeitstempel für Erstellung und Aktualisierung, Nutzerkontaktdaten, Gerätestatusinformationen, sowie detaillierte Standortdaten, was den hohen Informationsgehalt der Daten unterstreicht [120].

Ein besonderer Aspekt der Analyse ist die begrenzte Verfügbarkeit von Daten, wobei auffällt, dass ausschließlich die Location-Tabelle tatsächliche Daten vorweist. Diese speichert geografische Koordinaten im base64-Format, deren Dekodierung präzise Standortdaten offenbart,

was die Datenintegrität in diesem Bereich unterstreicht. Obwohl in den bereitgestellten Informationen keine explizite Erwähnung der Rechtskonformität erfolgt, heben die sensiblen Informationen, wie geografische Standorte, die Bedeutung des Datenschutzes hervor. Es wird implizit darauf hingewiesen, dass bei der Handhabung und Analyse solcher Daten Vorsicht geboten ist, um die Privatsphäre der Nutzer zu wahren und gesetzliche Bestimmungen zu erfüllen. [120]

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.4 die forensische Relevanz vom von der Kasa Smart Light Bulb anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 3,2 von 5 möglichen Bewertungspunkten.

Tabelle 3.4: Forensische Relevanz von Kasa Smart Light Bulb

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	3
Homogenität der Daten	4
Informationsgehalt	4
Datenintegrität	3
Rechtskonformität	2

Für die in Tabelle 3.1 aufgeführten Technologien Heizkörperthermostat, HEMS, Photovoltaik, Photovoltaik-Steuerung, Außenbeleuchtung, Rollladen und Rollladensteuerung konnten keine forensischen Arbeiten identifiziert werden.

3.3 Klima- und Umweltkontrolle

Zur Kategorie Klima- und Umweltkontrolle im Bereich Smart Home gehören verschiedene Geräte und Systeme, die darauf abzielen, das Raumklima und die Luftqualität im Haushalt zu überwachen und zu steuern.

3.3.1 Hersteller deutscher Smart-Home-Lösungen für Klima- und Umweltkontrolle

Tabelle 3.5 führt einige der wichtigsten Geräte und deren Hersteller auf, die auf dem deutschen Markt in dieser Kategorie zu finden sind. In Bezug auf Luftgütesensoren ist anzumerken, dass diese die Gesamtheit der Sensoren abdecken und unter dem Oberbegriff Partikelsensoren, Volatile Organic Compounds (VOC)-Sensoren (dt. Flüchtige Organische Verbindungen) , CO2-Sensoren, Feuchtigkeitssensoren, Temperatursensoren, Schadstoffsensoren und Formaldehysensoren umfassen.

Robert Bosch Smart Home GmbH Im Produktportfolio befinden sich Lüftungsgeräte, Klimageräte und Luftgütesensoren. Ein besonderes Merkmal ihrer Produkte ist der Rauchwarnmelder, der auch als Luftqualitätssensor fungiert. Nicht angeboten werden externe Wetterstationen. [121–123]

Tabelle 3.5: Hersteller deutscher Smart-Home-Lösungen für Klima- und Umweltkontrolle

Hersteller	Lüftungsgerät	Klimagerät	Wetterstation	Luftgütesensor
Robert Bosch Smart Home GmbH	✓	✓	✓	✓
eQ-3 AG	✗	✗	✗	✓
Vaillant Deutschland GmbH & Co. KG	✓	✓	✗	✓
Zehnder Group Deutschland GmbH	✓	✗	✗	✓
Blauberg Ventilatoren GmbH	✓	✗	✗	✓
Viessmann Climate Solutions SE	✓	✓	✗	✓
TFA Dostmann GmbH & Co. KG	✗	✗	✓	✓
Bresser GmbH	✗	✗	✓	✓
STIEBEL ELTRON GmbH & Co. KG	✓	✓	✗	✓

eQ-3 AG Das Produktportfolio beschränkt sich ausschließlich auf die Herstellung von Luftgütesensoren, während sie keine Lüftungsgeräte, Klimageräte oder Wetterstationen im Angebot haben. [124]

Vaillant Deutschland GmbH & Co. KG Im Produktportfolio befinden sich Lüftungsgeräten, Klimageräten und Luftgütesensoren. Nicht angeboten werden Wetterstationen. [125–127]

Zehnder Group Deutschland GmbH hat sich auf Lüftungsgeräte und Luftgütesensoren spezialisiert, bietet jedoch keine Wetterstationen oder Klimageräte an. [128, 129]

Blauberg Ventilatoren GmbH Im Produktportfolio befinden sich Lüftungsgeräte und Luftgütesensoren, jedoch ohne das Angebot von Wetterstationen oder Klimageräten. [130, 131]

Viessmann Climate Solutions SE Im Produktportfolio befinden sich Lüftungsgeräte, Klimageräte und Luftgütesensoren. Nicht angeboten werden Wetterstationen. [132–134]

TFA Dostmann GmbH & Co. KG Im Produktportfolio befinden sich Wetterstationen und Luftgütesensoren. Nicht angeboten werden Lüftungs- oder Klimageräte. [135, 136]

Bresser GmbH Im Produktportfolio befinden sich Wetterstationen und Luftgütesensoren. Nicht angeboten werden Lüftungs- und Klimageräte. [137, 138]

STIEBEL ELTRON GmbH & Co. KG Im Produktportfolio befinden sich Lüftungsanlagen, Klimageräte und Luftgütesensoren. Nicht angeboten werden Wetterstationen. [139–141]

3.3.2 Forensische Relevanz von Umwelt- und Klimakontrolle

In der Forschungsliteratur konnten bisher keine forensischen Arbeiten für den Zeitraum 2019 bis 2023 identifiziert werden, die sich spezifisch mit der forensischen Relevanz von Smart Home-Geräten aus der Kategorie Umwelt- und Klimakontrolle befassen. Trotz der zunehmenden Verbreitung dieser Technologien in modernen Haushalten, scheint es an spezifischen forensischen Untersuchungen zu mangeln, die sich auf die Datenerfassung, -analyse und -verwertung dieser Geräte konzentrieren.

3.4 Sicherheitssysteme

Zur Kategorie Sicherheit im Bereich Smart Home gehören verschiedene Geräte und Systeme, die darauf ausgelegt sind, ein Zuhause vor Sicherheitsbedrohungen wie Einbrüchen, Bränden und Umweltgefahren zu schützen.

3.4.1 Hersteller deutscher Smart-Home-Lösungen für Sicherheitssysteme

Tabelle 3.6 führt einige der wichtigsten Geräte und deren Hersteller auf, die auf dem deutschen Markt in dieser Kategorie zu finden sind.

Tabelle 3.6: Hersteller deutscher Smart-Home-Lösungen für Sicherheitssysteme

Hersteller	Alarmsystem	Überwachungskamera	Gegensprechanlage	Schließsystem	TFS	Bewegungsmelder	CO-Melder	Wassermelder
Robert Bosch Smart Home GmbH	✓	✓	✓	✗	✓	✓	✓	✓
ABUS August Bremicker Söhne KG	✓	✓	✓	✓	✓	✓	✓	✓
INSTAR Deutschland GmbH	✗	✓	✗	✗	✗	✗	✗	✗
eQ-3 AG	✗	✗	✗	✗	✓	✓	✓	✗
BURG-WÄCHTER KG	✓	✓	✓	✓	✓	✓	✗	✓
Busch-Jaeger Elektro GmbH	✓	✓	✓	✓	✓	✓	✓	✓
Gira - Giersiepen GmbH & Co. KG	✓	✓	✓	✓	✓	✓	✓	✓
Blockalarm GmbH	✓	✓	✗	✓	✓	✓	✓	✓

Robert Bosch Smart Home GmbH Im Produktportfolio befinden sich Alarmsysteme, Überwachungskameras, eine Gegensprechanlage, TFS, Bewegungsmelder, CO-Melder und Wassermelder. Obwohl Bosch kein eigenes Schließsystem anbietet, besteht eine Kooperation mit Yale Linus Smart Lock, deren Schließsystem in Bosch Smart Home Umgebungen integriert werden kann. [142–148]

ABUS August Bremicker Söhne KG Im Produktportfolio befinden sich Alarmsysteme, Überwachungskameras, Gegensprechanlagen, Schließsysteme, TFS, Bewegungsmelder, CO-Melder und Wassermelder. [149–156]

INSTAR Deutschland GmbH Im Produktportfolio befinden sich IP-Innen- und Außenkameras sowie Power over Ethernet (PoE)-Kameras. INSTAR beschränkt sich auf diesen Bereich und ist in anderen Segmenten der Smart-Home-Sicherheit nicht vertreten. [157]

eQ-3 AG Im Produktportfolio befinden sich TFS, Bewegungsmelder für Innen- und Außenbereiche und CO-Melder. Nicht angeboten werden Alarmsysteme, Überwachungskameras, Gegensprechanlagen, Schließsysteme und Wassermelder. [158–161]

BURG-WÄCHTER KG Im Produktportfolio befinden sich Alarmsysteme, Überwachungskameras, Gegensprechanlagen, Schließsysteme,TFS, Bewegungsmelder und Wassermelder. Nicht angeboten werden CO-Melder. [162–167]

Busch-Jaeger Elektro GmbH Im Produktportfolio befinden sich Alarmsysteme, Überwachungskameras, Gegensprechanlagen, Schließsysteme, TFS, Bewegungsmelder, CO-Melder und Wassermelder. [168–174]

Gira - Giersiepen GmbH & Co. KG Im Produktportfolio befinden sich Alarmsysteme, Überwachungskameras, Gegensprechanlagen, Schließsystemen, TFS, Bewegungsmeldern, CO-Melder und Wassermelder. [175–182]

Blockalarm GmbH Im Produktportfolio befinden sich Alarmsysteme, Überwachungskameras, Schließsysteme, TFS, Bewegungsmelder, CO-Melder und Wassermelder. Nicht angeboten werden Gegensprechanlagen. [183–189]

3.4.2 Forensische Relevanz von Sicherheitssystemen

In dieser Forschungsarbeit konnten forensische Analysen für drei der in Unterabschnitt 3.4.1 aufgeführten Geräte identifiziert werden, welche in dem definierten Zeitraum von 2019 bis 2023 untersucht wurden. Es ist anzumerken, dass die betrachteten Produkte nicht von deutschen Unternehmen stammen. Konkret umfassen die Forschungsarbeiten die Eufy Floodlight Überwachungskamera, das smarte Schließsystem August Smart Lock Pro und die dazugehörige Video- und Gegensprechanlage August Smart Doorbell Cam Pro.

Überwachungskamera - Eufy Floodlight Camera Die Gewinnung des forensischen Images aus dem eingebetteten Multi-Media Controller verdeutlichte die hohe Zugänglichkeit der Daten für forensische Zwecke. Die Wiederherstellung diverser Dateitypen aus dem nicht zugewiesenen Speicherbereich, darunter Bilder, Audiodateien und Textdokumente, unterstreicht die Datenzugänglichkeit. [120]

Die Analyse offenbarte eine deutliche Diversität in den Datenformaten, was auf eine mangelnde Homogenität hinweist. Diese Vielfalt an Dateitypen, von Bildern über Audiodateien bis hin zu ausführbaren und Stream-Dateien, erfordert unterschiedliche Herangehensweisen in der Analyse, was die Komplexität der forensischen Untersuchung erhöht. [120]

Der Informationsgehalt der Daten ist besonders hoch. Die Protokolle enthielten detaillierte Informationen über Wireless Fidelity (WiFi)-Verbindungen, Systemgrößen, P2P-Netzwerkverbindungen sowie den Status von Licht- und Bewegungssensoren. Darüber hinaus lieferten sie präzise Angaben zu Kameratypen, verbundenen Mobilgeräten und den Pfaden gespeicherter Mediendateien. [120]

Zeitstempel und Ereignis-IDs in den Protokollen sowie die Verschlüsselung der gespeicherten Videodateien trugen dazu bei, die Authentizität und Unveränderlichkeit der Daten sicherzustellen. [120]

Die Untersuchung brachte Bedenken bezüglich der Rechtskonformität zum Vorschein, vor allem in Bezug auf den Datenschutz und die Datensicherheit. Das Auffinden von Videos und Bildern in verschlüsselter Form sowie von Sicherheitszertifikaten deutete zunächst auf ein Bewusstsein für den Schutz vertraulicher Daten hin. Allerdings löste der Fund von Passwörtern, die unverschlüsselt gespeichert waren, Bedenken bezüglich der Sicherheit bei der Datenübertragung und -speicherung aus. Dies betonte die dringende Notwendigkeit, bestehende Sicherheitsverfahren zu überprüfen, um sicherzustellen, dass sie den gesetzlichen Anforderungen zum Datenschutz entsprechen. [120]

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.7 die forensische Relevanz von der Eufy Floodlight Camera anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 4,4 von 5 möglichen Bewertungspunkten.

Tabelle 3.7: Forensische Relevanz von Eufy Floodlight Camera

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	5
Homogenität der Daten	3
Informationsgehalt	5
Datenintegrität	5
Rechtskonformität	4

Schließsystem - August Smart Lock Pro Die forensische Analyse des August Smart Lock Pro bietet eine detaillierte Einsicht in die Funktionsweise und die Datensicherheitsaspekte dieses intelligenten Schließsystems. Durch das Anwenden von Rooting- beziehungsweise Jailbreaking-Methoden auf die verbundenen Smartphones konnte ein vollständiger Zugriff auf das Dateisystem erreicht werden [190]. Dieser Schritt ist kritisch, um tiefgreifende Datenstrukturen zu erschließen und forensisch relevante Informationen zu extrahieren.

Besonders aufschlussreich war die Untersuchung der Datenbankdateien „ModelDatabase.db“ und „LocationDatabase.db“, die eine Fülle von Informationen offenbarten. Dazu gehören detaillierte Nutzerprofile, Geräteinteraktionen wie Lock/Unlock-Ereignisse und, bei Verwendung der Auto-Unlock-Funktion, auch Global Positioning System (GPS)-Daten. Diese Daten werden in einer strukturierten Weise in relationalen Datenbanken gespeichert, was eine homogene Datensammlung und einen hohen Informationsgehalt gewährleistet. [190]

Eine Betrachtung der Rechtskonformität wurde in der untersuchten Forschungsarbeit nicht vorgenommen.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.8 die forensische Relevanz vom August Smart Lock Pro anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 4,0 von 5 möglichen Bewertungspunkten.

Tabelle 3.8: Forensische Relevanz von August Smart Lock Pro

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	4
Homogenität der Daten	4
Informationsgehalt	5
Datenintegrität	4
Rechtskonformität	3

Gegensprechanlage - August Smart Doorbell Cam Pro Die forensische Untersuchung der August Smart Doorbell Cam Pro zeigt, wie detailliert und systematisch Daten von diesem Gerät erfasst und verwaltet werden. Ähnlich wie beim Smart Lock Pro, erwies sich das Rooting/Jailbreaking als entscheidend für den Zugang zu tiefgreifenden Datenbereichen und der damit verbundenen forensischen Relevanz. [190]

Die Analyse brachte zutage, dass Informationen über Türklingelaktivitäten und Bewegungserkennungsereignisse in spezifisch angelegten Datenbankdateien und Cache-Ordnern gespeichert werden. Die strukturierte Speicherung dieser Daten in App-spezifischen Ordnern unterstreicht die Homogenität und den hohen Informationswert der Daten. Dabei spielt insbesondere die Integrität der gespeicherten Bilder und Ereignislogs eine wichtige Rolle, auch wenn sich zeigte, dass der Zugriff auf bestimmte Daten wie Bild-URLs zeitlich begrenzt sein kann. [190]

Die detaillierte Erfassung und Speicherung von Informationen, insbesondere im Kontext der Bewegungserkennung, erfordert eine sorgfältige Beachtung von Datenschutzgesetzen. Jedoch wurde eine Untersuchung der Rechtskonformität in der untersuchten Forschungsarbeit nicht vorgenommen.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.9 die forensische Relevanz von der August Smart Doorbell Cam Pro anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 4,0 von 5 möglichen Bewertungspunkten.

Tabelle 3.9: Forensische Relevanz von August Smart Doorbell Cam Pro

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	4
Homogenität der Daten	4
Informationsgehalt	5
Datenintegrität	4
Rechtskonformität	3

Für die in Tabelle 3.6 aufgeführten Technologien Alarmsystem, TFS, Bewegungsmelder, CO-melder und Wassermelder konnten keine forensischen Arbeiten identifziert werden.

3.5 Multimedia und Unterhaltung

Multimedia und Unterhaltung im Bereich Smart Home beschreibt die Integration und Automatisierung von audiovisuellen Geräten und Systemen, die es ermöglichen, Medieninhalte wie Musik, Filme und Fernsehsendungen auf eine benutzerfreundliche und interaktive Weise zu erleben.

3.5.1 Hersteller deutscher Smart-Home-Lösungen für Multimedia und Unterhaltung

Tabelle 3.10 führt einige der wichtigsten Geräte und deren Hersteller auf, die auf dem deutschen Markt in dieser Kategorie zu finden sind.

Tabelle 3.10: Hersteller deutscher Smart-Home-Lösungen für Multimedia und Unterhaltung

Hersteller	Smart TV	Smart Speaker	Webcam	Netzwerkspeicher	Streaming-Dienst	Sprachassistent
Lautsprecher Teufel GmbH	✗	✓	✗	✗	✗	✗
Loewe Technology GmbH	✓	✓	✗	✗	✗	✗
MEDION AG	✓	✓	✓	✓	✗	✗
Beko Germany GmbH	✓	✗	✗	✗	✗	✗
Metz Consumer Electronics GmbH	✓	✗	✗	✗	✗	✗
Sennheiser electronic SE & Co. KG	✗	✓	✗	✗	✗	✗

Teufel GmbH Im Produktportfolio befinden sich Smart Speaker, die sich mit Sprachassistenten wie Alexa koppeln lassen. Nicht angeboten werden Smart TVs, Webcams, Netzwerkspeicher, eigene Streaming-Dienste oder Sprachassistenten. [191]

Loewe Technology GmbH Im Produktportfolio befinden sich Smart TVs und Smart Speaker, die in Radio- und Multiroom-Formaten verfügbar sind. Nicht angeboten werden Webcams, Netzwerkspeicher, eigenen Streaming-Diensten oder Sprachassistenten. [192, 193]

MEDION AG Im Produktportfolio befinden sich Smart TVs, Smart Speaker mit Multiroom-Funktionalität, Webcams und Netzwerkspeicher. Nicht angeboten werden eigene Streaming-Dienste oder Sprachassistenten. [194–197]

Beko Germany GmbH Im Produktportfolio befinden sich Smart TVs. Nicht angeboten werden Smart Speaker, Webcams, Netzwerkspeicher, eigene Streaming-Dienste oder Sprachassistenten. [198]

Metz Consumer Electronics GmbH Im Produktportfolio befinden sich Smart TVs. Nicht angeboten werden smarte Lautsprecher, Webcams, Netzwerkspeicher, eigenen Streaming-Dienste oder Sprachassistenten. [199]

Sennheiser electronic SE & Co. KG Im Produktportfolio befinden sich Smart Speaker. Nicht angeboten werden Smart TVs, Webcams, Netzwerkspeicher, eigene Streaming-Dienste oder Sprachassistenten. [200]

3.5.2 Forensische Relevanz von Geräten für Multimedia und Unterhaltung

In dieser Forschungsarbeit konnten forensische Analysen für drei der in Unterabschnitt 3.5.1 aufgeführten Geräte identifiziert werden, welche in dem definierten Zeitraum von 2019 bis 2023 untersucht wurden. Es ist anzumerken, dass die betrachteten Produkte nicht von deutschen Unternehmen stammen. Konkret umfassen die Forschungsarbeiten den Smart Speaker Amazon Echo, Smart Speaker von Xiaomi, Amazon Echo Dot 4, sowie den Sprachassistenten Google Assistant und die Kamerafirmware von der D-Link DSC-5020L Kamera.

Smart Speaker - Amazon Echo Die Zugänglichkeit von Daten auf Amazon Echo-Geräten variiert je nach Untersuchungsmethode. Eine Geräteuntersuchung ermöglicht den Zugriff auf Konfigurationsdaten und Einstellungen über einen Universal Asynchronous Receiver Transmitter (UART)-Port. Obwohl eine Firmware-Analyse die Erstellung eines Disk-Images ermöglicht, ist der Beweiswert begrenzt und das Risiko der Datenzerstörung hoch. Die Netzwerkuntersuchung ist durch verschlüsselten Datenverkehr eingeschränkt, da ohne Benutzeranmeldeinformationen nur begrenzt beweiskräftige Daten zugänglich sind. Bei Cloud-Untersuchungen hingegen ist die Zugänglichkeit hoch, sofern Benutzeranmeldeinformationen vorliegen. Die Herausforderung besteht jedoch in der Kooperation mit Cloud-Anbietern ohne entsprechende Zugriffsberechtigungen. [201]

Auf Geräteebene ist die Homogenität der Daten gering, da sie stark von individuellen Gerätekonfigurationen und -einstellungen abhängen. Im Gegensatz dazu ist die Homogenität auf Netzwerk- und Cloud-Ebene höher, da die Daten dort in strukturierter Form vorliegen, beispielsweise über Application Programming Interface (API)s oder in Cloud-Datenbanken. [201]

Die Cloud-Untersuchung bietet einen sehr hohen Informationsgehalt, da die Cloud die meisten Benutzerdaten speichert und direkten Zugang zu Benutzeraktivitäten und -interaktionen ermöglicht. Netzwerkuntersuchungen sind durch Verschlüsselung begrenzt, während Geräteuntersuchungen überwiegend nur technische Konfigurationsdaten liefern. Interaktionsdaten, Kalenderinformationen, Listen, Verkehrsdaten und Haushaltsprofile bieten jedoch potenziell wertvolle Einsichten in Benutzeraktivitäten und -präferenzen. [201]

Das Risiko der Datenbeschädigung ist besonders bei der physischen Untersuchung von Geräten gegeben. Auf Netzwerk- und Cloud-Ebene ist die Datenintegrität hingegen höher, da digitale Forensikmethoden die Daten weniger beeinträchtigen und Beweise in unverändertem Zustand extrahiert werden können. Die Untersuchung von Cache-Daten kann Möglichkeiten bieten, gelöschte oder verborgene Daten wiederherzustellen, was auf eine hohe Datenintegrität hinweist. [201]

Die Rechtskonformität stellt insbesondere bei Cloud-Untersuchungen eine Herausforderung dar, da die Kooperation der Cloud-Anbieter erforderlich ist und Datenschutzgesetze eingehalten werden müssen. In Bezug auf die Geräte- und Netzwerkuntersuchung ist festzustellen, dass diese stark von der jeweiligen Rechtslage abhängt, insbesondere im Hinblick auf den Zugang zu verschlüsselten Daten und die physische Untersuchung von Geräten. Die Aufzeichnung privater Konversationen durch Echo-Geräte ohne das Aktivierungswort wirft zusätzliche Bedenken hinsichtlich Datenschutz und Einwilligung auf und könnte die Rechtskonformität beeinflussen. [201]

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.11 die forensische Relevanz vom Amazon Echo anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 3,4 von 5 möglichen Bewertungspunkten.

Tabelle 3.11: Forensische Relevanz von Amazon Echo

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	3
Homogenität der Daten	3
Informationsgehalt	5
Datenintegrität	4
Rechtskonformität	2

Smart Speaker - Xiaomi Smart Speaker Bei der forensischen Untersuchung von Smart Speakern, hier am Beispiel des Xiaomi Smart Speakers, wird sich primär auf die Extraktion und Analyse von Daten konzentriert, die lokal auf zugänglichen Geräten gespeichert sind. Dieser

Ansatz wird gewählt, da die Kooperation von Cloud-Servern oft limitiert ist, was den Zugriff auf in der Cloud gespeicherte Daten erschwert. Als Schlüsselquellen für forensische Daten dienen die offizielle Android-Anwendung des Smart Speakers und die Netzwerkkommunikation, die beide eine Fülle von leicht zugänglichen Informationen bieten. [202]

Die Android-Anwendung ermöglicht es den Nutzern, mit dem Smart Speaker zu interagieren und speichert kritische Datensätze wie Konversationen zwischen dem Nutzer und dem Sprachassistenten sowie Auditing-Logs der Anwendung. Diese Konversationen, die durch grafische Benutzeroberflächen sichtbar sind, und die Auditing-Logs, die in unverschlüsselten Log-Dateien festgehalten werden, bieten detaillierte Einblicke in die Nutzung des Geräts. Die Analyse dieser Daten mittels Natural Language Processing und Optical Character Recognition Technologien ermöglicht es, bedeutende Informationen aus den Textinhalten zu extrahieren und den Kommunikationsprozess zwischen Benutzer und Sprachassistent zu verstehen. [202]

Die Netzwerkkommunikation zwischen Smart Speaker und Cloud-Server, die über Hypertext Transfer Protocol Secure (HTTPS)-Protokolle abläuft, wird mittels Tools wie Fiddler analysiert, um verschlüsselte Daten mittels Man-in-the-Middle Technik zu entschlüsseln. Diese Analyse liefert wertvolle Informationen, die anderweitig nicht zugänglich wären, wie zum Beispiel die Metadaten der abgespielten Musik. Trotz der Herausforderungen bei der Analyse verschlüsselter Netzwerkdaten des Smart Speakers selbst, bietet die Untersuchung der Netzwerkkommunikation der Android-Anwendung ausreichende forensische Daten für die Untersuchung. [202]

Eine Untersuchung hinsichtlich Rechtskonformität und Homogenität wurde in der untersuchten Forschungsarbeit nicht vorgenommen.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.12 die forensische Relevanz vom Xiaomi Smart Speaker anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 4,3 von 5 möglichen Bewertungspunkten.

Tabelle 3.12: Forensische Relevanz von Xiaomi Smart Speaker

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	4
Homogenität der Daten	-
Informationsgehalt	5
Datenintegrität	4
Rechtskonformität	-

Smart Speaker - Amazon Echo Dot 4 Die forensische Analyse des Amazon Echo Dot 4. Generation Smart Speakers offenbart eine komplexe Landschaft an Datenzugänglichkeiten und Herausforderungen. Durch die Anwendung von manuellen und logischen Backup-Extraktionsmethoden konnten Daten effektiv sowohl direkt vom Gerät als auch aus der Cloud gewonnen werden. Besonders die logische Backup-Extraktion sticht hervor, da sie die foren-

sische Integrität der Daten durch Nicht-Veränderung während des Extraktions- und Analyseprozesses gewährleistet. Diese Methodik ist entscheidend, um die Authentizität der Beweise zu sichern und ihre forensische Verwendbarkeit zu garantieren. [203]

Die Analyse deckt auf, dass die Daten aus einer Vielfalt von Quellen stammen und in verschiedenen Formaten gespeichert sind, darunter SQLite-Datenbanken und Web-Cache-Dateien, die relevante Informationen wie Nutzerkonten und Interaktionen mit Alexa enthalten. Trotz dieser Diversität an Datenquellen und -formaten unterstützt der Einsatz von standardisierten Datenformaten eine gewisse Homogenität, die die Analyse und Interpretation der Daten erleichtert. [203]

Der Informationsgehalt der gewonnenen Daten ist hoch und umfasst ein breites Spektrum von Informationen, das von Nutzerkonten über Interaktionen mit dem Gerät bis hin zu Audioaufnahmen und Netzwerkeinstellungen reicht. Diese Daten bieten einen tiefen Einblick in das Nutzerverhalten und die Nutzung des Smart Speakers, was ihre hohe forensische Relevanz unterstreicht. [203]

Um die Integrität der Daten zu bewahren, wurden spezielle Maßnahmen ergriffen, wie die Erstellung eines Hashes nach der Datenerfassung, um sicherzustellen, dass die analysierten Daten nicht verändert wurden. Diese Sorgfalt in der Bewahrung der Datenintegrität ist essenziell, um die Glaubwürdigkeit der Beweise zu gewährleisten. [203]

Eine Untersuchung hinsichtlich Rechtskonformität wurde in der untersuchten Forschungsarbeit nicht vorgenommen.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.13 die forensische Relevanz vom Amazon Echo Dot 4 anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 4,0 von 5 möglichen Bewertungspunkten.

Tabelle 3.13: Forensische Relevanz vom Amazon Echo Dot 4

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	4
Homogenität der Daten	3
Informationsgehalt	5
Datenintegrität	4
Rechtskonformität	-

Sprachassistent - Google Home Assistant Bei der forensischen Analyse des Google Home Assistant, insbesondere in Verbindung mit Android-Smartphones, offenbart sich eine umfassende Datenzugänglichkeit. Die Extraktion von Rohkopien der Sprachaufnahmen, die für das Training des Google Assistant verwendet wurden, sowie der Zugriff auf Cloud-gespeicherte Daten zeigen, dass sowohl physische als auch Cloud-basierte Datenquellen effektiv genutzt werden können. Die Verwendung von Tools wie Audacity für Audiofiles und Cellebrite für die Datenextraktion unterstreicht die technischen Möglichkeiten zur Datenanalyse. [204]

Die Daten selbst präsentieren eine bemerkenswerte Homogenität, wobei Informationen systematisch in Datenbanken auf dem Gerät und in Cloud-Archiven gespeichert werden. Dies erleichtert die Analyse und Auswertung der forensischen Artefakte erheblich. Der Informationsgehalt der extrahierten Daten ist hoch und reicht von Sprachaufnahmen über Texttranskriptionen bis hin zu spezifischen Nutzeraktivitäten, wie erstellten Einkaufslisten. Diese Daten bieten tiefgreifende Einblicke in das Nutzerverhalten und die Interaktion mit dem Google Assistant. [204]

Die Integrität der Daten wird durch die Möglichkeit, Konversationen chronologisch zu rekonstruieren und gelöschte Konversationen zu identifizieren und teilweise wiederherzustellen, bestätigt. Die spezifische Kennzeichnung von Einträgen in der Datenbank und die präzise Zuordnung von Zeitstempeln ermöglichen eine genaue Nachverfolgung von Interaktionen und Löschvorgängen. [204]

Eine Untersuchung hinsichtlich Rechtskonformität und Homogenität wurde in der untersuchten Forschungsarbeit nicht vorgenommen.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.14 die forensische Relevanz vom Google Home Assistant anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 4,25 von 5 möglichen Bewertungspunkten.

Tabelle 3.14: Forensische Relevanz von Google Home Assistant

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	4
Homogenität der Daten	4
Informationsgehalt	5
Datenintegrität	4
Rechtskonformität	-

Webcam - D-Link DSC-5020L Die forensische Analyse von IoT-Kamera-Firmware, wie sie in der Arbeit von Akashdeep Bhardway et al. durchgeführt wurde, bietet tiefgreifende Einblicke in die Sicherheit und Funktionsweise dieser Geräte. Dies ist besonders relevant, da IoT-Kameras zunehmend in Smart Homes integriert werden und Funktionen wie Remote Monitoring und Control bieten. Die untersuchten Geräte von Marken wie Wyze, Netatmo, Arlo, Blink und Nest zeigten eine einheitliche Verfügbarkeit dieser Features und eine Integration in eigene Mobile Apps [205].

Die Analyse der D-Link DSC-5020L Kamera enthüllte, dass es möglich war, ein komprimiertes Dateisystem zu extrahieren. Diese Zugänglichkeit von Daten in der Firmware zeigt auf, wie leicht Informationen ausgelesen werden können. [205]

Die Homogenität der Daten ist hoch, da die meisten IoT-Kameras ähnliche Funktionen wie Remote Monitoring und eine eigene App anbieten, was darauf hinweist, dass die Firmware-Struktur und die darin enthaltenen Daten zwischen verschiedenen Marken und Modellen ähnlich sein könnten [205].

Die Analyse offenbarte einen hohen Informationsgehalt in der Firmware. So konnten Secure Sockets Layer (SSL)-Schlüssel, Ordner mit sensiblen Informationen wie „admin“, „root“, „password“ und „passwd“ sowie IP-Adressen, URLs und hart kodierten E-Mail-Adressen gefunden werden [205].

Die Tatsache, dass solch kritische Informationen wie SSL-Schlüssel und hart kodierte Anmeldedaten extrahiert werden konnten, wirft Fragen bezüglich der Datenintegrität auf. Dies deutet darauf hin, dass die Firmware möglicherweise anfällig für Manipulationen sein könnte, was ein ernstes Sicherheitsrisiko darstellt. [205]

Die Entdeckung von hart kodierten Informationen in der Firmware wirft Bedenken hinsichtlich der Rechtskonformität auf. Solche Praktiken können gegen Datenschutzgesetze verstoßen und die Privatsphäre der Nutzer gefährden. [205]

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.15 die forensische Relevanz von der D-Link DSC-5020L Webcam anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 3,8 von 5 möglichen Bewertungspunkten.

Tabelle 3.15: Forensische Relevanz von D-Link DSC-5020L Webcam

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	5
Homogenität der Daten	4
Informationsgehalt	5
Datenintegrität	3
Rechtskonformität	2

Für die in Tabelle 3.10 aufgeführten Technologien Smart TV, Netzwerkspeicher und Streaming-Dienst konnten keine forensischen Arbeiten identifziert werden.

3.6 Gesundheit

Geräte für Gesundheit im Smart Home sind Technologien, die darauf ausgelegt sind, die körperliche und geistige Gesundheit der Bewohner zu überwachen, zu unterstützen und zu verbessern.

3.6.1 Hersteller deutscher Smart-Home-Lösungen für Gesundheit

Tabelle 3.16 führt einige der wichtigsten Geräte und deren Hersteller auf, die auf dem deutschen Markt in dieser Kategorie zu finden sind.

medisana GmbH bietet alle Gesundheitsprodukte im Smart Home Bereich an, darunter Wearables, smarte Waagen, Blutdruckmessgeräte, Blutzuckermessgeräte und Schlafüberwachungsgeräte. Besonders hervorzuheben ist die Integration dieser Geräte mit der VitaDock+ App, welche es ermöglicht, Daten nahtlos vom Gerät zum Smartphone zu übertragen und zu verwalten. [206–210]

Beurer GmbH bietet ähnlich wie medisana GmbH eine gesamtheitliche Auswahl an Wearables, smarten Waagen, Blutdruckmessgeräten, Blutzuckermessgeräten und Schlafüberwachungsgeräten an. Ein besonderes Merkmal der Produkte von Beurer ist die Kompatibilität mit Bluetooth und USB, was eine flexible und bequeme Übertragung der Gesundheitsdaten auf das Smartphone ermöglicht. [211–215]

Leifheit AG ein weiterer deutscher Hersteller im Bereich der Gesundheitstechnologie, bietet ebenfalls eine Reihe von Produkten wie Wearables, smarte Waagen und Blutdruckmessgeräte an. Ein Aspekt bei Leifheit AG ist die Integration der Schlafüberwachung in das Wearable, im Gegensatz zu dedizierten Schlafüberwachungsgeräten bei medisana GmbH und Beurer GmbH. Es ist jedoch zu beachten, dass Leifheit AG keine Blutzuckermessgeräte im Produktportfolio führt. [216–218]

Tabelle 3.16: Hersteller deutscher Smart-Home-Lösungen für Gesundheit

Hersteller	Wearables	Smarte Waage	Blutdruckmessgerät	Blutzuckermessgerät	Schlafüberwachung
medisana GmbH	✓	✓	✓	✓	✓
Beurer GmbH	✓	✓	✓	✓	✓
Leifheit AG	✓	✓	✓	✗	✓

3.6.2 Forensische Relevanz von Geräten für Gesundheit

In dieser Forschungsarbeit konnten mehrere forensische Analysen für ein der in Unterabschnitt 3.6.1 aufgeführten Geräte identifiziert werden, welche in dem definierten Zeitraum von 2019 bis 2023 untersucht wurden. Es ist anzumerken, dass die betrachteten Produkte nicht von deutschen Unternehmen stammen. Konkret umfassen die Forschungsarbeiten die Wearables und Fitnesstracker Xiaomi Mi Band 2, Fitbit Alta HR, Fitbit Ionic und Alta Tracker, Fitbit Charge 2 und Huawei Band 2 Pro.

Wearable - Xaomi Mi Band 2 Das Gerät und seine begleitende Mi Fit App sammeln und speichern Nutzerdaten in einer SQLite3-formatierten Datenbank. Diese Organisation ermöglicht eine effiziente Datenzugänglichkeit, indem jede Nutzerinformation, Schlaf- und Aktivitäts-

daten eindeutig einem User ID zugeordnet und in einer separaten Datenbank gespeichert werden. Die Struktur dieser Datenbanken und die klare Trennung der verschiedenen Datentypen in definierten Tabellen weisen auf eine hohe Homogenität der Daten hin. [219]

Innerhalb dieser Datenbanken lassen sich Einblicke in das Nutzerverhalten und die persönlichen Gewohnheiten des Nutzers bieten. Dazu gehören nicht nur Basisinformationen wie Name, Geburtstag, Größe und Gewicht des Nutzers, sondern auch detaillierte Aufzeichnungen über tägliche Aktivitäten, Schlafmuster und spezifische Bewegungsdaten, inklusive GPS -Koordinaten. [219]

Die Datenintegrität wird durch die Verwendung von UNIX-Zeitstempeln für alle zeitlichen Aufzeichnungen sowie durch die konsistente Erfassung von Aktivitäts- und Bewegungsdaten gewährleistet. Besonders hervorzuheben ist die Fähigkeit der Mi Fit App, GPS-Daten in Keyhole Markup Language (KML)-Dateien zu exportieren und diese visuell auf Plattformen wie Google Earth darzustellen, was die Verlässlichkeit und Genauigkeit der aufgezeichneten Daten unterstreicht. [219]

Die untersuchte Forschungsarbeit liefert keine spezifischen Informationen zur Rechtskonformität der Daten im Bezug auf das Mi Band 2.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.17 die forensische Relevanz vom Xiaomi Mi Band 2 anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 4,25 von 5 möglichen Bewertungspunkten.

Tabelle 3.17: Forensische Relevanz von Xiaomi Mi Band 2

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	4
Homogenität der Daten	4
Informationsgehalt	5
Datenintegrität	4
Rechtskonformität	-

Wearable - Fitbit Alta HR Die Fitbit Alta HR nutzt diverse SQLite3-formatierte Datenbanken, um eine Vielzahl von Informationen zu sammeln und zu speichern, darunter Gerätedaten, Schritte, Schlafmuster und physische Aktivität. Diese Datenbanken dokumentieren detailliert die Interaktionen des Nutzers mit dem Gerät, wie etwa die Anzahl der Schritte, die zu bestimmten Zeiten unternommen wurden, und zeichnen diese in 15-Minuten-Intervallen auf. Besonders interessant ist die Klassifizierung der Daten, wobei Schritte, Körpergewicht und Kalorienverbrauch durch spezifische Objekttypen unterschieden werden, was eine strukturierte und homogene Datenerfassung impliziert. [219]

Die Analyse der Schlafdaten, die auf der Bewegungsdetektion des tragenden Bands basiert, sowie der GPS-Daten, die aktiviert werden, wenn der Nutzer die „Mobile Run“-Funktion in der Anwendung nutzt, enthüllt den reichen Informationsgehalt der durch das Gerät gesammelten

Daten. Diese Daten, einschließlich der aufgezeichneten Schlafphasen und der präzisen GPS-Koordinaten, sind auf einer Karte visualisiert und bieten tiefe Einblicke in das Verhalten und die Vorlieben des Nutzers. [219]

Von besonderem Interesse für forensische Untersuchungen ist die Fähigkeit, Modifikationen und Löschungen von Daten zu erkennen. Obwohl Schlafdaten zum Zeitpunkt der Modifikation aktualisiert werden und somit eine Herausforderung darstellen, die Originalität der Daten nachzuweisen, bleibt die Erkennung gelöschter Datensätze möglich. Gelöschte Datensätze sind nicht direkt sichtbar, verbleiben jedoch mit der Markierung „pendingDelete“ in der Datei. Diese subtilen Unterschiede im Binärformat der Datensätze vor und nach einer Löschung, einschließlich der Aktualisierung von Zeitstempeln, unterstreichen die Bedeutung der Datenintegrität und ermöglichen eine detaillierte forensische Analyse. [219]

Die untersuchte Forschungsarbeit liefert keine spezifischen Informationen zur Rechtskonformität der Daten in Bezug auf die Fitbit Alta HR.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.18 die forensische Relevanz von Fitbit Alta HR anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 4,0 von 5 möglichen Bewertungspunkten.

Tabelle 3.18: Forensische Relevanz von Fitbit Alta HR

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	4
Homogenität der Daten	4
Informationsgehalt	5
Datenintegrität	3
Rechtskonformität	-

Wearable - Fitbit Ionic und Alta Tracker Die forensische Analyse von Fitbit-Geräten, speziell des Ionic Smartwatch und des Alta Trackers, offenbart komplexe Herausforderungen und Möglichkeiten in Bezug auf die Sicherung und Analyse digitaler Beweise. Um die Integrität der Daten auf diesen Geräten zu gewährleisten, ist es entscheidend, während der Beschlagnahmung Vorsichtsmaßnahmen zu treffen. Diese Geräte, ähnlich wie Mobiltelefone, sammeln kontinuierlich Daten und können, wenn nicht korrekt gehandhabt, Informationen erfassen, die die Beweiskette verfälschen. Daher ist es unerlässlich, die Geräte sofort auszuschalten und in Faraday-Taschen zu platzieren, um unbeabsichtigte Synchronisationen oder Datenübertragungen zu verhindern. Zusätzlich sollten sie an Powerbanks angeschlossen werden, um den Zustand der Geräte zu konservieren. [220]

Die Daten auf Fitbit-Geräten selbst sind vielfältig, bis sie mit der Cloud synchronisiert werden. Die Synchronisation der Geräte vor der Beschlagnahme ist empfohlen, um Datenverlust zu vermeiden, wobei technische Schwierigkeiten, wie Probleme bei der Synchronisation mit

bestimmten Anwendungen, überwunden werden müssen. Ein Soft Reset kann in einigen Fällen erforderlich sein, birgt jedoch das Risiko, nicht synchronisierte Daten zu verlieren. Dies unterstreicht die Bedeutung einer sorgfältigen Abwägung durch den Ermittler. [220]

Die forensischen Analysen beider Fitbit-Geräte ergaben ähnliche Datenstrukturen und Speicherorte, was die Homogenität der Daten zwischen den Geräten verdeutlicht. Die erfassten Daten umfassen Nutzerinformationen, Geräteinteraktionen, Aktivitätslogs und sogar E-Wallet-Transaktionen, was den hohen Informationsgehalt dieser Geräte unterstreicht. Darüber hinaus bieten die Geräte Einblicke in manuelle versus automatisch erstellte Logs, was für die Überprüfung der Datenauthentizität von Bedeutung ist. Die Fähigkeit, den Erstellungsmodus eines Logs zu identifizieren, ist ein bedeutender Vorteil in forensischen Untersuchungen, da sie Aufschluss über die Zuverlässigkeit der Daten gibt. [220]

Die untersuchte Forschungsarbeit liefert keine spezifischen Informationen zur Rechtskonformität der Daten in Bezug auf Fitbit Ionic und Fitbit Alta.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.19 die forensische Relevanz von Fitbit Ionic und Alta Tracker anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 3,75 von 5 möglichen Bewertungspunkten.

Tabelle 3.19: Forensische Relevanz von Fitbit Ionic und Alta Tracker

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	3
Homogenität der Daten	4
Informationsgehalt	5
Datenintegrität	3
Rechtskonformität	-

Wearable - Fitbit Charge 2 Bei der forensischen Untersuchung von dem Fitbit Gerät Charge 2 stellte sich heraus, dass die Synchronisierung der Geräte mit den Fitbit-Servern über das Smartphone erfolgt, wobei die Daten zunächst verschlüsselt übermittelt und erst nach der Verarbeitung durch die Server für die Nutzer über ihre Smartphones zugänglich gemacht werden. Diese Art der Datenübertragung erschwert die direkte Extraktion von Fitnessinformationen mittels BLE, da die Daten nicht unmittelbar vom Gerät abgerufen werden können. Im Benutzerbereich des Smartphones wurden lediglich Binärdateien der Fitbit-App gefunden, deren Format zunächst nicht interpretierbar war. Weitere Einblicke bot der Root-Bereich, in dem unter anderem Google Maps Miniaturansichten von zurückgelegten Routen und Cache-Verzeichnisse mit verschiedenen Subverzeichnissen gefunden wurden. Diese enthielten unter anderem nicht verschlüsselte JavaScript Object Notation (JSON)-Dateien mit detaillierten Schrittzähldaten pro Minute. [221]

Die Untersuchung offenbarte eine Vielzahl von Datenformaten und -speicherorten, darunter SQLite-Datenbanken im Verzeichnis `/data/data/com.fitbit.FitbitMobile/`, die eine Fülle von Informationen enthielten. Dazu gehörten Daten zu Übungen, Nutzerprofilen, Herz-

frequenzen und Schlafzyklen. Diese Daten ermöglichten es, Pfade von Übungen zu rekonstruieren und boten tiefgehende Einblicke in die körperliche Aktivität und Gesundheit der Nutzer. Allerdings wurde die Integrität der Daten durch die Einschränkung beeinträchtigt, dass GPS-Informationen nur erfasst wurden, wenn das Telefon mit dem Internet verbunden war, und durch die Unzuverlässigkeit der Zeitreihendaten in den entsprechenden Datenbanktabellen aufgrund fehlender Daten. [221]

Während die Homogenität der Daten durch die Vielfalt der Datenformate und -speicherorte beeinträchtigt wurde, war der Informationsgehalt der erfassten Daten hoch, wenngleich die Reproduzierbarkeit der Existenz bestimmter Cache-Dateien ungewiss blieb. Fragen der Rechtskonformität, insbesondere im Hinblick auf Datenschutz und Sicherheit der Datenübertragung, blieben in der Untersuchung unadressiert, obwohl die Verschlüsselung von Benutzerdaten und die Verwendung öffentlicher APIs potenzielle Datenschutzherausforderungen darstellen. [221]

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.20 die forensische Relevanz von Fitbit Charge 2 anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 3,0 von 5 möglichen Bewertungspunkten.

Tabelle 3.20: Forensische Relevanz von Fitbit Charge 2

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	3
Homogenität der Daten	2
Informationsgehalt	4
Datenintegrität	3
Rechtskonformität	-

Wearable - Huawei Band 2 Pro Bei der forensischen Analyse des Huawei Band 2 Pro wurde festgestellt, dass die Datenübertragung zwischen dem Tracker und dem verbundenen Smartphone über Bluetooth erfolgt, wobei spezifische Charakteristiken für das Senden und Empfangen von Daten genutzt werden. Die Aktivierung von Benachrichtigungen ist erforderlich, um die Kommunikation zu ermöglichen. Diese scheint verschlüsselt zu sein, da in den übertragenen Byte-Strings kein erkennbares Muster identifiziert werden konnte. Ein Versuch, den Tracker direkt mit einem Laptop zu verbinden, scheiterte unabhängig vom Zustand des Trackers, was die Zugänglichkeit der Daten erschwert. [221]

Die Analyse der zugehörigen Huawei-Apps, insbesondere der Health- und Mobile Services-Apps, ergab die Speicherung von Daten in verschlüsselten Datenbanken und Log-Dateien. In der Mobile Service-App wurden Domain Name System (DNS)-Einträge zu Huawei-Diensten und eine Cookie-Datenbank mit abgelaufenen Sitzungsschlüsseln gefunden. Die Verschlüsselung dieser Datenbanken, zusammen mit den in den App-Daten gefundenen Schlüsseln und Salzwerten, stellt eine hohe Datenintegrität sicher, obwohl die Entschlüsselung mit Standardmethoden erfolglos blieb. [221]

Die Health-App speichert Daten über verbundene Geräte sowie verschlüsselte Gesundheitsdaten, deren Verschlüsselung nicht aufgebrochen werden konnte. Log-Dateien offenbarten jedoch detaillierte Informationen über Nutzerinteraktionen mit der App, einschließlich Schritt-, Kalorien- und Distanzdaten, was auf einen hohen Informationsgehalt hinweist. Positionen oder Herzfrequenzdaten wurden jedoch nicht gefunden. [221]

Die Netzwerkkommunikation der Health-App mit externen Servern, die direkte Anfragen ohne Proxy-Nutzung umfasst, könnte die Überwachung dieser Kommunikation und damit die Bewertung der Datenintegrität erschweren. [221]

Die untersuchte Forschungsarbeit liefert keine spezifischen Informationen zur Rechtskonformität der Daten in Bezug auf Huawei Band 2 Pro.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.21 die forensische Relevanz von Huawei Band 2 Pro anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 3,25 von 5 möglichen Bewertungspunkten.

Tabelle 3.21: Forensische Relevanz von Huawei Band 2 Pro

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	2
Homogenität der Daten	3
Informationsgehalt	4
Datenintegrität	4
Rechtskonformität	-

Für die in Tabelle 3.16 aufgeführten Technologien smarte Waage, Blutdruckmessgerät, Blutzuckermessgerät und Geräte zur Schlafüberwachung konnten keine forensischen Arbeiten identifiziert werden.

3.7 Haushalt und Garten

Geräte für Haushalt und Garten im Smart Home umfassen eine Vielzahl von intelligenten Geräten und Systemen, die darauf ausgerichtet sind, die alltäglichen Aufgaben im Haushalt und Garten effizienter, bequemer und automatisierter zu gestalten. Diese Geräte bieten Funktionen wie Fernsteuerung, Automatisierung, Echtzeit-Überwachung und -Feedback sowie die Integration in ein zentrales Smart Home-System.

3.7.1 Hersteller deutscher Smart-Home-Lösungen für Haushalt und Garten

Tabelle 3.22 führt einige der wichtigsten Geräte und deren Hersteller auf, die auf dem deutschen Markt in dieser Kategorie zu finden sind.

Tabelle 3.22: Hersteller deutscher Smart-Home-Lösungen für Haushalt und Garten

Hersteller	Smarte Waschmaschine	Smarter Trockner	Smarter Backofen	Smarter Geschirrspüler	Smarter Kühlschrank	Saugroboter	Mähroboter
Bosch * GmbH	✓	✓	✓	✓	✓	✓	✓
Siemens - SEG Hausgeräte GmbH	✓	✓	✓	✓	✓	✗	✗
Electrolux Hausgeräte GmbH - Markenvertrieb AEG	✓	✓	✓	✓	✓	✓	✗
Alfred Kärcher Vertriebs-GmbH	✗	✗	✗	✗	✗	✓	✗
Vorwerk Deutschland Stiftung & Co. KG	✗	✗	✗	✗	✗	✓	✗
STIHL Vertriebszentrale AG & Co. KG	✗	✗	✗	✗	✗	✗	✓
Miele Vertriebsgesellschaft Deutschland KG	✓	✓	✓	✓	✓	✓	✗

Bosch Bosch unterteilt sich im Bereich Haushalt und Garten in die Robert Bosch Hausgeräte GmbH und Robert Bosch Power Tools GmbH. Im Produktportfolio befinden sich smarte Waschmaschinen, Trockner, Backöfen, Geschirrspüler, Kühlschränke, Saugroboter und Mähroboter, die alle über die gemeinsam von Bosch und Siemens entwickelte Home Connect App gesteuert werden können. [222–228]

Siemens Siemens ist im Bereich Haushalt und Garten durch die SEG Hausgeräte GmbH vertreten. Im Produktportfolio befinden sich smarte Waschmaschinen, Trockner, Backöfen, Geschirrspüler und Kühlschränke, die von der Home Connect App gesteuert werden können. Siemens baut auch Staubsaugroboter, jedoch ohne Integration in das Smart Home. Nicht angeboten werden Mähroboter. [229–233]

Electrolux Hausgeräte GmbH Electrolux Hausgeräte GmbH ist zuständig für den Markenvertrieb von AEG. Im Produktportfolio befinden sich smarte Waschmaschinen, Trockner, Backöfen, Geschirrspüler, Kühlschränke und Saugroboter, die über die AEG Care App gesteuert werden können. Nicht angeboten werden Mähroboter. [234–238]

Alfred Kärcher Vertriebs-GmbH Im Produktportfolio befinden sich smarte Saugroboter und Mähroboter, wobei nur der Saugroboter in das Smart Home integriert werden kann. Nicht angeboten werden smarte Waschmaschinen, Trockner, Backöfen, Geschirrspüler oder Kühlschränke. [239]

Vorwerk Deutschland Stiftung & Co. KG Im Produktportfolio befinden sich smarte Saugroboter, die über eine App gesteuert werden können. Nicht angeboten werden smarte Waschmaschinen, Trockner, Backöfen, Geschirrspüler, Kühlschränke oder Mähroboter. [240]

STIHL Vertriebszentrale AG & Co. KG Im Produktportfolio befinden sich ausschließlich smarte Mähroboter, die über Bluetooth oder WLAN mit der MY iMOW App gesteuert werden können. Nicht angeboten werden smarte Waschmaschinen, Trockner, Backöfen, Geschirrspüler, Kühlschränke oder Saugroboter. [241]

Miele Vertriebsgesellschaft Deutschland KG Im Produktportfolio befinden sich smarte Waschmaschinen, Trockner, Backöfen, Geschirrspüler, Kühlschränke und Saugroboter. Diese Haushaltsgeräte sind über die Miele Cloud Schnittstelle mit Smart Home Partneranwendungen integrierbar, während die Saugroboter über die Miele Scout App gesteuert werden. Nicht angeboten werden smarte Mähroboter. [242–245]

3.7.2 Forensische Relevanz von Geräten für Haushalt und Garten

In dieser Forschungsarbeit konnte eine forensische Analyse für ein der in Unterabschnitt 3.7.1 aufgeführten Geräte identifiziert werden, welche in dem definierten Zeitraum von 2019 bis 2023 untersucht wurden. Es ist anzumerken, dass das betrachtete Produkt nicht von einem deutschen Unternehmen stammt. Konkret umfasst die Forschungsarbeit den Saugroboter Roomba j7+.

Saugroboter - Roomba j7+ Die Datenzugägnlichkeit kann durch Daten wie das Installationsdatum und die Uhrzeit der App, die Versionsnummer der App, Nutzungsereignisse, Reinigungspläne der Roboter und Benutzeranmeldeinformationen sowie Netzwerkinformationen über spezifische Verzeichnisse und Dateien auf dem Telefon untersucht werden. Diese Daten können durch direkten Zugriff auf bestimmte Verzeichnisse oder Dateien wie das „usagestats“ Verzeichnis, interne Speicherdatenbanken oder spezifische Extensible Markup Language (XML)-Dateien in der App-Datenstruktur abgerufen werden. [246]

Die Homogenität dieser Daten variiert. Während Installationsdatum und -zeit sowie die Versionsnummer der App in einem konsistenten und homogenen Format gespeichert werden, zeigen sich bei Nutzungsereignissen und Benutzeranmeldeinformationen sowie Netzwerkinformationen Inhomogenitäten. Diese Daten erfordern eine spezifische Konvertierung und Analyse, um sie intuitiv interpretieren zu können. Reinigungspläne werden hingegen in einem relativ homogenen und standardisierten Format gespeichert, was die Analyse erleichtert. [246]

Der Informationsgehalt der erhobenen Daten ist hoch und bietet Einblicke in verschiedene Aspekte der Nutzung. Das Installationsdatum und die Uhrzeit geben Aufschluss über den ersten Einsatz der App, während die Versionsnummer der App wichtige Hinweise auf die verwendete Softwareversion liefert. Nutzungsereignisse bieten einen detaillierten Einblick in das Verhalten und die Interaktionen der Nutzer mit der App. Reinigungspläne wiederum spiegeln die Gewohnheiten und Präferenzen der Nutzer wider. Benutzeranmeldeinformationen und Netzwerkinformationen sind besonders wertvoll, da sie sensible Daten enthalten, die Aufschluss über die Identität und das Netzwerkumfeld des Nutzers geben. [246]

Die Datenintegrität wird durch die feste Speicherung von Installationsdatum und -zeit sowie die Speicherung der Versionsnummer in der internen Datenbank gewährleistet. Die Integrität von Nutzungsereignissen hängt von der Genauigkeit der verwendeten Tools zur Datenaggregation ab. [246]

Informationen zur Rechtskonformität wurden in der wissenschaftlichen Arbeit nicht identifiziert.

Basierend auf den untersuchten Forschungsarbeiten wird in Tabelle 3.23 die forensische Relevanz von Roomba j7+ anhand der definierten Bewertungskriterien bewertet und erhält einen Durchschnittsscore von 4,0 von 5 möglichen Bewertungspunkten.

Tabelle 3.23: Forensische Relevanz von Roomba j7+

Bewertungskriterium	Forensische Wertigkeit
Datenzugänglichkeit	4
Homogenität der Daten	3
Informationsgehalt	5
Datenintegrität	4
Rechtskonformität	-

Für die in Tabelle 3.22 aufgeführten Technologien smarte Waschmaschine, smarter Trockner, smarter Backofen, smarter Geschirrspüler, smarter Kühlschrank und Mähroboter konnten keine forensischen Arbeiten identifziert werden.

3.8 Zusammenfassung der Ergebnisse

Tabelle 3.24 präsentiert einen vergleichenden Überblick über die forensische Relevanz der untersuchten Geräte aus den Forschungsarbeiten. Jedes Gerät erhält in diesen Kategorien eine Bewertung, die in einem Gesamtscore resultiert, welcher die forensische Relevanz widerspiegelt.

Die Eufy Floodlight Camera führt die Liste mit einem Gesamtscore von 4,4 an, was hohe Bewertungen in den Kategorien Datenzugänglichkeit, Informationsgehalt und Datenintegrität reflektiert. Smart Speaker von Xiaomi und der Google Home Assistant folgen mit Scores von 4,3 bzw. 4,25, beide mit hohen Werten im Informationsgehalt. Ähnliche Bewertungen erhalten das Xiaomi Mi Band 2 und der Amazon Echo Dot 4, die neben anderen Geräten wie dem August Smart Lock Pro und der August Smart Doorbell Cam Pro für ihre forensische Bedeutung hervorgehoben werden. Wearables wie das Fitbit Alta HR und der Roomba j7+ Saugroboter erzielen ebenfalls hohe Gesamtscores, was ihre Relevanz in forensischen Untersuchungen unterstreicht. Die D-Link DSC-5020L Webcam und verschiedene Smart Plugs werden ebenfalls analysiert, wobei ihre Bewertungen insbesondere in den Bereichen Datenintegrität und Rechtskonformität variieren.

Das untere Ende der Liste umfasst Geräte mit geringeren Bewertungen in bestimmten Kategorien, wie das Huawei Band 2 Pro und die Kasa Smart Light Bulb, deren Scores ihre begrenzte forensische Relevanz andeuten.

Tabelle 3.24: Übersicht über die forensische Relevanz der untersuchten Geräte

Gerätebezeichnung	Datenzugänglichkeit	Homogenität der Daten	Informationsgehalt	Datenintegrität	Rechtskonformität	Gesamtscore
Überwachungskamera - Eufy Floodlight Camera	5	3	5	5	4	4,4
Smart Speaker - Xiaomi Smart Speaker	4	-	5	4	-	4,3
Sprachassistent - Google Home Assistant	4	4	5	4	-	4,25
Wearable - Xiaomi Mi Band 2	4	4	5	4	-	4,25
Smart Speaker - Amazon Echo Dot 4	4	3	5	4	-	4,0
Schließsystem - August Smart Lock Pro	4	4	5	4	3	4,0
Gegensprechanlage - August Smart Doorbell Cam Pro	4	4	5	4	3	4,0
Wearable - Fitbit Alta HR	4	4	5	3	-	4,0
Saugroboter - Roomba j7+	4	3	5	4	-	4,0
Webcam - D-Link DSC-5020L	5	4	5	3	2	3,8
Wearable - Fitbit Ionic und Alta Tracker	3	4	5	3	-	3,75
Raumthermostat - Google Nest Raumthermostat	4	-	5	3	3	3,5
Smart Speaker - Amazon Echo	3	3	5	4	2	3,4
Wearable - Huawei Band 2 Pro	2	3	4	4	-	3,25
Smart Plug - Verschiedene Smart Plugs	4	2	5	2	-	3,25
Smarte Innenbleuchtung - Kasa Smart Light Bulb	3	4	4	3	2	3,2
Wearable - Fitbit Charge 2	3	2	4	3	-	3,0

4 Diskussion

Dieses Kapitel der vorliegenden Arbeit bietet eine Analyse und Interpretation der im Rahmen der Forschung gewonnenen Erkenntnisse. Ziel dieses Kapitels ist es, die Bedeutung der Ergebnisse im Kontext bestehender Theorien und vorangegangener Studien zu erörtern, mögliche Implikationen für die Praxis sowie für zukünftige Forschungsarbeiten aufzuzeigen und die festgestellten Limitationen kritisch zu reflektieren.

4.1 Interpretation des Bewertungsergebnisses

Nach der Analyse der Bewertungsdaten erfolgt nun die Interpretation der Ergebnisse, um deren Bedeutung für die Zielsetzungen der Forschungsarbeit vollständig zu erfassen.

4.1.1 Muster und Trends in der forensischen Relevanz

Tabelle 3.24 bietet eine Übersicht über die forensische Relevanz der untersuchten Smart Home-Geräte aus Forschungsarbeiten, basierend auf einem Bewertungssystem, das mehrere Kriterien umfasst: Datenzugänglichkeit, Homogenität der Daten, Informationsgehalt, Datenintegrität und Rechtskonformität. Jedes dieser Kriterien trägt zur Gesamtbewertung der forensischen Relevanz bei, wobei der Gesamtscore einen aggregierten Wert darstellt, der die Eignung der Geräte für forensische Untersuchungen widerspiegelt.

Die Analyse der Tabelle zeigt, dass die Überwachungskamera - Eufy Floodlight Camera mit einem Gesamtscore von 4,4 die höchste forensische Relevanz aufweist. Dies lässt auf eine ausgezeichnete Datenzugänglichkeit, einen hohen Informationsgehalt sowie eine robuste Datenintegrität schließen. Zudem deutet der vergleichsweise hohe Wert in der Kategorie Rechtskonformität darauf hin, dass die Nutzung der Daten aus dieser Kamera in forensischen Kontexten rechtlich verhältnismäßig unproblematisch ist.

Auffällig ist, dass Geräte wie der Xiaomi Smart Speaker und der Google Home Assistant trotz des Fehlens einer Bewertung für die Homogenität der Daten bzw. der Rechtskonformität mit Gesamtscores von 4,3 beziehungsweise 4,25 ebenfalls eine hohe forensische Relevanz aufweisen. Dies unterstreicht die Bedeutung des Informationsgehaltes und der Datenintegrität für die forensische Bewertung, selbst wenn nicht alle Kriterien bewertet werden können.

Die konsistente Bewertung von 5 im Bereich des Informationsgehalts für die meisten Geräte deutet auf ein allgemein hohes Potenzial hin, forensisch relevante Informationen zu liefern. Dies ist insbesondere im Kontext von Smart Home-Umgebungen von Bedeutung, in denen eine Vielzahl von Datenpunkten generiert wird, die Aufschluss über Nutzerverhalten und -interaktionen geben können.

Die Variation in der Kategorie Rechtskonformität, mit Werten, die von 2 bis 4 reichen, und mehreren Geräten, bei denen diese Kategorie als nicht anwendbar gekennzeichnet ist, wirft Fragen hinsichtlich der rechtlichen Rahmenbedingungen und der Zulässigkeit der Speicherung sowie Nutzung gesammelter Daten auf. Die Abwesenheit einer Bewertung in dieser Kategorie bei vielen Geräten könnte auf eine rechtliche Unsicherheit oder auf die Notwendigkeit weiterer Untersuchungen hinweisen.

Interessant ist auch die Beobachtung, dass Wearables und Smart Speaker durchweg hohe Bewertungen erhalten, was ihre potenzielle Nützlichkeit in forensischen Untersuchungen unterstreicht. Andererseits weisen Geräte mit spezifischeren Anwendungsfällen, wie Smart Plugs und smarte Innenbeleuchtung, niedrigere Gesamtscores auf. Dies könnte auf eine geringere Datenmenge oder eine geringere Vielfalt an nutzbaren Informationen zurückzuführen sein, die solche Geräte im Vergleich zu persönlicheren und interaktiveren Geräten wie Wearables und Smart Speakern bieten.

Abschließend lässt die Tabelle erkennen, dass die forensische Relevanz von Smart Home-Geräten von einer Reihe von Faktoren abhängt, die über die bloße technische Leistungsfähigkeit hinausgehen. Die rechtliche Komplexität und die Variabilität in der Bewertung bestimmter Kriterien verdeutlichen die Notwendigkeit einer multidisziplinären Herangehensweise bei der forensischen Analyse solcher Geräte.

4.1.2 Herausforderungen basierend auf der Auswertung

Eine forensische Analyse in der Welt der Smart Home-Technologien ist mit einer Reihe von Herausforderungen konfrontiert, die sowohl die Komplexität als auch die Dynamik dieser Technologien betreffen. Insbesondere die Vielfalt an Betriebssystemen, Softwareversionen und Hardwarekonfigurationen erhöht die Komplexität der Aufgabe, eine umfassende Bewertung der forensischen Relevanz vorzunehmen. Jedes dieser Systeme mag einen individuellen, auf das spezifische Betriebssystem zugeschnittenen forensischen Ansatz erfordern, was die Analyse verkompliziert und eine standardisierte Vorgehensweise erschwert.

Parallel dazu sorgt die schnelle Entwicklung innerhalb des Smart Home-Bereichs für eine ständige Evolution der Technologien. Neue Sicherheitsfeatures, die durch regelmäßige Updates implementiert werden, können die Art und Weise, wie Daten zugänglich gemacht werden, verändern und somit eine kontinuierliche Anpassung der Bewertungskriterien und -methoden erforderlich machen, um ihre Effektivität zu bewahren.

Neben technischen Herausforderungen spielen auch rechtliche Rahmenbedingungen eine wesentliche Rolle. Datenschutzrechtliche Beschränkungen können den Zugang zu benötigten Daten erheblich einschränken und beeinflussen damit direkt die Möglichkeit, eine forensische Bewertung durchzuführen. Diese rechtlichen Beschränkungen erfordern eine sorgfältige Navigation, um die forensische Arbeit im Einklang mit den gesetzlichen Vorgaben zu halten.

Ein nicht zu unterschätzendes Problem stellt zudem der Mangel an standardisierten Protokollen und Schnittstellen dar. Dieser Mangel führt zu einer Fragmentierung der Technologien, was die Analyse und Integration von Daten aus verschiedenen Quellen erschwert. Die unterschiedlichen Kommunikationsprotokolle zwischen Geräten können somit ein Hindernis für eine effiziente Analyse darstellen.

Die Vernetzung und Abhängigkeit der Geräte untereinander in Smart Home-Systemen fügt eine weitere Ebene der Komplexität hinzu. Die Funktionalität eines Geräts kann von einem anderen abhängig sein, was die Isolierung und Bewertung seiner individuellen forensischen Relevanz erschwert. Die Daten eines Geräts können nicht immer ohne den Kontext der Systemumgebung betrachtet werden, in der sie generiert wurden.

Schließlich ist die Art und Weise, wie Nutzer mit den Technologien im Alltag interagieren, von entscheidender Bedeutung. Die unterschiedlichen Nutzungsweisen führen zu einer Vielfalt an Daten, deren forensische Relevanz variieren kann. Dies betont die Bedeutung, das Benutzerverhalten zu verstehen und in die Analyse einzubeziehen, um ein umfassendes Bild der forensischen Möglichkeiten und Grenzen in Smart Home-Umgebungen zu gewinnen. Diese vielschichtigen Herausforderungen illustrieren die Notwendigkeit einer adaptiven und multidisziplinären Herangehensweise in der forensischen Analyse von Smart Home-Technologien.

4.1.3 Limitationen der Forschungsarbeit

In der vorliegenden Forschungsarbeit zur forensischen Analyse von Smart Home-Technologien wurden spezifische methodologische Entscheidungen getroffen, die gewisse Limitationen mit sich bringen. Erstens wurde der Untersuchungszeitraum auf die letzten fünf Jahre begrenzt, was zur Folge hatte, dass frühere Forschungsergebnisse, obwohl sie relevante Erkenntnisse bieten könnten, nicht berücksichtigt wurden. Insbesondere Studien und Analysen, die sich seit nahezu einem Jahrzehnt mit der forensischen Relevanz von Smart Home-Geräten, wie beispielsweise Smart TVs, auseinandersetzen und bereits im Jahr 2014 signifikante Ergebnisse lieferten, fielen durch dieses zeitliche Raster.

Zweitens beschränkte sich die Literaturrecherche ausschließlich auf akademische Portale. Diese Vorgehensweise gewährleistet zwar eine hohe Integrität und Sicherheit der herangezogenen Quellen, schließt jedoch gleichzeitig die sogenannte graue Literatur und damit potenziell wertvolle praktische Erkenntnisse und Analysen aus dem Untersuchungsspektrum aus.

Des Weiteren wurden in der Literaturrecherche nur Arbeiten berücksichtigt, die in deutscher oder englischer Sprache verfasst wurden. Diese sprachliche Limitierung könnte den Zugang zu Forschungsergebnissen und Entwicklungen einschränken, die in anderen Sprachen publiziert wurden, und somit die Perspektivenvielfalt der Analyse reduzieren.

Schließlich liegt eine Einschränkung in der Verfügbarkeit der Daten. Die Recherche ergab lediglich Arbeiten, die sich mit der technischen Analyse der Geräte und deren Steuerungssoftware auseinandersetzen. Studien, die im Rahmen rechtlicher Auseinandersetzungen angefertigt wurden und eventuell ebenfalls tiefgreifende Analysen beinhalten, konnten aufgrund rechtlicher Restriktionen und der damit verbundenen Zurückhaltung der Informationen nicht identifiziert werden.

Diese Limitationen verdeutlichen die Herausforderungen, die sich bei der Erforschung der forensischen Relevanz von Smart Home-Technologien ergeben und unterstreichen die Bedeutung einer kritischen Reflexion der methodologischen Rahmenbedingungen. Sie weisen auf die Notwendigkeit hin, zukünftige Forschungsarbeiten breiter anzulegen, um ein umfassenderes Verständnis der Thematik zu erlangen.

4.2 Hypothesenbildung für den forensischen Einsatz von Smart Home Geräten

Nachdem die Ergebnisse und Herausforderungen der digitalen Forensik im Kontext des IoT diskutiert wurden, erfolgt nun die Hypothesenbildung für den forensischen Einsatz von Smart Home Geräten. Dieses Kapitel zielt darauf ab, theoretische Szenarien zu formulieren, die als Grundlage für die effektive Untersuchung und Analyse von Beweismitteln innerhalb vernetzter Haushalte dienen.

4.2.1 Energieverwaltung

In diesem Abschnitt werden die potenziellen Einsatzmöglichkeiten von Geräten aus dem Bereich des Energiemanagements im forensischen Kontext beleuchtet, die über die in der Forschungsliteratur beschriebenen Anwendungsfälle hinausgehen.

Heizkörperthermostat und Raumthermostat Heizkörperthermostate und Raumthermostate, die individuell einstellbar sind und oft Nutzungsdaten speichern, könnten in forensischen Untersuchungen genutzt werden, um Präsenzmuster in Wohnräumen zu rekonstruieren. Die Analyse von Temperaturregelungsdaten könnte Aufschluss über An- und Abwesenheitszeiten der Bewohner geben. In Fällen von Einbruch oder Vandalismus könnten solche Daten als Beweismittel dienen, um zu zeigen, ob und wann Bewohner zuletzt anwesend waren.

HEMS Ein HEMS, das eine zentrale Rolle in der Koordination von Energieflüssen innerhalb eines Haushalts spielt, kann detaillierte Daten über den Energieverbrauch der angeschlossenen Geräte liefern. Im forensischen Kontext könnten diese Daten genutzt werden, um ungewöhnliche Aktivitäten oder Änderungen im Energieverbrauchsmuster zu identifizieren, die auf unautorisierte Zugriffe oder andere sicherheitsrelevante Vorfälle hindeuten könnten.

Smart Plug Smart Plugs, die zwischen elektrische Geräte und ihre Energiequelle geschaltet werden, erfassen Daten über den Energieverbrauch und die Betriebszeiten der angeschlossenen Geräte. Diese Informationen könnten forensisch genutzt werden, um die Nutzung von Geräten in einem Haushalt zu einem bestimmten Zeitpunkt nachzuvollziehen. Beispielsweise könnte die plötzliche Aktivierung eines Geräts in den Nachtstunden auf eine unerlaubte Anwesenheit hinweisen.

Photovoltaik und Photovoltaiksteuerung Photovoltaiksysteme und deren Steuerungseinheiten zeichnen Daten über die Energieproduktion, den Energieverbrauch und möglicherweise auch über die Steuerung der Energieverteilung auf. Diese Daten könnten forensische Hinweise auf die Nutzungsmuster des Haushalts und eventuelle Manipulationen oder Störungen im System bieten, die auf kriminelle Handlungen schließen lassen.

Innen- und Außenbeleuchtung, Lichtsteuerung Daten von intelligent gesteuerten Innen- und Außenbeleuchtungssystemen können Informationen über Bewegungs- und Anwesenheitsmuster innerhalb eines Gebäudes liefern. Beispielsweise könnte die Aktivierung der Außenbeleuchtung in Verbindung mit anderen Sicherheitssystemdaten genutzt werden, um die Zeitpunkte von Einbruchsversuchen zu bestimmen. Ebenso könnten Muster der Innenbeleuchtung Aufschluss über Lebensgewohnheiten der Bewohner oder über Anomalien in diesen Mustern geben, die mit spezifischen Ereignissen in Verbindung stehen.

Rollladen und Rollladensteuerung Die automatische oder manuelle Steuerung der Rollladen könnte Hinweise auf die An- oder Abwesenheit von Bewohnern zu bestimmten Zeiten geben. Darüber hinaus könnten ungewöhnliche Aktivitäten bei der Bedienung der Rollladen auf Eingriffe von außen hinweisen, insbesondere wenn diese Aktivitäten mit anderen Datenquellen, wie Sicherheitskameras, korrelieren.

4.2.2 Klima- und Umweltkontrolle

In diesem Abschnitt werden die potenziellen Einsatzmöglichkeiten von Geräten aus dem Bereich der Klima- und Umweltkontrolle im forensischen Kontext beleuchtet, die über die in der Forschungsliteratur beschriebenen Anwendungsfälle hinausgehen.

Lüftungs- und Klimageräte Diese Geräte bieten ähnliche forensische Daten, allerdings mit unterschiedlichen Informationen bezüglich der Temperaturregelung in einem Raum oder Gebäude. Die Analyse der Betriebsdaten eines Klimageräts könnte nicht nur die Präsenz von Personen aufzeigen, sondern auch auf eine gezielte Manipulation der Geräteeinstellungen hindeuten, beispielsweise um bestimmte physikalische Bedingungen für unerlaubte Aktivitäten zu schaffen oder zu verschleiern. Die Erfassung von Temperaturdaten über Zeit könnte zudem bei der Rekonstruktion von Ereignisabläufen helfen, insbesondere wenn diese Daten mit anderen forensischen Beweisen korreliert werden.

Wetterstationen Als Teil des Smart Home Systems, liefern Wetterstationen präzise Daten über die äußeren Wetterbedingungen. Diese Daten könnten in forensischen Untersuchungen von Nutzen sein, indem sie als Vergleichsbasis für die Plausibilität anderer gesammelter Daten dienen. Beispielsweise könnten Temperatur- und Feuchtigkeitsdaten von außen mit den Daten der Klima- und Lüftungssteuerung im Inneren abgeglichen werden, um Manipulationen oder Anomalien zu identifizieren. Weiterhin könnten Informationen über Niederschläge oder Sturmbedingungen in der Analyse von Einbruchsmustern oder Unfallereignissen von Bedeutung sein.

Luftgütesensoren Diese Sensoren sind in der Lage, eine Vielzahl von Daten bezüglich der Zusammensetzung der Luft in Innenräumen zu liefern, einschließlich der Konzentrationen von CO2, VOCs (flüchtige organische Verbindungen), Feinstaub und anderen Schadstoffen. Die forensische Analyse dieser Daten könnte Hinweise auf spezifische Aktivitäten oder Ereignisse innerhalb des überwachten Bereichs geben. Eine plötzliche Veränderung in der Luftqualität könnte auf chemische Prozesse, Brandereignisse oder die Anwesenheit von Personen in einem ansonsten leeren Raum hinweisen. Darüber hinaus könnten langfristige Datenaufzeichnungen von Luftgütesensoren dazu beitragen, Muster unerlaubter Aktivitäten oder Umweltvergehen zu erkennen.

4.2.3 Sicherheitssysteme

In diesem Abschnitt werden die potenziellen Einsatzmöglichkeiten von Geräten aus dem Bereich der Sicherheitssysteme im forensischen Kontext beleuchtet, die über die in der Forschungsliteratur beschriebenen Anwendungsfälle hinausgehen.

Alarmsysteme Diese Systeme sind zentral in der Detektion unautorisierten Zugangs oder anderer sicherheitsrelevanter Ereignisse. Im forensischen Kontext könnten die von diesen Systemen gespeicherten Protokolle und Alarmhistorien dazu genutzt werden, zeitliche Abläufe von Einbrüchen oder Sicherheitsverletzungen genau nachzuvollziehen. Über die reine Detektion hinaus könnten diese Systeme auch Aufschluss über die Anwesenheit oder Abwesenheit von Bewohnern zum Zeitpunkt eines Vorfalls geben.

Überwachungskameras Diese Geräte bieten eine visuelle Dokumentation von Ereignissen in und um das Eigentum. Die in den Aufnahmen enthaltenen Bilder und Videos können in forensischen Untersuchungen als direkte Beweismittel für die Identifizierung von Tätern, die Rekonstruktion von Tatverläufen oder das Nachvollziehen von Bewegungsmustern genutzt werden. Besonders die Integration von Gesichtserkennungstechnologien erhöht die forensische Wertigkeit dieser Geräte.

Gegensprechanlagen Diese Systeme sind oft verbunden mit Videoüberwachung, erweitern das Spektrum forensisch relevanter Daten um audiovisuelle Kommunikation. Die Analyse von Audioaufnahmen kann dabei helfen, Stimmen zu identifizieren, Zeitaussagen zu verifizieren und Hinweise auf die Anzahl der an einem Vorfall beteiligten Personen zu geben.

Schließsysteme Smart Locks protokollieren Zugänge und Zugriffszeiten. Diese Daten ermöglichen es, Bewegungsprofile von Personen zu erstellen und den physischen Zugang zu kritischen Bereichen im Zeitverlauf zu analysieren. Im Falle eines Einbruchs können Informationen über die Verwendung von Zugangscodes oder die Manipulation des Schließsystems entscheidende Hinweise liefern.

Tür- und Fensterkontakte Diese Kontakte signalisieren Öffnungen und Schließungen und können somit zur Rekonstruktion von Ein- oder Ausbruchssequenzen herangezogen werden. Die zeitliche Korrelation solcher Ereignisse mit anderen Sicherheitsdaten kann die Ermittlungen präzisieren.

Bewegungsmelder Diese Melder spielen eine zentrale Rolle in der automatisierten Überwachung von Räumlichkeiten. Die von ihnen erfassten Bewegungsdaten sind insbesondere dann von forensischem Interesse, wenn es darum geht, die Präsenz von Personen in spezifischen Bereichen eines Gebäudes zu bestimmten Zeiten zu belegen oder zu widerlegen.

CO-Melder und Wassermelder Diese Melder sind Beispiele für Geräte, die spezifische Umweltbedingungen überwachen. Während ihre primäre Funktion in der Gefahrenabwehr liegt, könnten die von ihnen erfassten Daten in Fällen, in denen Gesundheitsrisiken oder Schäden durch Umwelteinflüsse eine Rolle spielen, forensisch relevant sein. Die zeitliche Zuordnung und Intensität detektierter Ereignisse können hierbei Aufschluss über Ursachen und Verlauf von Vorfällen geben.

4.2.4 Multimedia und Unterhaltung

In diesem Abschnitt werden die potenziellen Einsatzmöglichkeiten von Geräten aus dem Bereich von Multimedia und Unterhaltung im forensischen Kontext beleuchtet, die über die in der Forschungsliteratur beschriebenen Anwendungsfälle hinausgehen.

Smart TVs Diese Geräte bieten nicht nur Zugang zu einem breiten Spektrum von Streaming-Diensten, sondern verfügen oft auch über integrierte Webcams und Mikrofone. Diese können zur Überwachung und Aufzeichnung von Gesprächen oder Aktivitäten im Raum genutzt werden, was sie zu potenziellen Quellen forensisch relevanter Informationen macht. Beispielsweise könnten in einem Smart TV gespeicherte Zugriffsprotokolle und Betrachtungshistorien Aufschluss über die Anwesenheit einer Person in einem bestimmten Zeitraum oder ihre Konsumgewohnheiten geben.

Smart Speaker und Sprachassistenten Sie sind in der Lage, Sprachbefehle zu erfassen und zu speichern. Diese Geräte könnten somit Aufzeichnungen von sprachlichen Interaktionen enthalten, die für Ermittlungen von Bedeutung sind. Beispielsweise könnten Aufzeichnungen von Sprachbefehlen dazu verwendet werden, die Anwesenheit bestimmter Personen im Haushalt zu bestimmten Zeiten zu beweisen oder Hinweise auf die Planung krimineller Aktivitäten zu liefern.

Webcams Diese Geräte sind häufig Bestandteil des Heimnetzwerks und können sowohl in Tablets und Smartphones integriert als auch als eigenständige Einheiten vorhanden sein. Obwohl Sie nicht primär für Überwachungszwecke ausgelegt sind, können kontinuierlich oder bei erkannter Bewegung Aufnahmen machen. Die Analyse der von diesen Kameras gespeicherten Videos könnte wichtige Beweise liefern, etwa indem sie Einbrecher identifiziert oder die letzten bekannten Bewegungen einer vermissten Person aufzeichnet.

Netzwerkspeicher Sie dienen als zentrale Speicherorte für digitale Dateien, einschließlich Fotos, Videos, Dokumente und mehr. Die Analyse der auf einem Network Attached Storage (NAS) gespeicherten Daten kann Aufschluss über die digitale Aktivität und Interaktionen der Nutzer geben. Zudem könnten Zeitstempel und Metadaten von gespeicherten Dateien dazu dienen, die Chronologie von Ereignissen zu rekonstruieren oder die Authentizität von Dokumenten zu überprüfen.

Streaming-Dienste Diese Dienste protokollieren die Sehgewohnheiten der Nutzer und können so detaillierte Informationen über deren Präferenzen und Lebensgewohnheiten liefern. Die Analyse von Nutzungsdaten könnte beispielsweise dabei helfen, Alibis zu überprüfen, indem sie zeigt, ob ein Verdächtiger zum Zeitpunkt eines Verbrechens einen Film angesehen hat.

4.2.5 Gesundheit

In diesem Abschnitt werden die potenziellen Einsatzmöglichkeiten von Geräten aus dem Bereich der Gesundheit im forensischen Kontext beleuchtet, die über die in der Forschungsliteratur beschriebenen Anwendungsfälle hinausgehen.

Wearables Wearables, einschließlich Fitness-Tracker und Smartwatches, zeichnen eine Vielzahl von Gesundheits- und Aktivitätsdaten auf, wie Schrittzahl, Herzfrequenz, Schlafmuster und sogar Standortdaten über eingebaute GPS-Funktionen. Im forensischen Kontext könnten diese Geräte genutzt werden, um die physische Aktivität und den Standort einer Person in einem bestimmten Zeitraum zu rekonstruieren. Beispielsweise könnten die aufgezeichneten Bewegungsprofile helfen, die Alibis von Verdächtigen zu überprüfen oder die letzten bekannten Standorte vermisster Personen zu ermitteln. Die Herzfrequenz- und Schlafdaten könnten zudem Aufschluss über Stressniveaus oder ungewöhnliche Aktivitäten vor einem kritischen Ereignis bieten.

Smarte Waagen Smarte Waagen messen nicht nur das Gewicht, sondern bieten oft auch Analysen zur Körperzusammensetzung, wie Körperfettanteil, Muskelmasse und Wasserhaushalt. Im forensischen Kontext könnten solche Daten dazu verwendet werden, Veränderungen im physischen Zustand einer Person über die Zeit hinweg zu dokumentieren, was bei Ermittlungen zu Fällen von Vernachlässigung oder Missbrauch relevant sein könnte. Darüber hinaus könnten signifikante und plötzliche Gewichtsveränderungen in Verbindung mit anderen Daten Hinweise auf Stress, Krankheit oder Drogenkonsum liefern.

Blutdruckmessgeräte Die regelmäßige Überwachung des Blutdrucks durch Smart Home-Geräte kann wertvolle Informationen über den Gesundheitszustand einer Person liefern. Im Kontext forensischer Untersuchungen könnten Blutdruckdaten genutzt werden, um Hinweise auf mögliche gesundheitliche Probleme oder Stressreaktionen in Zusammenhang mit kriminellen Aktivitäten zu identifizieren. Beispielsweise könnte ein auffälliges Muster von Bluthochdruck vor einem Verbrechen auf eine stressbedingte Beteiligung oder Vorbereitung hindeuten.

Blutzuckermessgeräte Blutzuckermessgeräte, die kontinuierlich oder bei Bedarf Glukosewerte messen, könnten forensisch genutzt werden, um den Gesundheitszustand und das Verhalten von Personen mit Diabetes zu überwachen. Unregelmäßigkeiten oder signifikante Veränderungen in den Blutzuckerdaten könnten auf nicht-eingehaltene Medikationspläne, ernährungsbedingte Probleme oder körperliche Belastungen hinweisen, die im Zusammenhang mit kriminellen Aktivitäten oder deren Folgen stehen könnten.

Schlafüberwachungsgeräte Schlafüberwachungsgeräte bieten Einblicke in Schlafmuster, -dauer und -qualität. Solche Daten könnten in forensischen Ermittlungen genutzt werden, um die Aussagen von Verdächtigen bezüglich ihres Aufenthaltsortes oder Aktivitäten in bestimmten Nächten zu verifizieren. Auffällige Veränderungen im Schlafverhalten könnten zudem auf psychischen Stress oder eine direkte Beteiligung an kriminellen Aktivitäten hinweisen.

4.2.6 Haushalt und Garten

In diesem Abschnitt werden die potenziellen Einsatzmöglichkeiten von Geräten aus dem Bereich von Haushalt und Garten im forensischen Kontext beleuchtet, die über die in der Forschungsliteratur beschriebenen Anwendungsfälle hinausgehen.

Smarte Waschmaschinen und Trockner Diese Geräte bieten Daten über Wasch- und Trocknungszyklen, die Zeitpunkte der Nutzung und die Art der gewählten Programme. Aus forensischer Sicht könnten solche Daten dazu beitragen, die An- oder Abwesenheit von Personen in einem Haushalt zu bestimmten Zeiten zu bestätigen oder zu widerlegen. Zudem könnten Abweichungen von üblichen Mustern auf besondere Ereignisse oder Verhaltensänderungen hinweisen, die mit einem zu untersuchenden Vorfall in Verbindung stehen könnten.

Smarte Backöfen und Geschirrspüler Diese Geräte zeichnen ähnlich wie Waschmaschinen und Trockner Informationen über Nutzungszeiten und Programmoptionen auf. Die Analyse dieser Daten kann aufzeigen, zu welchen Zeiten Mahlzeiten zubereitet oder Geschirr gereinigt wurde, was wiederum Rückschlüsse auf die Tagesabläufe der Haushaltsmitglieder und mögliche Änderungen im Zusammenhang mit kriminellen Aktivitäten zulässt.

Smarter Kühlschrank Diese Geräte bieten Einblicke in die Lebensmittelverwaltung und -nutzung im Haushalt. Sie können Informationen über die Häufigkeit der Türöffnungen, die Lagerung von Lebensmitteln und möglicherweise sogar über den Verbrauch bestimmter

Produkte erfassen. Diese Daten könnten forensisch genutzt werden, um Ernährungsgewohnheiten oder Änderungen im Lebensmittelkonsum zu untersuchen, die mit spezifischen Ereignissen oder Verhaltensweisen in Verbindung stehen könnten.

Saugroboter und Mähroboter Diese Geräte zeichnen Daten über ihre Einsatzzeiten, die gereinigten oder gemähten Bereiche und möglicherweise auftretende Hindernisse oder Störungen auf. Diese Informationen können Hinweise auf die Raumnutzung, die Anwesenheit von Personen oder Objekten zu bestimmten Zeiten und mögliche Veränderungen in der Umgebung bieten. Insbesondere Saugroboter könnten durch die Analyse gesammelter Staubproben sogar materielle Beweise liefern, die zur Aufklärung von Straftaten beitragen könnten.

5 Fazit und Ausblick

In diesem abschließenden Kapitel werden die wesentlichen Erkenntnisse der Forschungsarbeit reflektiert und es wird ein Ausblick auf die zukünftigen Entwicklungen geboten.

5.1 Zusammenfassung der Haupterkenntnisse

Im Rahmen der Forschungsarbeit wurde die aktuelle Lage der Smart Home Forensik eingehend analysiert, wobei ein besonderes Augenmerk auf die Untersuchung deutscher Produkte gelegt wurde. Trotz des signifikanten Anstiegs an Forschungsarbeiten in diesem Bereich konzentriert sich die Mehrheit der Studien auf ausländische Erzeugnisse, was eine deutliche Forschungslücke im Hinblick auf deutsche Hersteller offenbart. Durch die Identifizierung und Untersuchung von 35 deutschen Herstellern und 41 Smart Home Produkten wurde festgestellt, dass der deutsche Markt, insbesondere in den Bereichen Energieverwaltung und Sicherheit, signifikant durch einheimische Anbieter geprägt ist. Diese Dominanz ist nicht nur auf die Anzahl der Hersteller zurückzuführen, sondern auch darauf, dass viele dieser Unternehmen ein breites oder sogar vollständiges Produktspektrum abdecken.

Die methodische Herangehensweise an die forensische Analyse von Smart Home Geräten folgt überwiegend einem dreistufigen Ansatz, der sich aus physischer Geräteuntersuchung, Netzwerkverkehranalyse und Cloud-Forensik zusammensetzt. Diese Vorgehensweise unterstreicht die Abgrenzung zur klassischen Forensik, da bei der Smart Home Forensik die Analyse des Cloud-Providers selten ausgeschlossen wird.

Trotz der häufigen Bezeichnung der Smart Home Forensik als ein sich noch im Anfangsstadium befindendes Feld, zeigt ein Rückblick, dass die Anfänge dieser Disziplin bereits über ein Jahrzehnt zurückliegen. Dies relativiert die Wahrnehmung ihrer Neuheit, wenngleich Smart Home Forensik im Vergleich zur traditionellen Forensik immer noch als ein relativ junges Forschungsfeld betrachtet werden kann. Auffällig ist zudem, dass Forschungsarbeiten häufig nicht die neuesten auf dem Markt verfügbaren Geräte untersuchen. Stattdessen liegt der Fokus auf der Etablierung von Best Practices und der Erforschung effektiver Ansätze zur Bewältigung der Herausforderungen in diesem dynamischen Feld.

Ein wesentlicher Teil der Forschung widmet sich der theoretischen Entwicklung von Frameworks zur Standardisierung der Untersuchung von IoT-Geräten, wobei ein besonderes Interesse an der forensischen Analyse von Smart Speakern und Wearables zu beobachten ist. Demgegenüber stehen Systeme, die nicht durch Interaktivität mit dem Menschen geprägt sind, sowie die Produktkategorien Klima- und Umweltkontrolle, Haushalt und Garten, in denen eine deutliche Forschungslücke besteht.

Die Auswertung der Forschungsarbeiten offenbart einen deutlichen Mangel an Untersuchungen zur Rechtskonformität und zum gesetzlich vorgeschriebenen Datenmanagement. Dies hebt nicht nur das generelle Forschungsdefizit bezüglich deutscher Produkte hervor, sondern betont auch die dringende Notwendigkeit, den Fokus verstärkt auf inländische Erzeugnisse zu legen, um die identifizierten Lücken zu schließen.

5.2 Bewertung der Zielsetzung und Forschungsfrage

Die eingehende Bewertung der Zielsetzung der Forschungsfragen, wie in Abschnitt 1.2 skizziert, ermöglicht eine detaillierte Reflexion über den Umfang und die Tiefe der Forschungsarbeiten bezüglich der Smart Home-Technologien. Diese Arbeiten erstrecken sich nicht nur auf die Untersuchung der einzelnen Geräte, sondern auch auf deren Steuerungssoftwares und Smartphone-Applikationen, wodurch eine Fülle von digitalen Spuren aufgedeckt wurde, die ein umfassendes Bild der Interaktionsmuster innerhalb von Smart Home-Systemen zeichnen.

Ein wesentliches Merkmal der aktuellen Forschungslandschaft ist die Präferenz für die Entwicklung von forensischen Frameworks, die das gesamte Ökosystem von Smart Home umfassen, gegenüber der isolierten Analyse einzelner Geräte. Diese holistische Betrachtungsweise spiegelt das Verständnis wider, dass Smart Home-Systeme als vernetzte Einheiten agieren, in denen die Geräte in einem zusammenhängenden Verhältnis stehen.

Die forensische Bedeutung eines Smart Home-Geräts ergibt sich signifikant aus der Art und Weise, wie mit ihm interagiert wird. So kann beispielsweise ein Smart Speaker, der auf die Verarbeitung von Sprachbefehlen ausgelegt ist, einen erheblich größeren forensischen Wert bieten als ein simpler Lichtschalter. Diese Erkenntnis betont die Notwendigkeit, die Geräte nicht isoliert, sondern als integralen Bestandteil eines vernetzten Systems zu betrachten, um ein umfassendes Verständnis der Vorgänge im Smart Home zu erlangen.

Abschließend rückt die cloudbasierte Forensik immer stärker in den Vordergrund der forensischen Forschung, was die Anpassung an die zunehmende Datenverlagerung in die Cloud widerspiegelt. Diese Entwicklung stellt neue Herausforderungen für die forensische Analyse dar, bietet jedoch gleichzeitig auch neue Möglichkeiten, um umfangreiche Datenmengen effektiv zu untersuchen.

5.3 Zukünftige Forschungsfelder

In Anbetracht der schnellen Entwicklung und Verbreitung von IoT-Geräten in privaten sowie beruflichen Umgebungen unterliegt das Feld der IoT-Forensik und somit auch Smart Home Forensik einem kontinuierlichen Wandel, der sowohl neue Möglichkeiten als auch Herausforderungen mit sich bringt. Die Gewährleistung der Effektivität und Zuverlässigkeit

forensischer Methoden erfordert eine stetige Anpassung und Weiterentwicklung der Praktiken in diesem Bereich. Vor diesem Hintergrund lassen sich mehrere Empfehlungen für die Praxis und zukünftige Forschung formulieren:

Weiterentwicklung von Untersuchungsmethoden Angesichts der schnellen technologischen Fortschritte ist es imperativ, dass forensische Fachkräfte ihre Methoden und Techniken kontinuierlich weiterentwickeln. Dies schließt ein vertieftes Verständnis der Einsatzmöglichkeiten von IoT-Geräten in kriminellen Aktivitäten ein. Eine solche Dynamik erfordert eine agile Herangehensweise an die forensische Analyse, um mit der Geschwindigkeit der technologischen Entwicklungen mitzuhalten und potenzielle kriminelle Ausnutzungen effektiv zu adressieren.

Entwicklung standardisierter Prozesse Die Schaffung robuster, standardisierter Prozesse für die Erstellung, Dokumentation und Wartung von Forensik-Werkzeuge und Best Practices ist essenziell. Die Förderung von offenen Standards und die Sicherstellung der Überprüfbarkeit dieser Werkzeuge und Vorgehensweisen sind zentral, um deren Zuverlässigkeit und Eignung für gerichtliche Zwecke zu gewährleisten. Die Kooperation zwischen akademischen Einrichtungen und der Praxis spielt hierbei eine entscheidende Rolle, um Werkzeuge zu entwickeln, die real weltliche Herausforderungen adressieren und effektiv in diesen angewendet werden können.

Einrichtung zentraler Repositorien Die Entwicklung und Pflege zentraler Repositorien für forensische Werkzeuge steht im Vordergrund offener Forschungsfelder. Zukünftige Arbeiten sollten sich darauf konzentrieren, die Effizienz und Benutzerfreundlichkeit dieser Datenbanken zu verbessern. Dies schließt die Erweiterung der Funktionalitäten ein, um den Austausch von Wissen und bewährten Verfahren zu erleichtern. Forschung in diesem Bereich ist entscheidend, um die Nachhaltigkeit und Zugänglichkeit forensischer Ressourcen zu steigern und somit die gesamte forensische Gemeinschaft zu stärken.

Datenschutz und Rechtsrahmen Ein weiteres kritisches Forschungsfeld liegt in der Anpassung forensischer Praktiken an sich wandelnde Datenschutzbestimmungen und juristische Rahmenbedingungen. Forschungsinitiativen sind erforderlich, um Methoden und Werkzeuge zu entwickeln, die nicht nur effizient in der Beweissammlung sind, sondern auch die Privatsphäre der Beteiligten wahren und vollständig rechtskonform agieren. Die Herausforderung besteht darin, innovative Ansätze zu finden, die sowohl die Sicherheitsanforderungen erfüllen als auch den Schutz persönlicher Daten gewährleisten.

Entwicklung integrierter Rahmenwerke Angesichts der spezifischen Herausforderungen im IoT-Bereich ist die Ausarbeitung neuer Methoden und Techniken erforderlich, die sowohl technologische als auch soziotechnische Aspekte umfassen. Integrierte Rahmenwerke, die die komplexen Interaktionen zwischen Menschen, Technologien und der Umwelt berücksichtigen, sind unerlässlich, um ein umfassendes Verständnis der IoT-Landschaft zu erlangen und dieses effektiv in forensischen Untersuchungen zu nutzen.

Die kontinuierliche Anpassung an die dynamische Entwicklung des IoT-Sektors und die proaktive Auseinandersetzung mit den daraus resultierenden forensischen Herausforderungen sind entscheidend für die Zukunftssicherung der Forensik. Zukünftige Forschungsarbeiten sollten sich daher nicht nur auf die technologische Evolution konzentrieren, sondern auch soziotechnische Dynamiken und rechtliche Aspekte miteinbeziehen, um ganzheitliche und effektive forensische Lösungen zu entwickeln.

Literaturverzeichnis

[1] L. Caviglione, S. Wendzel und W. Mazurczyk, „The future of digital forensics: Challenges and the road ahead“, S. 12–17, 2017.

[2] R. Montasari, *An overview of cloud forensics strategy: capabilities, challenges, and opportunities*. Springer, 2017, S. 189–205, ISBN: 978-3-319-52491-7.

[3] A. Pichan, M. Lazarescu und S. T. Soh, „Cloud forensics: Technical challenges, solutions and comparative analysis“, S. 38–57, 2015.

[4] R. Heartfield u. a., „A taxonomy of cyber-physical threats and impact in the smart home“, *Computers & Security*, Jg. 78, S. 398, 2018.

[5] S. J. Darby, „Smart technology in the home: time for more clarity“, S. 140–147, 2018.

[6] W. K. Edwards und R. E. Grinter, *At home with ubiquitous computing: Seven challenges*. 2001, S. 256–272, ISBN: 3-540-42614-0.

[7] S. K. Das, D. J. Cook, A. Battacharya, E. O. Heierman und T.-Y. Lin, „The role of prediction algorithms in the MavHome smart home architecture“, S. 77–84, 2002.

[8] R. Blasco, Á. Marco, R. Casas, D. Cirujano und R. Picking, „A smart kitchen for ambient assisted living“, S. 1629–1653, 2014.

[9] F. Buttussi und L. Chittaro, „MOPET: A context-aware and user-adaptive wearable system for fitness training“, S. 153–163, 2008.

[10] F. Hüning, *Embedded Systems für IoT*. Springer, 2019, S. 13, 22–25, ISBN: 978-3-662-57901-5.

[11] C. Pätz, *Z-Wave: Die Funktechnologie für das Smart Home*. BoD–Books on Demand, 2017, S. 24–25, 34–45, 44–48, ISBN: 978-3738601947.

[12] Robert Bosch Smart Home GmbH, *Smart Home erklärt*, 2023. Adresse: `https://www.bosch-smarthome.com/de/de/smart-home-erklaert/so-funktionierts/` (besucht am 18. 01. 2024).

[13] G. Beniwal und A. Singhrova, „A systematic literature review on IoT gateways“, S. 9541–9563, 2022.

[14] Gastautor von Haus-XXL.de, *Wie kommuniziert ein Smart Home?*, Haustechnikverstehen.de, 2020. Adresse: `https://www.haustechnikverstehen.de/wie-kommuniziert-ein-smart-home/#Die_Kommunikation_zwischen_den_Geraumlten` (besucht am 22. 01. 2024).

[15] E. Sabanovic, „Historie und Technologie von WLAN-Standards der IEEE 802.11-Familie in Hinblick auf Angriffsszenarien“, S. 1–10,

[16] W. W. Osterhage und W. W. Osterhage, *WLAN*. Springer, 2018, S. 8, ISBN: 978-3-662-57902-2.

[17] Patrick Schnabel, *IEEE 802.11 / WLAN-Grundlagen*, Elektronik-Kompendium.de, 2024. Adresse: https://www.elektronik-kompendium.de/sites/net/0610051.htm (besucht am 29. 01. 2024).

[18] Patrick Schnabel, *WLAN-Topologie*, Elektronik-Kompendium.de, 2024. Adresse: https://www.elektronik-kompendium.de/sites/net/0907071.htm (besucht am 30. 01. 2024).

[19] C. Baun und Baun, *Computernetze kompakt*. Springer, 2012, S. 61, ISBN: 9783662574690.

[20] Patrick Schnabel, *Bluetooth 1.0/1.1/1.2 (IEEE 802.15)*, Elektronik-Kompendium.de, 2024. Adresse: https://www.elektronik-kompendium.de/sites/kom/0803301.htm (besucht am 29. 01. 2024).

[21] Patrick Schnabel, *Bluetooth Low Energy (4.0 / 4.1 / 4.2)*, Elektronik-Kompendium.de, 2024. Adresse: https://www.elektronik-kompendium.de/sites/kom/1805171.htm (besucht am 30. 01. 2024).

[22] Patrick Schnabel, *ZigBee*, Elektronik-Kompendium.de, 2024. Adresse: https://www.elektronik-kompendium.de/sites/kom/2212041.htm (besucht am 30. 01. 2024).

[23] Z. Alliance, „Zigbee alliance“, *WPAN industry group, http://www. zigbee. org/. The industry group responsible for the ZigBee standard and certification*, S. 297, 2010.

[24] D. Komilov, „Application of zigbee technology in IOT“, *International Journal of Advance Scientific Research*, Jg. 3, Nr. 09, S. 343–349, 2023.

[25] Patrick Schnabel, *Z-Wave*, Elektronik-Kompendium.de, 2024. Adresse: https://www.elektronik-kompendium.de/sites/kom/2212051.htm (besucht am 01. 02. 2024).

[26] Steffen Ewald, *Z-Wave Gen7 – Das Z-Wave Upgrade*, homee GmbH, 2022. Adresse: https://hom.ee/z-wave-gen7-das-z-wave-upgrade/ (besucht am 01. 02. 2024).

[27] D. Brodski, „Vergleich des Energieverbrauches der Protokolle Z-Wave und Zigbee“, in *Proceeding of the Seminar Sensor nodes-Operation, Network and Application (SN)*, Citeseer, S. 97–105.

[28] Effizienzhaus-online, *Smart Home – Zentral oder Dezentral*, DAA GmbH, 2024. Adresse: https://www.effizienzhaus-online.de/smart-home-zentral-oder-dezentral/ (besucht am 22. 01. 2024).

[29] Kai Kreuzer, *Positioning openHAB*, Aufruf: 17.01.2024, 2010. Adresse: http://www.kaikreuzer.de/2010/02/23/positioning-openhab/.

[30] openHAB Community, *openHAB Documentation*, openHAB Foundation e.V., 2024. Adresse: https://www.openhab.org/docs/ (besucht am 17. 01. 2024).

[31] openHAB Foundation e.V., *openHAB Demo*, 2024. Adresse: https://demo.openhab.org/page/temperatures (besucht am 08. 02. 2024).

[32] ioBroker Community, *ioBroker Architecture*, ioBroker GmbH, 2022. Adresse: https://www.iobroker.net/#en/documentation/basics/architecture.md (besucht am 22. 01. 2024).

[33] ioBroker GmbH, *[Projekt] Material Design CSS für ioBroker.vis*, 2024. Adresse: https://forum.iobroker.net/topic/7322/projekt-material-design-css-f%C3%BCr-iobroker-vis/273?lang=de (besucht am 28. 02. 2024).

[34] Home Assistant, *YAML*, 2024. Adresse: https://www.home-assistant.io/docs/configuration/yaml/ (besucht am 22. 01. 2024).

[35] Home Assistant, *Integrations*, 2024. Adresse: https://www.home-assistant.io/integrations/ (besucht am 22. 01. 2024).

[36] Home Assistant, *Automation YAML*, 2024. Adresse: https://www.home-assistant.io/docs/automation/yaml/ (besucht am 22. 01. 2024).

[37] Home Assistant, *Home Assistant Demo*, 2024. Adresse: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiAiP_F5pOEAxX1a_EDHegWCegQFnoECAgQAQ&url=https%3A%2F%2Fdemo.home-assistant.io%2F&usg=AOvVaw3yQvdgSuUCPVitNficJiNi&opi=89978449 (besucht am 05. 02. 2024).

[38] Google Ireland Limited, *Google Nest*, 2024. Adresse: https://store.google.com/de/category/connected_home?hl=de&pli=1 (besucht am 04. 03. 2024).

[39] Amazon Europe Core SARL, *Amazon Alexa*, 2024. Adresse: https://www.amazon.de/b?ie=UTF8&node=14100226031 (besucht am 04. 03. 2024).

[40] Apple Inc., *Apple HomeKit*, 2024. Adresse: https://www.apple.com/de/home-app/ (besucht am 04. 03. 2024).

[41] Samsung Electronics GmbH, *Samsung SmartThings*, 2024. Adresse: https://www.samsung.com/de/smartthings/app/ (besucht am 04. 03. 2024).

[42] Signify Holding, *Philips Hue*, 2024. Adresse: https://www.philips-hue.com/de-de (besucht am 04. 03. 2024).

[43] Robert Bosch Smart Home GmbH, *Bosch Smart Home*, 2024. Adresse: https://www.bosch-smarthome.com/de/de/ (besucht am 04. 03. 2024).

[44] A. Alenezi, H. Atlam, R. Alsagri, M. Alassafi und G. Wills, „IoT forensics: A state-of-the-art review, callenges and future directions“, in *Proceedings of the 4th international conference on complexity, future information systems and risk*, SCITEPRESS - Science und Technology Publications, 2019, S. 1–10, ISBN: 9789897583667.

[45] P. Lutta, M. Sedky, M. Hassan, U. Jayawickrama und B. B. Bastaki, „The complexity of internet of things forensics: A state-of-the-art review“, *Forensic Science International: Digital Investigation*, Jg. 1-10, S. 301 210, 2021.

[46] A. Goudbeek, K.-K. R. Choo und N.-A. Le-Khac, „A Forensic Investigation Framework for Smart Home Environment“, in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, S. 1446–1451. DOI: 10.1109/TrustCom/BigDataSE.2018.00201.

[47] K. Kaushik, A. Bhardwaj und S. Dahiya, „Smart Home IoT Forensics: Current Status, Challenges, and Future Directions“, in *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, 2023, S. 716–721. DOI: 10.1109/InCACCT57535.2023.10141730.

[48] A. Aljahdali, H. Aldissi, S. Banafee, S. Sobahi und W. Nagro, „IoT Forensic models analysis.“, *Romanian Journal of Information Technology & Automatic Control/Revista Română de Informatică și Automatică*, Jg. 31, Nr. 2, S. 27–28, 2021.

[49] T. Wu, F. Breitinger und S. O'Shaughnessy, „Digital forensic tools: Recent advances and enhancing the status quo“, *Forensic Science International: Digital Investigation*, Jg. 34, S. 300 999, 2020.

[50] G. Surange und P. Khatri, „IoT forensics: A review on current trends, approaches and foreseen challenges“, in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, 2021, S. 909–913.

[51] Robert Bosch Smart Home GmbH, *Smartes Heizkörper-Thermostat II*, 2023. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/heizkoerper-thermostat/ (besucht am 22. 02. 2024).

[52] Robert Bosch Smart Home GmbH, *Raumthermostat II*, 2023. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/raumthermostat/ (besucht am 22. 02. 2024).

[53] Robert Bosch Smart Home GmbH, *Der Energiemanager von Bosch*, 2023. Adresse: https://www.bosch-smarthome.com/de/de/produkte/weitere-bosch-produkte/energiemanager/ (besucht am 22. 02. 2024).

[54] Robert Bosch Smart Home GmbH, *Zwischenstecker kompakt*, 2023. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/zwischenstecker-kompakt/ (besucht am 22. 02. 2024).

[55] Robert Bosch Smart Home GmbH, *Lichtsteuerung*, 2023. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/lichtsteuerung/ (besucht am 22. 02. 2024).

[56] Robert Bosch Smart Home GmbH, *Rolladensteuerung*, 2023. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/rollladensteuerung/ (besucht am 22. 02. 2024).

[57] tado GmbH, *Smartes Heizkörper-Thermostat - Starter Kit V3+*, 2024. Adresse: https://shop.tado.com/products/smart-radiator-thermostat-starter-kit-v3 (besucht am 22. 02. 2024).

[58] tado GmbH, *Starter Kit – Smartes Thermostat*, 2024. Adresse: https://www.tado.com/at-de/smartes-thermostat (besucht am 22. 02. 2024).

[59] tado GmbH, *Energiemanagement-Service*, 2024. Adresse: https://www.tado.com/de-de/entdecken (besucht am 22. 02. 2024).

[60] eQ-3 AG, *HomeMatic Funk-Heizkörperthermostat*, 2024. Adresse: https://www.eq-3.de/produkte/homematic/detail/homematic-funk-heizkoerperthermostat.html (besucht am 22. 02. 2024).

[61] eQ-3 AG, *HomeMatic Funk-Wandthermostat*, 2024. Adresse: https://www.eq-3.de/produkte/homematic/detail/homematic-funk-wandthermostat-aufputzmontage.html (besucht am 22. 02. 2024).

[62] eQ-3 AG, *Flexible Heizungssteuerung per Smartphone und Internet*, 2024. Adresse: https://www.eq-3.de/produkte/max.html (besucht am 22. 02. 2024).

[63] eQ-3 AG, *Schaltsteckdose*, 2024. Adresse: https://homematic-ip.com/de/produkt/schaltsteckdose (besucht am 22. 02. 2024).

[64] eQ-3 AG, *Licht*, 2024. Adresse: https://www.eq-3.de/produkte/homematic/licht.html (besucht am 22. 02. 2024).

[65] eQ-3 AG, *Rollläden und Markisen*, 2024. Adresse: https://www.eq-3.de/produkte/homematic/rolllaeden-und-markisen.html (besucht am 22. 02. 2024).

[66] devolo GmbH, *Home Control Heizkörperthermostat*, 2024. Adresse: https://www.devolo.de/devolo-home-control-heizkoerperthermostat (besucht am 22. 02. 2024).

[67] devolo GmbH, *devolo Home Control Raumthermostat*, 2024. Adresse: https://www.devolo.de/devolo-home-control-raumthermostat (besucht am 22. 02. 2024).

[68] devolo GmbH, *E-Mobilität & Energiemanagement im Privathaushalt*, 2024. Adresse: https://business.devolo.de/emobility/ac-charging-energiemanagement (besucht am 22. 02. 2024).

[69] devolo GmbH, *devolo Home Control Schalt- und Messsteckdose*, 2024. Adresse: https://www.devolo.de/devolo-home-control-schalt-und-messsteckdose-20 (besucht am 22. 02. 2024).

[70] devolo GmbH, *devolo Home Control Dimmer-Unterputz*, 2024. Adresse: https://www.devolo.de/devolo-home-control-dimmer-unterputz (besucht am 22. 02. 2024).

[71] devolo GmbH, *devolo Home Control Rollladensteuerung-Unterputz*, 2024. Adresse: https://www.devolo.de/devolo-home-control-rollladensteuerung-unterputz (besucht am 22. 02. 2024).

[72] DELTA DORE RADEMACHER GmbH, *DuoFern Heizkörperstellantrieb 2 9433-1 (2. Generation)*, 2024. Adresse: https://www.rademacher.de/produkte/licht-heizung/heizungssteuerung/duofern-heizkoerperstellantrieb-9433-1 (besucht am 22. 02. 2024).

[73] DELTA DORE RADEMACHER GmbH, *DuoFern Raumthermostat 2 9485-1 (2. Generation)*, 2024. Adresse: https://www.rademacher.de/produkte/licht-heizung/heizungssteuerung/duofern-raumthermostat-9485-1 (besucht am 22. 02. 2024).

[74] DELTA DORE RADEMACHER GmbH, *DuoFern Zwischenstecker 9472-1*, 2024. Adresse: https://www.rademacher.de/produkte/licht-heizung/lichtsteuerung/duofern-zwischenstecker-9472-1 (besucht am 22. 02. 2024).

[75] DELTA DORE RADEMACHER GmbH, *Smarte Lichtsteuerung*, 2024. Adresse: https://www.rademacher.de/licht-heizung/produkte/lichtsteuerung (besucht am 22. 02. 2024).

[76] DELTA DORE RADEMACHER GmbH, *Elektrischer Gurtwickler – RolloTron*, 2024. Adresse: https://www.rademacher.de/rollladen-sonnenschutz/produkte/rollotron-elektrischer-gurtwickler (besucht am 22. 02. 2024).

[77] DELTA DORE RADEMACHER GmbH, *Zeitschaltuhren zur Steuerung von Rohrmotoren*, 2024. Adresse: https://www.rademacher.de/rollladen-sonnenschutz/produkte/steuerung (besucht am 22. 02. 2024).

[78] AVM Computersysteme Vertriebs GmbH, *FRITZ!DECT 301*, 2024. Adresse: https://avm.de/produkte/smart-home/fritzdect-301/ (besucht am 22. 02. 2024).

[79] AVM Computersysteme Vertriebs GmbH, *FRITZ!DECT 440*, 2024. Adresse: https://avm.de/produkte/smart-home/fritzdect-440/ (besucht am 22. 02. 2024).

[80] AVM Computersysteme Vertriebs GmbH, *FRITZ!DECT 200*, 2024. Adresse: https://avm.de/produkte/smart-home/fritzdect-200/ (besucht am 22. 02. 2024).

[81] AVM Computersysteme Vertriebs GmbH, *FRITZ!DECT 500*, 2024. Adresse: https://avm.de/smarthome/die-intelligente-led-lampe/ (besucht am 22. 02. 2024).

[82] AVM Computersysteme Vertriebs GmbH, *Festbeleuchtung mit FRITZ! – Neue Funktion der FRITZ!App Smart Home*, 2024. Adresse: https://avm.de/unternehmen/presse/presseinformationen/2021/12/festbeleuchtung-mit-fritz-neue-funktion-der-fritzapp-smart-home/ (besucht am 22. 02. 2024).

[83] AVM Computersysteme Vertriebs GmbH, *Intelligente Rollläden im Smart Home: kein Problem mit FRITZ!Box*, 2024. Adresse: https://avm.de/aktuelles/neues-von-fritz/2023/intelligente-rolllaeden-im-smart-home-kein-problem-mit-fritzbox/ (besucht am 22. 02. 2024).

[84] Schneider Electric GmbH, *Wiser, Heizkörperthermostat, schwarz*, 2024. Adresse: https://www.se.com/de/de/product/CCTFR6101/wiser-heizk%C3%B6rperthermostat-schwarz/ (besucht am 22. 02. 2024).

[85] Schneider Electric GmbH, *Wiser Raumthermostat mit Display*, 2024. Adresse: https://shop.se.com/de/de/wiser-thermostat-d-ambiance-connecte-liaison-zigbee-2-4ghz-cctfr6400.html (besucht am 22. 02. 2024).

[86] Schneider Electric GmbH, *Wiser™ Energiemanagement*, 2024. Adresse: https://www.se.com/de/de/product-range/62107-wiser-energiemanagement/ (besucht am 22. 02. 2024).

[87] Schneider Electric GmbH, *Wiser Smart Plug (Zwischenstecker)*, 2024. Adresse: https://www.se.com/de/de/product/CCTFR6501/wiser-smart-plug-zwischenstecker/ (besucht am 22. 02. 2024).

[88] Schneider Electric GmbH, *Lichtsteuerung*, 2024. Adresse: https://shop.se.com/de/de/produkte/schalter-und-steckdosen/lichtsteuerung.html (besucht am 22. 02. 2024).

[89] Schneider Electric GmbH, *Wiser Starter Kit für Rollladen- & Jalousiesteuerung*, 2024. Adresse: https://shop.se.com/de/de/wiser-kit-fur-rollladen-jalousiesteuerung.html (besucht am 22. 02. 2024).

[90] SMA Solar Technology AG, *Sunny Home Manager 2.0*, 2024. Adresse: https://www.sma.de/produkte/monitoring-control/sunny-home-manager (besucht am 22. 02. 2024).

[91] SMA Solar Technology AG, *Das SMA Produktportfolio*, 2024. Adresse: https://www.sma.de/produkte (besucht am 22. 02. 2024).

[92] Solarwatt GmbH, *SOLARWATT Manager*, 2024. Adresse: https://www.solarwatt.de/loesungen/unsere-produkte/uebersicht/manager (besucht am 22. 02. 2024).

[93] Solarwatt GmbH, *Dein Zuhause verdient das Original*, 2024. Adresse: https://www.solarwatt.de/loesungen/unsere-produkte/uebersicht/module (besucht am 22. 02. 2024).

[94] Solarwatt GmbH, *SOLARWATT Battery flex*, 2024. Adresse: https://www.solarwatt.de/loesungen/unsere-produkte/uebersicht/speicher (besucht am 22. 02. 2024).

[95] Giersiepen GmbH & Co. KG, *Gira System 3000 Raumtemperaturregler*, 2024. Adresse: https://www.gira.de/produkte/heizung-klima/gira-system-3000-heizungssteuerung#mehr-wohnkomfort (besucht am 22. 02. 2024).

[96] Giersiepen GmbH & Co. KG, *Verbesserte Energieeffizienz durch intelligente Verbrauchssteuerung*, 2024. Adresse: https://partner.gira.de/systeme/knx-system/knx-produkte/server/homeserver/energie.html (besucht am 22. 02. 2024).

[97] Giersiepen GmbH & Co. KG, *Steckdosen von Gira – Vielfalt in Material und Funktion*, 2024. Adresse: https://www.gira.de/produkte/steckdosen# (besucht am 22. 02. 2024).

[98] Giersiepen GmbH & Co. KG, *Gira X1*, 2024. Adresse: https://partner.gira.de/systeme/knx-system/knx-produkte/server/x1.html (besucht am 22. 02. 2024).

[99] Giersiepen GmbH & Co. KG, *Gira Licht- und Energiesäule für außen*, 2024. Adresse: https://www.gira.de/produkte/loesungen-fuer-aussen/gira-licht-und-energiesaeule (besucht am 22. 02. 2024).

[100] Busch-Jaeger Elektro GmbH, *Energie effizient einsetzen*, 2024. Adresse: https://www.busch-jaeger.de/inspiration/neubau-renovierung/start-ins-energiemanagement (besucht am 22. 02. 2024).

[101] Busch-Jaeger Elektro GmbH, *Heizkörperthermostat Basic free@home, Wireless für Busch-free@home®*, 2024. Adresse: https://www.busch-jaeger.de/online-katalog/detail/2CKA006200A0131 (besucht am 22. 02. 2024).

[102] Busch-Jaeger Elektro GmbH, *Raumtemperaturregler, Busch-free@home®*, 2024. Adresse: https://www.busch-jaeger.de/produkt/raumtemperaturregler-busch-freehome (besucht am 22. 02. 2024).

[103] Busch-Jaeger Elektro GmbH, *Energiemanagement effizient – mit dem Busch-EnergyMonitor®*, 2024. Adresse: https://www.busch-jaeger.de/files/files_ONLINE/Brosch%C3%BCre_EnergyMonitor_druck.pdf (besucht am 22. 02. 2024).

[104] Busch-Jaeger Elektro GmbH, *Jalousiemanagement*, 2024. Adresse: https://www.busch-jaeger.de/produkt/kategorie/jalousiemanagement (besucht am 22. 02. 2024).

[105] Busch-Jaeger Elektro GmbH, *Beleuchtungssteuerung*, 2024. Adresse: https://www.busch-jaeger.de/produkt/kategorie/beleuchtungssteuerung (besucht am 22. 02. 2024).

[106] Alfred Schellenberg GmbH, *Digitales Heizkörperthermostat*, 2024. Adresse: https://schellenberg-shop.de/digitales-heizkoerperthermostat/20101 (besucht am 22. 02. 2024).

[107] Alfred Schellenberg GmbH, *Schellenberg Smart Home Funk-Steckdose*, 2024. Adresse: https://your-smarthome.com/shop/schellenberg-smart-home-funk-steckdose-zwischenstecker-innenbereich-plug-app-steuerung-schuko (besucht am 22. 02. 2024).

[108] Alfred Schellenberg GmbH, *Schellenberg Rollladen*, 2024. Adresse: https://schellenberg-shop.de/rollladen/ (besucht am 22. 02. 2024).

[109] Alfred Schellenberg GmbH, *Funk-Lichtmodul*, 2024. Adresse: https://schellenberg-shop.de/funk-lichtmodul/21003 (besucht am 22. 02. 2024).

[110] Alfred Schellenberg GmbH, *Qcells Solarmodule*, 2024. Adresse: https://schellenberg-energieberatung.de/solar/produkte/#solarmodule (besucht am 22. 02. 2024).

[111] Alfred Schellenberg GmbH, *Qcells Speicher*, 2024. Adresse: https://schellenberg-energieberatung.de/solar/produkte/#speicher (besucht am 22. 02. 2024).

[112] Albrecht JUNG GmbH & Co. KG, *Raumthermostat (Heizen/Kühlen) 24 V, Schließer, AC 230 V*, 2024. Adresse: https://www.jung-group.com/de-DE/Abdeckung-fuer-Thermostat-alpinweiss/LS-1749-BF-WW (besucht am 22. 02. 2024).

[113] Albrecht JUNG GmbH & Co. KG, *Die JUNG HOME SCHUKO® Steckdosen*, 2024. Adresse: https://www.jung-group.com/de-DE/Produkte/Systeme/JUNG-HOME/JUNG-HOME-Steckdosen/ (besucht am 22. 02. 2024).

[114] Albrecht JUNG GmbH & Co. KG, *Beleuchtung*, 2024. Adresse: https://www.jung.de/at/637/loesungen/beleuchtung/ (besucht am 22. 02. 2024).

[115] Albrecht JUNG GmbH & Co. KG, *Jalousie- und Rollladensteuerung*, 2024. Adresse: https://www.jung.de/at/769/produkte/technik/jalousie-und-rollladensteuerung/ (besucht am 22. 02. 2024).

[116] Grant Hernandez, Orlando Arias, Daniel Buentello, Yier Jin, *Smart Nest Thermostat: A Smart Spy in Your Home*, 2024. Adresse: https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf (besucht am 08. 02. 2024).

[117] M. Moody und A. Hunter, „Exploiting known vulnerabilities of a smart thermostat“, in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, S. 50–53. DOI: 10.1109/PST.2016.7906936.

[118] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu und X. Fu, „Security vulnerabilities of internet of things: A case study of the smart plug system“, *IEEE Internet of Things Journal*, Jg. 4, Nr. 6, S. 1899–1909, 2017.

[119] A. Iqbal, J. Olegård, R. Ghimire, S. Jamshir und A. Shalaginov, „Smart Home Forensics: An Exploratory Study on Smart Plug Forensic Analysis“, in *2020 IEEE International Conference on Big Data (Big Data)*, 2020, S. 2283–2290. DOI: 10.1109/BigData50022.2020.9378183.

[120] F. E. Salamh, „A Forensic Analysis of Home Automation Devices (FAHAD) Model: Kasa Smart Light Bulb and Eufy Floodlight Camera as Case Studies“, 2021, S. 1–9. Adresse: https://api.semanticscholar.org/CorpusID:230534090.

[121] Bosch Thermotechnik GmbH, *Kontrollierte Wohnungslüftung*, 2024. Adresse: https://www.bosch-homecomfort.com/de/de/ocs/wohngebaeude/kontrollierte-wohnungslueftung-854504-c/ (besucht am 23. 02. 2024).

[122] Bosch Thermotechnik GmbH, *Multisplit-Klimageräte*, 2024. Adresse: https://www.bosch-homecomfort.com/de/de/ocs/wohngebaeude/multisplit-klimageraete-1150268-c/ (besucht am 23. 02. 2024).

[123] Robert Bosch Smart Home GmbH, *Twinguard Rauchwarnmelder*, 2024. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/twinguard/ (besucht am 23. 02. 2024).

[124] eQ-3 AG, *Homematic IP Wired CO2 Sensor mit Display*, 2024. Adresse: https://www.eq-3.de/presse/detail/luftqualitaet-ueberwachen-effizient-lueften-gesuender-wohnen.html (besucht am 23. 02. 2024).

[125] Vaillant Deutschland GmbH & Co. KG, *Zentrale Wohnraumlüftung recoVAIR – Wandgerät*, 2024. Adresse: https://www.vaillant.de/heizung/produkte/wohnraumluftung-recovair-wandgerate-966.html (besucht am 23. 02. 2024).

[126] Vaillant Deutschland GmbH & Co. KG, *Klimagerät climaVAIR exclusive*, 2024. Adresse: https://www.vaillant.de/heizung/produkte/klimagerat-climavair-exclusive-172672.html (besucht am 23. 02. 2024).

[127] Heizungsdiscount 24 GmbH, *Vaillant CO2-Luftqualitätssensor*, 2024. Adresse: https://www.heizungsdiscount24.de/wohnungslueftung/vaillant-co2-luftqualitaetssensor.html (besucht am 23. 02. 2024).

[128] Zehnder Group Deutschland GmbH, *Zehnder Lüftungsgeräte*, 2024. Adresse: https://www.zehnder-systems.de/de/zuhause-profi/produkte-zubehoer/produkte-wohnraumlueftung/lueftungsgeraete (besucht am 23. 02. 2024).

[129] Lüftungsland GmbH, *Zehnder CO2-Sensor RF 55 Unterputz*, 2024. Adresse: https://www.lueftungsland.de/de_DE/p/zehnder-co2-sensor-rf-55-inbouw/15688/ (besucht am 23. 02. 2024).

[130] Blauberg Ventilatoren GmbH, *Zentrale Lüftungsanlagen mit Wärmerückgewinnung*, 2024. Adresse: https://blaubergventilatoren.de/catalog/air-handling-units-with-heat-recovery (besucht am 23. 02. 2024).

[131] Blauberg Ventilatoren GmbH, *Blauberg DPWQ30600*, 2024. Adresse: https://blaubergventilatoren.de/series/dpwq30600 (besucht am 23. 02. 2024).

[132] Viessmann Climate Solutions SE, *Zentrale Lüftungsanlage: Funktion, Planung & Verlegung*, 2024. Adresse: https://www.viessmann.de/de/wissen/technik-und-systeme/zentrale-lueftungsanlage.html (besucht am 23. 02. 2024).

[133] Viessmann Climate Solutions SE, *Viessmann Klimaanlagen für Ihr Haus – ein Überblick*, 2024. Adresse: https://www.viessmann.de/de/wissen/technik-und-systeme/klimaanlage.html (besucht am 23. 02. 2024).

[134] Viessmann Climate Solutions SE, *ViCare CO2-Sensor*, 2024. Adresse: https://www.viessmann.de/de/produkte/steuerung-und-konnektivitaet/vicare-co2-sensor.html (besucht am 23. 02. 2024).

[135] TFA Dostmann GmbH & Co. KG, *Wetterstation WLAN*, 2024. Adresse: https://www.tfa-dostmann.de/produkte/wetterstationen/wetterstationen-wlan/ (besucht am 23. 02. 2024).

[136] TFA Dostmann GmbH & Co. KG, *CO2-Monitor AIRCO2NTROL UP Dual Beam 31.5010*, 2024. Adresse: https://www.tfa-dostmann.de/produkt/co2-monitor-airco2ntrol-up-dual-beam-31-5010/ (besucht am 23. 02. 2024).

[137] Bresser GmbH, *BRESSER 5-in-1 Comfort Wetterstation mit Farbdisplay*, 2024. Adresse: https://www.bresser.de/Wetter-Zeit/Wettercenter/BRESSER-5-in-1-Comfort-Wetterstation-mit-Farbdisplay.html (besucht am 23. 02. 2024).

[138] Bresser GmbH, *Sensoren*, 2024. Adresse: https://www.bresser.de/Wetter-Zeit/Zubehoer-bresser-1/Sensoren/ (besucht am 23. 02. 2024).

[139] STIEBEL ELTRON GmbH & Co. KG, *Zentrale Lüftungsanlage*, 2024. Adresse: https://www.stiebel-eltron.de/de/home/produkte-loesungen/erneuerbare_energien/lueftung/zentral.html (besucht am 23. 02. 2024).

[140] STIEBEL ELTRON GmbH & Co. KG, *Klimageräte – Alle Produkte*, 2024. Adresse: https://www.stiebel-eltron.de/de/home/produkte-loesungen/klima/klimageraete/alle-produkte.html (besucht am 23. 02. 2024).

[141] STIEBEL ELTRON GmbH & Co. KG, *189800 Stiebel Eltron FEQ*, 2024. Adresse: https://www.hte-shop.de/189800-Stiebel-Eltron-FEQ (besucht am 23. 02. 2024).

[142] Robert Bosch Smart Home GmbH, *Mehr Sicherheit: Smart Home Alarmsystem*, 2024. Adresse: https://www.bosch-smarthome.com/de/de/loesungen/sicher-leben/haus-schuetzen/ (besucht am 23. 02. 2024).

[143] Robert Bosch Smart Home GmbH, *Eyes Innenkamera II*, 2024. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/eyes-innenkamera/ (besucht am 23. 02. 2024).

[144] Robert Bosch Smart Home GmbH, *Eyes Außenkamera*, 2024. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/eyes-aussenkamera/ (besucht am 23. 02. 2024).

[145] Robert Bosch Smart Home GmbH, *Tür-/Fensterkontakt II (Plus)*, 2024. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/tuer-fensterkontakt/ (besucht am 23. 02. 2024).

[146] Robert Bosch Smart Home GmbH, *Smarter Bewegungsmelder*, 2024. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/bewegungsmelder/ (besucht am 23. 02. 2024).

[147] Robert Bosch Smart Home GmbH, *Twinguard Rauchwarnmelder*, 2024. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/twinguard/ (besucht am 23. 02. 2024).

[148] Robert Bosch Smart Home GmbH, *Smarter Wassermelder*, 2024. Adresse: https://www.bosch-smarthome.com/de/de/produkte/geraete/wassermelder/ (besucht am 23. 02. 2024).

[149] ABUS August Bremicker Söhne KG, *ABUS Alarmanlagen: Schutz für Ihr Haus & Hilfe im Notfall*, 2024. Adresse: https://www.abus.com/Sicherheit-Zuhause/Alarmanlagen (besucht am 23. 02. 2024).

[150] ABUS August Bremicker Söhne KG, *Alles im Blick*, 2024. Adresse: https://mobil.abus.com/de/Privat/Videoueberwachung/Heimwerker-Systeme/Kameras (besucht am 23. 02. 2024).

[151] ABUS August Bremicker Söhne KG, *Mehr Komfort an der Tür*, 2024. Adresse: https://mobil.abus.com/de/Privat/Tuersicherheit/Tuersprechsysteme (besucht am 23. 02. 2024).

[152] ABUS August Bremicker Söhne KG, *Smartes Türschloss*, 2024. Adresse: https://mobil.abus.com/de/Privat/Tuersicherheit/Tuerschlossantrieb-HomeTec-Pro-Bluetooth-R (besucht am 23. 02. 2024).

[153] ABUS August Bremicker Söhne KG, *ABUS Z-Wave Tür-/ Fensterkontakt*, 2024. Adresse: https://mobil.abus.com/de/Privat/Alarmsysteme/Smartvest-Funk-System/Z-Wave-Erweiterung/ABUS-Z-Wave-Tuer-Fensterkontakt (besucht am 23. 02. 2024).

[154] ABUS August Bremicker Söhne KG, *Smartvest Funk-Bewegungsmelder*, 2024. Adresse: https://mobil.abus.com/de/Privat/Smart-Home/DIY-Alarmanlage/Sensoren-Aktoren/Smartvest-Funk-Bewegungsmelder (besucht am 23. 02. 2024).

[155] ABUS August Bremicker Söhne KG, *CO-Warnmelder COWM510*, 2024. Adresse: https://mobil.abus.com/at/Privat/Brandschutz-Gefahrenmelder/Gaswarnmelder/Gaswarnmelder/CO-Warnmelder-COWM510 (besucht am 23. 02. 2024).

[156] ABUS August Bremicker Söhne KG, *Wassermelder*, 2024. Adresse: https://mobil.abus.com/de/Privat/Brandschutz-Gefahrenmelder/Wasserwarnmelder/Schutz-vor-Wasser/Wassermelder (besucht am 23. 02. 2024).

[157] INSTAR Deutschland GmbH, *INSTAR Onlineshop*, 2024. Adresse: https://www.instar.com/ (besucht am 23. 02. 2024).

[158] eQ-3 AG, *HomeMatic Funk-Tür-/Fensterkontakt, optisch*, 2024. Adresse: https://www.eq-3.de/produkte/homematic/detail/homematic-funk-tuer-fensterkontakt-optisch.html (besucht am 23. 02. 2024).

[159] eQ-3 AG, *HomeMatic Funk-Bewegungsmelder, innen*, 2024. Adresse: https://www.eq-3.de/produkte/homematic/detail/homematic-funk-bewegungsmelder-innen.html (besucht am 23. 02. 2024).

[160] eQ-3 AG, *HomeMatic Funk-Bewegungsmelder, außen*, 2024. Adresse: https://www.eq-3.de/produkte/homematic/detail/homematic-funk-bewegungsmelder-aussen.html (besucht am 23. 02. 2024).

[161] eQ-3 AG, *HomeMatic Funk-Rauchwarnmelder*, 2024. Adresse: https://www.eq-3.de/produkte/homematic/detail/homematic-funk-rauchwarnmelder.html (besucht am 23. 02. 2024).

[162] BURG-WÄCHTER KG, *Videosicherheit*, 2024. Adresse: https://burg.biz/collections/videosicherheit (besucht am 23. 02. 2024).

[163] BURG-WÄCHTER KG, *DOOR eGUARD Video Bell DG8500*, 2024. Adresse: https://burg.biz/products/door-eguard-video-bell-dg8500 (besucht am 23. 02. 2024).

[164] BURG-WÄCHTER KG, *Elektronisches Türschloss*, 2024. Adresse: https://burg.biz/collections/tuerschlosselektronik (besucht am 23. 02. 2024).

[165] BURG-WÄCHTER KG, *BURGsmart Protect CONTACT 2032*, 2024. Adresse: https://burg.biz/products/burgsmart-protect-contact-2032 (besucht am 23. 02. 2024).

[166] BURG-WÄCHTER KG, *BURGsmart Protect MOTION 2012*, 2024. Adresse: https://burg.biz/products/burgsmart-protect-motion-2012 (besucht am 23. 02. 2024).

[167] BURG-WÄCHTER KG, *BURGsmart Protect WATER 2062*, 2024. Adresse: https://burg.biz/products/burgsmart-protect-water-2062 (besucht am 23. 02. 2024).

[168] Busch-Jaeger Elektro GmbH, *Dome-Kamera Externe analoge Kamera für die Türsprechanlage*, 2024. Adresse: https://www.busch-jaeger.de/online-katalog/detail/2CKA008300A0488 (besucht am 23. 02. 2024).

[169] Busch-Jaeger Elektro GmbH, *Busch-Welcome®*, 2024. Adresse: https://www.busch-jaeger.de/systeme/busch-welcome (besucht am 23. 02. 2024).

[170] Busch-Jaeger Elektro GmbH, *Busch-AccessControl*, 2024. Adresse: https://www.busch-jaeger.de/systeme/busch-accesscontrol (besucht am 23. 02. 2024).

[171] Busch-Jaeger Elektro GmbH, *Fenstermelder*, 2024. Adresse: https://www.busch-jaeger.de/produkt/fenstermelder (besucht am 23. 02. 2024).

[172] Busch-Jaeger Elektro GmbH, *Bewegungs- und Präsenzmelder*, 2024. Adresse: https://www.busch-jaeger.de/produkt/kategorie/bewegungs-praesenzmelder (besucht am 23. 02. 2024).

[173] Busch-Jaeger Elektro GmbH, *Busch-CO Alarm*, 2024. Adresse: https://www.busch-jaeger.de/produkt/busch-co-alarm (besucht am 23. 02. 2024).

[174] Busch-Jaeger Elektro GmbH, *SWM4/RN Wassermelder mit Relais für 12 V*, 2024. Adresse: https://www.busch-jaeger.de/online-katalog/detail/GHQ4030001R0012 (besucht am 23. 02. 2024).

[175] Giersiepen GmbH & Co. KG, *Sicherheit für Ihr Zuhause*, 2024. Adresse: https://www.gira.de/produkte/sicherheit# (besucht am 23. 02. 2024).

[176] Giersiepen GmbH & Co. KG, *Externe Kamera*, 2024. Adresse: https://katalog.gira.de/de_DE/datenblatt.html?id=687630 (besucht am 23. 02. 2024).

[177] Giersiepen GmbH & Co. KG, *Türsprechanlagen von Gira*, 2024. Adresse: https://www.gira.de/produkte/tuersprechanlagen (besucht am 23. 02. 2024).

[178] Giersiepen GmbH & Co. KG, *Gira Keyless In*, 2024. Adresse: https://www.gira.de/produkte/tuersprechanlagen/gira-keyless-in# (besucht am 23. 02. 2024).

[179] Giersiepen GmbH & Co. KG, *Tür- bzw. Fensterkontakt*, 2024. Adresse: https://katalog.gira.de/de_DE/datenblatt.html?id=636908 (besucht am 23. 02. 2024).

[180] Giersiepen GmbH & Co. KG, *Gira Bewegungsmelder*, 2024. Adresse: https://www.gira.de/produkte/lichtsteuerung/gira-bewegungsmelder#vorteile (besucht am 23. 02. 2024).

[181] Giersiepen GmbH & Co. KG, *Gira Rauchmelder*, 2024. Adresse: https://www.gira.de/produkte/sicherheit/gira-rauchmelder#hoechste-qualtitaet (besucht am 23. 02. 2024).

[182] Giersiepen GmbH & Co. KG, *Leckagesensor*, 2024. Adresse: https://katalog.gira.de/de_DE/datenblatt.html?id=771703 (besucht am 23. 02. 2024).

[183] Blockalarm GmbH, *Beste Alarmanlage fürs Haus, Wohnung, Firma und Gewerbe*, 2024. Adresse: https://www.blockalarm.de/alarmanlage/ (besucht am 23. 02. 2024).

[184] Blockalarm GmbH, *Überwachungskameras von BLOCKALARM®*, 2024. Adresse: https://www.blockalarm.de/ueberwachungskameras/ (besucht am 23. 02. 2024).

[185] Blockalarm GmbH, *Komfort ohne Schlüssel*, 2024. Adresse: https://www.blockalarm.de/transponder/ (besucht am 23. 02. 2024).

[186] Blockalarm GmbH, *Öffnungsmelder für Fenster und Türen*, 2024. Adresse: https://www.blockalarm.de/alarmanlage/einbruchschutz/funk-oeffnungsmelder/ (besucht am 23. 02. 2024).

[187] Blockalarm GmbH, *Bewegungsmelder als Einbruchschutz*, 2024. Adresse: https://www.blockalarm.de/alarmanlage/einbruchschutz/bewegungsmelder/ (besucht am 23. 02. 2024).

[188] Blockalarm GmbH, *Kohlenmonoxid Melder / CO-Alarm Funk*, 2024. Adresse: https://www.blockalarm.de/brandschutz/co-melder/ (besucht am 23. 02. 2024).

[189] Blockalarm GmbH, *Wassermelder für Haus und Keller*, 2024. Adresse: https://www.blockalarm.de/brandschutz/funk-wassermelder-haus/ (besucht am 23. 02. 2024).

[190] S. Hutchinson und U. Karabiyik, „Forensic Analysis of the August Smart Device Ecosystem“, in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 2020, S. 1–7. DOI: 10.1109/ISNCC49221.2020.9297346.

[191] Lautsprecher Teufel GmbH, *Gut vernetzt Smart Speaker*, 2024. Adresse: https://teufel.de/wlan-lautsprecher/smart-speaker (besucht am 23. 02. 2024).

[192] Loewe Technology GmbH, *Alle Fernseher Modell-Serien*, 2024. Adresse: https://www.loewe.de/alleFernseher (besucht am 23. 02. 2024).

[193] Loewe Technology GmbH, *Multiroom Sound*, 2024. Adresse: https://www.loewe.de/de/audio/soundbar-loewe/multiroom-lautsprecher (besucht am 23. 02. 2024).

[194] MEDION AG, *Smart-TVs*, 2024. Adresse: https://www.medion.com/de/shop/smart-tv (besucht am 23. 02. 2024).

[195] MEDION AG, *LIFE® P61142 WLAN Lautsprecher mit Amazon Alexa*, 2024. Adresse: https://www.medion.com/de/shop/p/bluetooth-lautsprecher-medion-life-p61142-wlan-lautsprecher-mit-amazon-alexa-spotify-connect-wlan-bluetooth--multiroom-party-mode-dlna-kabellose-musikuebertragung-2-x-10-w-rms-50060455A1 (besucht am 23. 02. 2024).

[196] MEDION AG, *LIFE® P86366 Webcam*, 2024. Adresse: https://www.medion.com/de/shop/p/pc-zubehoer-medion-life-p86366-webcam-fhd-videoaufloesung-mit-30-bildern-sek--integr-mikrofon-fotomodus-autofokus-inklusive-belichtungskontrolle-flexibel-aufstellbar-plug--play-50066857A1 (besucht am 23. 02. 2024).

[197] MEDIA SOCIETY NETWORKS, *MEDION® LifeCloud® P89634 MD86783*, 2024. Adresse: https://plusxaward.de/portfolio/medion-lifecloud-p89634-md86783/ (besucht am 23. 02. 2024).

[198] Beko Grundig Deutschland GmbH, *TV*, 2024. Adresse: https://www.grundig.com/de-de/produkte/entertainment-tv (besucht am 23. 02. 2024).

[199] Metz Consumer Electronics GmbH, *Produktfinder -Alles auf einen Blick*, 2024. Adresse: https://metz-ce.de/fernseher/produktfinder (besucht am 23. 02. 2024).

[200] Sennheiser electronic SE & Co. KG, *TeamConnect Intelligent Speaker*, 2024. Adresse: https://www.sennheiser.com/de-de/product-families/tcisp (besucht am 23. 02. 2024).

[201] A. Kapoor und S. R. Qureshi, „Forensic Analysis of digital evidence extracted from Amazon Echo“, in *2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI)*, IEEE, 2020, S. 1–7.

[202] X. Liu, A. Li, X. Fu, B. Luo, X. Du und M. Guizani, „Understanding Digital Forensic Characteristics of Smart Speaker Ecosystems“, in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, S. 1–6. DOI: 10.1109/GLOBECOM46510.2021.9685816.

[203] D. Oladimeji und B. Zhou, „Forensic Analysis of Amazon Alexa Echo Dot 4th Generation“, in *2022 IEEE International Conference on Big Data (Big Data)*, 2022, S. 3053–3062. DOI: 10.1109/BigData55660.2022.10020328.

[204] A. Akinbi und T. Berry, „Forensic investigation of google assistant“, *SN Computer Science*, Jg. 1, Nr. 5, S. 1–10, 2020.

[205] A. Bhardwaj, K. Kaushik, S. Bharany und S. Kim, „Forensic analysis and security assessment of IoT camera firmware for smart homes“, *Egyptian Informatics Journal*, Jg. 24, Nr. 4, S. 4–13, 2023.

[206] Space Technologies GmbH, *ViFit Run connect Activity Tracker*, 2024. Adresse: https://www.medisana.de/Mobile-Gesundheit/Connect-Geraete/ViFit-Run-connect-Activity-Tracker.html (besucht am 25. 02. 2024).

[207] Space Technologies GmbH, *BS 450 connect Körperanalysewaage schwarz*, 2024. Adresse: https://www.medisana.de/Mobile-Gesundheit/Connect-Geraete/BS-450-connect-Koerperanalysewaage-schwarz.html (besucht am 25. 02. 2024).

[208] Space Technologies GmbH, *BU 580 connect Oberarm-Blutdruckmessgerät*, 2024. Adresse: https://www.medisana.de/Mobile-Gesundheit/Connect-Geraete/BU-580-connect-Oberarm-Blutdruckmessgeraet.html (besucht am 25. 02. 2024).

[209] S. T. GmbH, *MediTouch 2 connect dual Blutzuckermessgerät*, Aufruf: 25.02.2024. Adresse: https://www.medisana.de/Mobile-Gesundheit/Connect-Geraete/MediTouch-2-connect-dual-Blutzuckermessgeraet-inkl-Starterset-medisana.html.

[210] Space Technologies GmbH, *Sleepace Schlafmonitor*, 2024. Adresse: https://www.medisana.de/Angebote/Sleepace-Schlafmonitor.html (besucht am 25. 02. 2024).

[211] Beurer GmbH, *Sport und Aktivität von Beurer*, 2024. Adresse: https://www.beurer.com/web/de/produkte/active/sport-und-aktivitaet/ (besucht am 25. 02. 2024).

[212] Beurer GmbH, *Diagnosewaagen von Beurer*, 2024. Adresse: https://www.beurer.com/web/de/produkte/wellbeing/gewicht-und-diagnose/diagnosewaagen/ (besucht am 25. 02. 2024).

[213] Beurer GmbH, *Oberarm-Blutdruckmessgeräte von Beurer*, 2024. Adresse: https://www.beurer.com/web/de/produkte/medical/blutdruck/oberarm-blutdruckmessgeraete/ (besucht am 25. 02. 2024).

[214] Beurer GmbH, *Beurer Blutzuckermessgerät GL 49 mg/dL*, 2024. Adresse: https://www.beurer-shop.de/p/beurer-blutzuckermessgeraet-gl-49-mg-dl/ (besucht am 25. 02. 2024).

[215] Beurer GmbH, *Beurer Schlafsensor - SE 80 SleepExpert*, 2024. Adresse: https://snorflex.de/produkt/beurer-schlafsensor-se-80-sleepexpert/ (besucht am 25. 02. 2024).

[216] Leifheit AG, *Fitness-Tracker*, 2024. Adresse: https://www.leifheit.de/de-de/soehnle/fitness-tracker/17304 (besucht am 25. 02. 2024).

[217] Leifheit AG, *Connect-Körperanalysewaage Shape Sense Connect 200 mit Bluetooth*, 2024. Adresse: https://www.leifheit.de/de-de/soehnle/connect-personenwaagen/17299/connect-koerperanalysewaage-shape-sense-connect-200-mit-bluetooth%c2%ae/63873 (besucht am 25. 02. 2024).

[218] Leifheit AG, *Connect-Blutdruckmessgeräte*, 2024. Adresse: https://www.leifheit.de/de-de/soehnle/connect-blutdruckmessgeraete/17290 (besucht am 25. 02. 2024).

[219] S. Kang, S. Kim und J. Kim, „Forensic analysis for IoT fitness trackers and its application“, *Peer-to-Peer Networking and Applications*, Jg. 13, S. 564–573, 2020.

[220] A. Almogbil, A. Alghofaili, C. Deane, T. Leschke, A. Almogbil und A. Alghofaili, „Digital Forensic Analysis of Fitbit Wearable Technology: An Investigator's Guide“, in *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2020, S. 44–49. DOI: 10.1109/CSCloud-EdgeCom49738.2020.00017.

[221] F. Hantke und A. Dewald, „How can data from fitness trackers be obtained and analyzed with a forensic approach?“, in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2020, S. 500–508. DOI: 10.1109/EuroSPW51379.2020.00073.

[222] Robert Bosch Hausgeräte GmbH, *i-DOS: intelligente Waschmaschinen mit Dosierautomatik*, 2024. Adresse: https://www.bosch-home.com/de/produkte/waschen-trocknen/waschmaschinen/i-dos-waschmaschinen (besucht am 25. 02. 2024).

[223] Robert Bosch Hausgeräte GmbH, *Wäschetrockner*, 2024. Adresse: https://www.bosch-home.com/de/produkte/waschen-trocknen/waeschetrockner (besucht am 25. 02. 2024).

[224] Robert Bosch GmbH, *Mit dem KI-Backofen zum perfekten Kuchen*, 2024. Adresse: https://www.bosch.com/de/stories/smarter-backofen/ (besucht am 25. 02. 2024).

[225] Robert Bosch Hausgeräte GmbH, *Nutze die Intelligenz deines Geschirrspülers*, 2024. Adresse: https://www.bosch-home.com/de/produkte/geschirrspueler/intelligenter-geschirrspueler (besucht am 25. 02. 2024).

[226] Robert Bosch Hausgeräte GmbH, *Smarter Kühlschrank – so kühlen wir morgen*, 2024. Adresse: https://www.bosch-home.com/de/bosch-erleben/magazin/haushaltstipps/smart-kuehlschrank (besucht am 25. 02. 2024).

[227] Robert Bosch GmbH, *Roxxter: Fünf Gründe, warum Staubsaugen jetzt Spaß macht*, 2024. Adresse: https://www.bosch.com/de/stories/intelligente-saugroboter/ (besucht am 25. 02. 2024).

[228] Robert Bosch Power Tools GmbH, *Die Bosch Mähroboter*, 2024. Adresse: https://www.bosch-diy.com/de/de/gartengeraete/maehroboter (besucht am 25. 02. 2024).

[229] SEG Hausgeräte GmbH, *Was ist i-Dos?*, 2024. Adresse: https://www.siemens-home.bsh-group.com/de/produkte/waeschepflege/idos (besucht am 25. 02. 2024).

[230] SEG Hausgeräte GmbH, *Trockner*, 2024. Adresse: https://www.siemens-home.bsh-group.com/de/produkte/waeschepflege/trockner (besucht am 25. 02. 2024).

[231] SEG Hausgeräte GmbH, *Steuere deine Siemens Hausgeräte auf die clevere Art – mit Home Connect*, 2024. Adresse: https://www.siemens-home.bsh-group.com/de/inspiration/innovation/home-connect/vernetzte-hausgeraete/backen (besucht am 25. 02. 2024).

[232] SEG Hausgeräte GmbH, *Home Connect: Geschirrspüler vernetzen*, 2024. Adresse: https://www.siemens-home.bsh-group.com/de/inspiration/innovation/home-connect/vernetzte-hausgeraete/spuelen (besucht am 25. 02. 2024).

[233] SEG Hausgeräte GmbH, *Home Connect: Kühlschränke vernetzen*, 2024. Adresse: https://www.siemens-home.bsh-group.com/de/inspiration/innovation/home-connect/vernetzte-hausgeraete/kuehlen (besucht am 25. 02. 2024).

[234] Electrolux Hausgeräte GmbH, *AEG Smart Home - Wäschepflege*, 2024. Adresse: https://www.aeg.de/about-aeg/connectivity-hub/#732729 (besucht am 25. 02. 2024).

[235] Electrolux Hausgeräte GmbH, *AEG Smart Home - Backofen*, 2024. Adresse: https://www.aeg.de/about-aeg/connectivity-hub/#732728 (besucht am 25. 02. 2024).

[236] Electrolux Hausgeräte GmbH, *Erfahre mehr über unsere Geschirrspüler*, 2024. Adresse: https://www.aeg.de/taste/discover/buying-guides/dishwashers/#1224596 (besucht am 25. 02. 2024).

[237] Electrolux Hausgeräte GmbH, *Kühlschränke*, 2024. Adresse: https://www.aeg.de/kitchen/cooling/refrigerators/ (besucht am 25. 02. 2024).

[238] Electrolux Hausgeräte GmbH, *Saugroboter*, 2024. Adresse: https://www.aeg.de/vacuums-home-comfort/vacuum-cleaners/robotic-vacuum-cleaners/ (besucht am 25. 02. 2024).

[239] Alfred Kärcher Vertriebs-GmbH, *Wisch- und Saugroboter*, 2024. Adresse: https://www.kaercher.com/de/home-garden/saugroboter.html (besucht am 25. 02. 2024).

[240] Vorwerk Deutschland Stiftung & Co. KG, *Kobold VR7 Saugroboter mit RB7 Absaugstation*, 2024. Adresse: https://www.vorwerk.com/de/de/c/home/produkte/kobold/kobold-vr7-saugroboter (besucht am 25. 02. 2024).

[241] STIHL Vertriebszentrale AG & Co. KG, *Mähroboter iMOW 5*, 2024. Adresse: https://www.stihl.de/de/p/maehroboter-maehroboter-imow%C2%AE-5-164626#imow%25C2%25AE-5-164626 (besucht am 25. 02. 2024).

[242] Miele Vertriebsgesellschaft Deutschland KG, *Miele Hausgeräte im Smart Home*, 2024. Adresse: https://www.miele.de/c/smart-home-integration-3187.htm (besucht am 25. 02. 2024).

[243] Miele Vertriebsgesellschaft Deutschland KG, *Kochen auf dem nächsten Level mit künstlicher Intelligenz*, 2024. Adresse: https://www.miele.de/de/m/kochen-auf-dem-naechsten-level-mit-kuenstlicher-intelligenz-5368.htm (besucht am 25. 02. 2024).

[244] Miele Vertriebsgesellschaft Deutschland KG, *K 7433 E*, 2024. Adresse: https://www.miele.de/e/einbau-kuehlschrank-k-7433-e-11641270-p (besucht am 25. 02. 2024).

[245] Miele Vertriebsgesellschaft Deutschland KG, *Saugroboter*, 2024. Adresse: `https://www.miele.de/e/saugroboter-1016471-c` (besucht am 25. 02. 2024).

[246] H. Zhou, L. Deng, W. Xu, W. Yu, J. Dehlinger und S. Chakraborty, „Towards Internet of Things (IoT) Forensics Analysis on Intelligent Robot Vacuum Systems“, in *2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications (SERA)*, IEEE, 2022, S. 91–98.

Eidesstattliche Erklärung

Hiermit versichere ich – Max Führer – an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Mittweida, 10. März 2024 [redacted]

Ort, Datum Max Führer