Abschlussbericht
KI-gestützte Anomalieerkennung für Smart Homes (KIASH)

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) unter dem Förderkennzeichen 16KIS1612K gefördert.

Sachbericht (Teil II) für den Verwendungsnachweis der KOBIL GmbH

Projektpartner

Nr.	Name des Partners	Art des Partners
1.	**KOBIL GmbH – Sicherheitstechnologien [KOBIL]**	KMU
2.	August-Wilhelm Scheer Institut für digitale Produkte und Prozesse gGmbH [AWSi]	Verband / KMU
3.	eBusiness-Kompetenz Zentrum gGmbH [eBZ]	Verband / KMU
4.	Cleopa GmbH [Cleopa]	KMU
5.	Hochschule Worms – University of Applied Sciences – Zentrum für Technologie und Transfer [HS Worms]	Forschung
6.	TU Chemnitz - Professur für Privatrecht und Recht des geistigen Eigentums [TUC]	Forschung

Gefördert durch:

Bundesministerium für Forschung, Technologie und Raumfahrt

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

1 Kurzdarstellung des KIASH-Projektes 3
1.1 Motivation und Ausgangslage 3
1.2 Bezug zu förderpolitischen Zielen 3
1.3 Technologische und wissenschaftliche Ausgangslage 4
1.4 Zielsetzung des Projekts 4
1.5 Relevanz und Innovationshöhe 5
1.6 Bedeutung im Forschungskontext 5
1.7 Der Beitrag von KOBIL zum Projekt 6
2 Ablauf des Vorhabens 7
2.1 Vorgehen 7
2.2 Zusammenarbeit intern und extern des Konsortiums 8
2.2.1 Zuständigkeiten im Konsortium 8
2.2.2 Austausch innerhalb des Konsortiums 9
2.2.3 Projektexterne Stakeholder 9
2.3 Tätigkeiten und Ergebnisse in den einzelnen Arbeitspaketen 9
2.3.1 AP1 – Anforderungsanalyse 9
2.3.2 AP2 – ML-basierte Anomalieerkennung auf heterogenen IoT-Daten 9
2.3.3 AP3 – Betrachtung juristischer Aspekte 11
2.3.4 AP4 – Umsetzung Cloud-Service und Enduser-App 12
2.3.5 AP5 – Umsetzung des Demonstrators und der KIASH-Security-Box 16
2.3.6 AP6 – Pilotphase, Demonstrator-Optimierung, Weiterbildung und Zertifizierung 18
2.3.7 AP7 – Normung und Öffentlichkeitsarbeit 18
3 Zahlenmäßiger Nachweis 19
4 Ergebnisse 20
4.1 Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten 20
4.2 Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse 20
4.3 Fortschritte anderer Akteure während der Projektlaufzeit 21
4.4 Gesamtbewertung 21
5 Literaturverzeichnis 22
6 Abbildungsverzeichnis 23
7 Anhang 24

1 Kurzdarstellung des KIASH-Projektes

1.1 Motivation und Ausgangslage

Die zunehmende Digitalisierung und Vernetzung in privaten Wohnumgebungen führt zu einer stetig wachsenden Zahl vernetzter Geräte, vom intelligenten Thermostat bis zur sprachgesteuerten Leuchte. Diese Entwicklung verspricht Komfort, Energieeffizienz und neue Geschäftsmodelle, birgt aber zugleich erhebliche Sicherheitsrisiken. Studien zeigen, dass rund 16,7 % der deutschen Haushalte mindestens ein unsicheres IoT-Gerät besitzen, über das Angreifer Zugriff auf das gesamte Heimnetzwerk erlangen können [1, 2]. Neben klassischen IT-Systemen werden damit auch Kühlschränke, Lichtsysteme oder Heizungen zu potenziellen Einfallstoren für Cyberangriffe.

Gleichzeitig fehlt es kleinen und mittleren Unternehmen (KMU) im Handwerks- und Installationssektor an Ressourcen und Know-how, um diese Sicherheitsprobleme eigenständig zu adressieren. Sie stehen vor der Herausforderung, digitale Dienstleistungen anzubieten, ohne über tiefgehende Expertise in IT-Security oder Künstlicher Intelligenz (KI) zu verfügen.

Das Forschungsprojekt KIASH (KI-gestützte Anomalieerkennung für Smart Homes) setzt genau hier an: Ziel war die Entwicklung eines Systems, das es Handwerksbetrieben ermöglicht, ihren Kunden ein intelligentes, datenschutzkonformes Sicherheits-Monitoring bereitzustellen. Im Zentrum steht die KIASH-Security-Box, ein im Rahmen dieses Projekts entwickeltes, DSGVO-konformes Gerät, das Anomalien im Smart Home erkennt, bewertet und über eine Cloudplattform mit weiteren Diensten verbindet.

Damit leistet KIASH einen Beitrag zur Stärkung des Innovationspotenzials von KMU und zur Umsetzung der Hightech-Strategie 2025 der Bundesregierung [3], die auf die Verbindung von Spitzenforschung, Digitalisierung und gesellschaftlicher Wirkung zielt.

1.2 Bezug zu förderpolitischen Zielen

Das KIASH-Projekt leistete einen wesentlichen Beitrag zur Erreichung der förderpolitischen Ziele des Bundesministeriums für Bildung und Forschung (BMBF) sowie zur Umsetzung der Hightech-Strategie 2025 der Bundesregierung. Im Zentrum stand die Stärkung des Innovationspotenzials kleiner und mittlerer Unternehmen (KMU) im Bereich der Spitzenforschung sowie die Förderung des Transfers wissenschaftlicher Erkenntnisse in die wirtschaftliche Anwendung.

Durch die im Projekt durchgeführten industriellen Forschungs- und Entwicklungsarbeiten adressierte KIASH den Förderschwerpunkt „Informations- und Kommunikationstechnologien (IKT)“ und konzentrierte sich dabei auf zukunftsweisende Technologiebereiche wie Datenwissenschaft, Informationstechnologien, Industrie 4.0, Kommunikationssysteme und IT-Sicherheit. Darüber hinaus wurden Themen wie intelligente Netzwerktechnologien, Datenschutz und Privatsphäre sowie effizientes Datenmanagement aufgegriffen.

Das Hauptziel bestand darin, KMU bei der Beschleunigung des Technologietransfers aus der Forschung in marktfähige Anwendungen zu unterstützen. Die beteiligten Unternehmen bauten hierfür sowohl ihre eigenen Forschungsaktivitäten aus als auch enge Kooperationsstrukturen mit Hochschulen, Forschungseinrichtungen und weiteren Industriepartnern auf. Diese interdisziplinäre Zusammenarbeit bildete die Grundlage für einen funktionierenden Wissens- und Technologietransfer, der es den beteiligten KMU ermöglichte, neue Marktchancen im IKT-Sektor zu erschließen und ihre Wettbewerbsfähigkeit nachhaltig zu stärken.

Im Verlauf des Projekts zeigte sich, dass die Umsetzung dieser Ziele mit technischen und organisatorischen Herausforderungen verbunden war. Insbesondere die Entwicklung einer verlässlichen Anomalieerkennung auf Basis von Federated Learning erwies sich aufgrund der Heterogenität von Smart-Home-Systemen und Nutzerverhalten als anspruchsvoll. Weitere Risiken ergaben sich aus datenschutzrechtlichen Anforderungen (DSGVO), leistungsbeschränkten Schnittstellen (z. B. SMGW) sowie der Notwendigkeit, Geschäftsmodelle für Federated-Learning-basierte Systeme wirtschaftlich tragfähig zu gestalten.

Trotz dieser Herausforderungen trug das Projekt dazu bei, neue Erkenntnisse über die technische Umsetzbarkeit, wirtschaftliche Verwertbarkeit und datenschutzgerechte Anwendung von KI-Technologien in vernetzten Systemen zu gewinnen. Damit leistet KIASH einen wertvollen Beitrag zur Stärkung der technologischen Souveränität und Innovationskraft deutscher KMU im Bereich der Informations- und Kommunikationstechnologien.

1.3 Technologische und wissenschaftliche Ausgangslage

Die Sicherheitslage im Smart-Home-Umfeld ist von einer hohen Heterogenität geprägt. Geräte verschiedener Hersteller kommunizieren über unterschiedliche Protokolle, meist ohne einheitliche Sicherheitsstandards. Kommerzielle Lösungen bieten bislang oft nur heuristische Erkennungsverfahren oder signaturbasierte Ansätze, die weder anpassungsfähig noch hinreichend robust gegenüber neuartigen Angriffen sind.

Ein weiteres Defizit liegt im fehlenden Gerätepersönlichkeits-Fingerprinting – also der eindeutigen Identifikation von Firmware- und Konfigurationsständen einzelner Geräte. Diese Information ist jedoch entscheidend, um den Sicherheitsstatus eines Smart Homes zu bewerten. Bestehende Ansätze (z. B. PingPong [4] oder HomeSnitch [5]) beschränken sich auf die Erkennung einzelner Geräteaktionen, ohne Firmware- oder Konfigurationsdetails zu erfassen.

Parallel dazu gewinnt das Konzept des Federated Learning an Bedeutung. Es erlaubt das Training von KI-Modellen über verteilte Datenquellen hinweg, ohne dass Rohdaten die private Domäne verlassen müssen. Projekte wie IOTFLA [6] oder HAWatcher [7] zeigen, dass verteiltes Lernen in Smart-Home-Szenarien prinzipiell möglich ist, lassen jedoch zentrale Anforderungen offen – insbesondere hinsichtlich GAIA-X-Kompatibilität, Datensouveränität und wirtschaftlicher Nutzbarkeit für Handwerksbetriebe.

KIASH schließt diese Lücke, indem es eine eigene Cloudplattform mit einer lokalen Anomalieerkennung kombiniert. Durch den Einsatz von Federated Learning können die Modelle der einzelnen Haushalte zu einem Gesamtmodell aggregiert werden, ohne dass personenbezogene Daten übertragen werden. Damit verbindet KIASH aktuelle Forschung im maschinellen Lernen mit den Prinzipien von „Privacy by Design“ und „Security by Design“.

1.4 Zielsetzung des Projekts

Ziel des Projekts war die Entwicklung eines skalierbaren, datenschutzkonformen und praxistauglichen KI-Systems zur Anomalieerkennung in Smart-Home-Netzwerken. Dieses sollte sowohl technische als auch organisatorische Lücken zwischen Forschung, Handwerk und Endanwendern schließen.

Die Kernziele lassen sich wie folgt zusammenfassen:

- Entwicklung der KIASH-Security-Box: eine Hardware-/Software-Komponente zur Überwachung von IoT-Geräten im Smart Home, basierend auf sicherer KOBIL-Technologie.
- Realisierung einer Cloudplattform, die zentrale Dienste zur Verwaltung und Aggregation von KI-Modellen bereitstellt.
- Implementierung von KI-Verfahren zur lokalen Anomalieerkennung auf Basis heterogener IoT-Daten und zur Aggregation im Federated-Learning-Verbund.
- Entwicklung einer Enduser-App für Installation, Steuerung und Visualisierung, die eine intuitive Bedienung ohne technische Vorkenntnisse ermöglicht.
- Aufbau eines Schulungs- und Zertifizierungsmodells für Handwerksbetriebe und Endanwender, um Qualität, Sicherheit und Nachhaltigkeit der Anwendung sicherzustellen.
- Erstellung eines Leitfadens für die Anwendung von KI-basierten Sicherheitslösungen im Smart-Home-Umfeld, um den Wissenstransfer in Wirtschaft und Normung zu fördern.

Damit verfolgt KIASH ein interdisziplinäres Zielsystem, das technologische Innovation mit wirtschaftlicher Verwertbarkeit und gesellschaftlicher Akzeptanz verbindet.

1.5 Relevanz und Innovationshöhe

KIASH weist gegenüber bisherigen Ansätzen mehrere Alleinstellungsmerkmale auf:

Ganzheitlicher Ansatz

– Kombination von Hardware, Cloud, App und Schulungskonzept in einem DSGVO-konformen Gesamtsystem.

Federated Learning

– Verknüpfung von lokaler Datenverarbeitung und europäischer Cloud-Infrastruktur, wodurch Datenschutz und Skalierbarkeit vereint werden.

Praxisfokus auf KMU und Handwerk

– Einbeziehung von Handwerksbetrieben als zentrale Akteure der Wertschöpfungskette; Entwicklung neuer digitaler Geschäftsmodelle.

Starker Sicherheits- und Rechtsrahmen

– Juristische Begleitung durch die TU Chemnitz gewährleistete die Einhaltung von Datenschutzrecht, Datenwirtschaftsrecht und IT-Sicherheitsgesetz 2.0.

Normungs- und Transferorientierung

– Ergebnisse fließen in DIN SPEC-Aktivitäten (u. a. Privacy by Blockchain Design) und in einen öffentlichen Leitfaden zur Anwendung von KI-Sicherheitskonzepten ein.

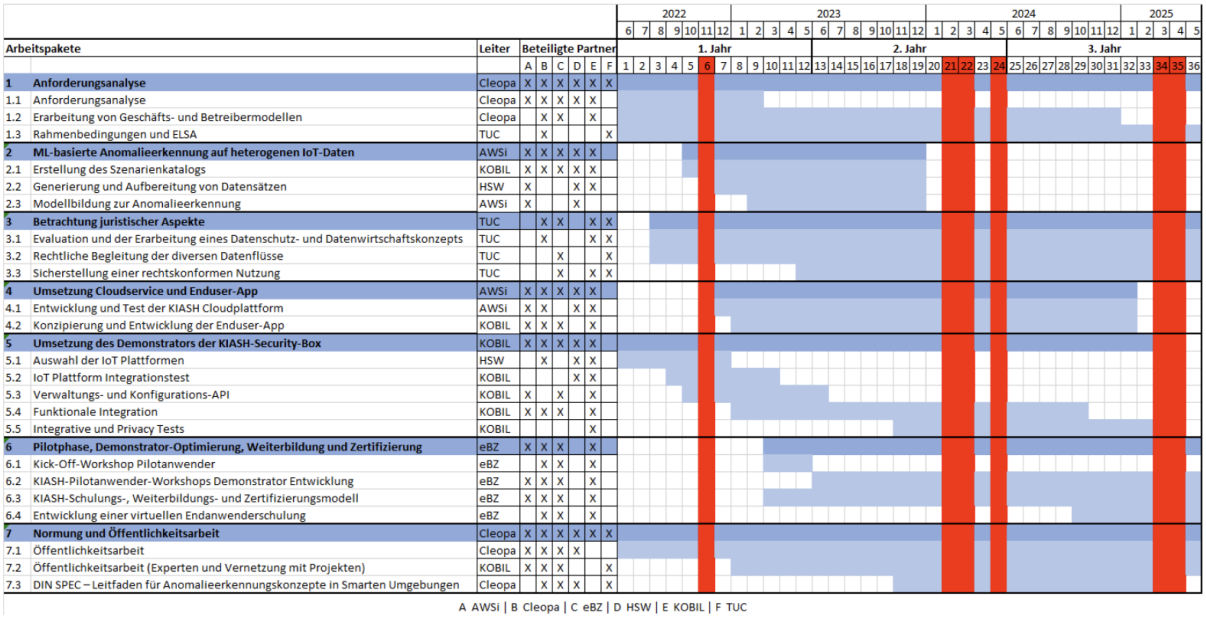
1.6 Bedeutung im Forschungskontext

Mit der Verbindung von KI-gestützter Anomalieerkennung, Datensouveränität und GAIA-X-Integration leistet KIASH einen Beitrag zur nationalen Digitalstrategie und zu europäischen Initiativen für vertrauenswürdige KI. Es adressiert aktuelle Forschungsthemen aus den Bereichen Edge Computing, IoT-Sicherheit, Federated Learning, Privacy Engineering und Mensch-Technik-Interaktion.

Darüber hinaus trägt das Projekt zur Standardisierung und Skalierbarkeit von Sicherheitslösungen bei, indem es ein reproduzierbares Referenzmodell für den sicheren

Einsatz von KI im Smart-Home-Sektor entwickelt. Damit entsteht eine Basis für künftige Forschungs- und Industrievorhaben, etwa im Kontext von Smart Cities oder energieeffizienten Gebäuden.

1.7 Der Beitrag von KOBIL zum Projekt



Arbeitspakete		Leiter	Beteiligte Partner					
			A	B	C	D	E	F
1	**Anforderungsanalyse**	Cleopa	X	X	X	X	X	X
1.1	Anforderungsanalyse	Cleopa	X	X	X	X	X	
1.2	Erarbeitung von Geschäfts- und Betreibermodellen	Cleopa		X	X		X	
1.3	Rahmenbedingungen und ELSA	TUC		X				X
2	**ML-basierte Anomalieerkennung auf heterogenen IoT-Daten**	AWSi	X	X	X	X	X	
2.1	Erstellung des Szenarienkatalogs	KOBIL	X	X	X	X	X	
2.2	Generierung und Aufbereitung von Datensätzen	HSW	X			X	X	
2.3	Modellbildung zur Anomalieerkennung	AWSi	X			X		
3	**Betrachtung juristischer Aspekte**	TUC		X	X		X	X
3.1	Evaluation und der Erarbeitung eines Datenschutz- und Datenwirtschaftskonzepts	TUC		X			X	X
3.2	Rechtliche Begleitung der diversen Datenflüsse	TUC			X			X
3.3	Sicherstellung einer rechtskonformen Nutzung	TUC			X		X	X
4	**Umsetzung Cloudservice und Enduser-App**	AWSi	X	X	X	X	X	
4.1	Entwicklung und Test der KIASH Cloudplattform	AWSi	X	X		X	X	
4.2	Konzipierung und Entwicklung der Enduser-App	KOBIL	X	X	X		X	
5	**Umsetzung des Demonstrators der KIASH-Security-Box**	KOBIL	X	X	X	X	X	
5.1	Auswahl der IoT Plattformen	HSW		X		X	X	
5.2	IoT Plattform Integrationstest	KOBIL				X	X	
5.3	Verwaltungs- und Konfigurations-API	KOBIL	X		X		X	
5.4	Funktionale Integration	KOBIL	X	X	X		X	
5.5	Integrative und Privacy Tests	KOBIL					X	
6	**Pilotphase, Demonstrator-Optimierung, Weiterbildung und Zertifizierung**	eBZ	X	X	X		X	
6.1	Kick-Off-Workshop Pilotanwender	eBZ		X	X		X	
6.2	KIASH-Pilotanwender-Workshops Demonstrator Entwicklung	eBZ	X	X	X		X	
6.3	KIASH-Schulungs-, Weiterbildungs- und Zertifizierungsmodell	eBZ	X	X	X		X	
6.4	Entwicklung einer virtuellen Endanwenderschulung	eBZ		X	X		X	
7	**Normung und Öffentlichkeitsarbeit**	Cleopa	X	X	X	X	X	X
7.1	Öffentlichkeitsarbeit	Cleopa	X	X	X	X		
7.2	Öffentlichkeitsarbeit (Experten und Vernetzung mit Projekten)	KOBIL	X	X	X			X
7.3	DIN SPEC – Leitfaden für Anomalieerkennungskonzepte in Smarten Umgebungen	Cleopa		X	X	X		X

Abbildung 1: Arbeitspakete (APs) des Projekts mit jeweiliger Zuständigkeit

Das KIASH Projekt wurde in sieben Arbeitspakete (AP) unterteilt. Wie in Abbildung 1 zu sehen ist, war die KOBIL GmbH insbesondere an AP2, 4, 5 und 7 beteiligt. Hierbei waren wir verantwortlich für die Erstellung eines Szenarienkatalogs zur Anomalieerkennung, der Konzipierung und Entwicklung einer Endnutzer-App, der Umsetzung der eigentlichen KIASH Box. Des Weiteren haben wir Öffentlichkeitsarbeit geleistet, indem wir das Projekt in einem Online Meetup eines Branchenverbandes vorgestellt haben. In den folgenden Abschnitt werden unsere Beiträge und Ergebnisse zu den jeweiligen Arbeitspaketen dargestellt und erläutert.

2 Ablauf des Vorhabens

2.1 Vorgehen

Der folgende Lösungsweg wurde im Laufe des Projekts KIASH („KI-gestützte Anomalieerkennung für Smart Homes“) umgesetzt und entsprach bis auf kleinen Ausnahmen der ursprünglichen Planung. Ziel war die Entwicklung einer datenschutzkonformen, KI-basierten Lösung zur Erkennung von Anomalien in Smart Homes, die Handwerksbetriebe, Installateure und Elektrotechniker befähigt, ihren Kunden Security-Monitoring als Service anzubieten, ohne selbst über tiefgehende KI- oder IT-Sicherheitskompetenz verfügen zu müssen.

Im ersten Schritt erfolgte eine umfassende Anforderungsanalyse unter Einbindung von Handwerksbetrieben, Technologiepartnern und Forschern. Hierbei wurden Anwendungsfälle und Geschäftsmodelle identifiziert, die den praktischen Nutzen der KIASH-Lösung sicherstellen sollten. Parallel wurden rechtliche und ethische Rahmenbedingungen (ELSA) erarbeitet, um Datenschutz und Datensouveränität nach DSGVO und GAIA-X-Vorgaben sicherzustellen.

Auf dieser Grundlage wurden in enger Abstimmung zwischen den Partnern Referenz- und Testszenarien für Smart Homes entwickelt, die sowohl reguläres Nutzerverhalten als auch potenzielle Anomalien – wie Fehlfunktionen, Angriffe oder defekte Geräte – abbildeten. Diese Szenarien wurden experimentell in einem realen Testbed simuliert. Auch wurden öffentlich verfügbare Datensätze zur Entwicklung von Machine-Learning-Modellen für die Anomalieerkennung genutzt.

Im Rahmen des Arbeitspakets zur KI-Entwicklung wurde ein zweistufiges Verfahren umgesetzt:

1. Lokale Anomalieerkennung auf der im Smart Home installierten KIASH-Security-Box, die das Verhalten der IoT-Geräte kontinuierlich analysiert.
2. Federated Learning zur Aggregation der lokal trainierten Modelle über eine zentrale Cloudplattform, ohne dass personenbezogene Daten die Domäne des Nutzers verlassen.

Die in Zusammenarbeit von AWSi, Hochschule Worms entwickelten ML-Modelle wurden iterativ verbessert, um Fehlalarme zu reduzieren und die Robustheit gegenüber Nutzungsänderungen zu erhöhen. Durch den föderierten Lernansatz konnten Verbesserungen aus einzelnen Haushalten anonymisiert in das Gesamtmodell einfließen, wodurch sich die Erkennungsqualität über alle Nutzer hinweg stetig erhöhte.

Parallel dazu wurde von KOBIL die KIASH-Security-Box als Hardware-Demonstrator auf Basis eines Raspberry Pi realisiert. Diese Box ermöglicht die sichere Kommunikation und integriert sich nahtlos in bestehende Energie- und Smart-Home-Infrastrukturen. Für den Endnutzer wurde eine App entwickelt, die eine intuitive Bedienung, Anzeige von Anomalien sowie die Beauftragung von Handwerksdiensten ermöglicht. Die Cloudplattform und App-Dienste wurden durch AWSi unter Beachtung des Security-by-Design-Prinzips implementiert.

Im Arbeitspaket zur rechtlichen Begleitung (TUC) wurden alle Datenflüsse, Verarbeitungsprozesse und Nutzerschnittstellen geprüft. Dabei wurden Handlungsempfehlungen zur Umsetzung von Privacy-by-Design und Datenwirtschaftskonzepten formuliert, um eine DSGVO-konforme Nutzung sicherzustellen.

2.2 Zusammenarbeit intern und extern des Konsortiums

2.2.1 Zuständigkeiten im Konsortium

Das Projekt KIASH wurde von einem interdisziplinären Konsortium aus Forschung, Industrie und Handwerk getragen. Die **KOBIL GmbH** (Worms) hat als Verbundkoordinator ihre langjährige Erfahrung im Bereich IT-Sicherheit, Authentifizierung, Kryptographie und digitaler Identitätslösungen eingebracht. KOBIL übernahm die Koordinierung des Projekts sowie die Entwicklung und Implementierung des Demonstrators der KIASH-Security-Box. Basierend auf der firmeneigenen Plattformtechnologie entwickelte KOBIL Software-Komponenten, die sichere Kommunikation u.a. zur Cloud und Datenschutz gewährleisten. Zudem koordinierte KOBIL die technische Integration von Cloudplattform, Enduser-App und Anomalieerkennungs-Algorithmen und stellte die Schnittstellen zu den anderen Partnern sicher.

Das **August-Wilhelm Scheer Institut** für digitale Produkte und Prozesse (**AWSi**) verantwortete die wissenschaftlich-technische Leitung der Arbeitspakete zur Entwicklung der KI-Modelle für Anomalieerkennung sowie zur Umsetzung der Cloudplattform. Aufbauend auf umfangreicher Erfahrung in den Bereichen maschinelles Lernen, KI-gestützte Qualitätskontrolle und Datenanalyse konzipierte AWSi die Cloudplattform. Damit legte das Institut die Grundlage für datenschutzkonforme, verteilte Lernprozesse zwischen einzelnen Smart-Home-Systemen.

Die Hochschule Worms (HSW), vertreten durch das Zentrum für Technologie und Transfer (ZTT), trug zur Entwicklung und Validierung der Anomalieerkennungsmodelle bei. Die HSW errichtete ein realistisches Smart-Home-Testbed mit 19 verschiedenen IoT-Geräten, darunter Smart Speaker, Sensoren, Haushaltsgeräte und Smart-Home-Controller. Über einen Zeitraum von 136 Tagen wurden umfangreiche Netzwerkverkehrsdaten (ca. 37 GB) erfasst, die als Grundlage für das Modelltraining dienten. Darüber hinaus entwickelte die HSW mehrere ML-Modelle, insbesondere ein Graph Neural Network (GNN) zur Angriffserkennung sowie ein CNN-basiertes Verfahren zum Device Fingerprinting. Die HSW war zudem für die Entwicklung der Datenverarbeitungspipeline verantwortlich, die eine Echtzeit-Analyse des Netzwerkverkehrs ermöglicht. Sie unterstützte das AWSi bei der Implementierung des Flower-Frameworks für Federated Learning und lieferte eine Docker-basierte Deployment-Lösung für die Integration in die KIASH-Security-Box.

Die **Cleopa GmbH** übernahm die Leitung der Anforderungsanalyse, der Geschäftsmodellentwicklung sowie der Wissenschafts- und Ergebniskommunikation. Cleopa brachte ihre Expertise ein und erstellte die Grundlagen für die wirtschaftliche Verwertung der Projektergebnisse. Darüber hinaus koordinierte Cleopa die Erstellung des Leitfadens für Anomalieerkennungskonzepte in smarten Umgebungen.

Das **eBusiness-Kompetenzzentrum (eBZ)** fungierte als Transfer- und Schulungspartner mit direktem Zugang zur Handwerksbranche. Es leitete die Pilotphase, in der KIASH mit ausgewählten Handwerksbetrieben praktisch erprobt wurde, und entwickelte ein Schulungs-, Weiterbildungs- und Zertifizierungsmodell für Anwender und Betriebe. Zudem organisierte das eBZ Workshops und baute eine digitale Lern- und Wissensplattform auf, um die Projektergebnisse nachhaltig in die Praxis zu übertragen.

Die **Technische Universität Chemnitz (TUC)** verantwortete das Arbeitspaket zur rechtlichen Begleitung des Projekts. Unter Leitung der Professur für Privatrecht und Recht des geistigen Eigentums wurde ein datenschutzrechtlich fundiertes Konzept für die KIASH-Security-Box und die zugehörige Enduser-App erarbeitet. Dabei standen DSGVO-Konformität, Privacy-by-Design, Datenwirtschaftsrecht sowie Fragen der Datenportabilität und

Zertifizierungsanforderungen nach IT-Sicherheitsgesetz 2.0 im Mittelpunkt. Die TUC stellte sicher, dass alle entwickelten Komponenten rechtssicher und marktfähig sind.

2.2.2 Austausch innerhalb des Konsortiums

Zum Austausch von Informationen und zum Teilen von Neuigkeiten fand alle zwei Wochen (montags um 10:00 Uhr) ein etwa einstündiges Jour-fixe-Meeting online über Microsoft Teams statt. Zusätzlich fanden mehrere persönliche Konsortialtreffen an verschiedenen Standorten der Partner statt, die einen noch engeren Austausch im Projekt ermöglichten. Im Rahmen dieser Konsortialtreffen hat jeder Projektpartner ein kurzes Statusupdate in Form eines Kurzvortrags (ca. 20 Minuten) gegeben.

2.2.3 Projektexterne Stakeholder

Im Vorfeld hatten mehrere externe Stakeholder in Form eines „Letter of Intent“ (LOI, dt. „Absichtserklärung zur Beteiligung“) ihre Unterstützung für das Projekt zugesichert. Hierzu gehörten die folgenden, überwiegend mittelständisch angesiedelten Betriebe:

- **Struck-Belz**, „Stuck – Putz – Trockenbau“, https://www.belz.de/
- **Discovergy**, heute „inexogy smart metering GmbH & Co. KG“, https://discovergy.com/
- **Dörflinger Elektrotechnik GmbH**, https://www.doerflinger-elektrotechnik.de/

2.3 Tätigkeiten und Ergebnisse in den einzelnen Arbeitspaketen

Dieser Abschnitt gibt einen detaillieren Überblick über die Arbeiten in den einzelnen Arbeitspaketen. Da KOBIL lediglich an den an AP2, 4, 5 und 7 beteiligt war, liegt hierauf das Hauptaugenmerk.

2.3.1 AP1 – Anforderungsanalyse

Arbeitspaket 1 diente der Erhebung der technischen, rechtlichen und nutzerbezogenen Anforderungen. Cleopa koordinierte die Workshops, führte die Stakeholder-Abstimmung durch und entwickelte die Nutzersegmente und Personas. Das eBZ brachte Anforderungen aus dem Handwerk ein und sammelte Rückmeldungen zur Installierbarkeit, Bedienbarkeit und zum praktischen Einsatz der KIASH-Komponenten. AWSi ergänzte technische Anforderungen, insbesondere zu Cloud-Architektur, Schnittstellen, Sicherheitsaspekten und der Integration von Machine-Learning- und Federated-Learning-Verfahren. Die TUC lieferte die rechtlichen und datenschutzbezogenen Anforderungen sowie die juristischen Beiträge zur ELSA-Analyse.

Die Ergebnisse umfassten einen konsolidierten Anforderungskatalog, eine Nutzer- und Anwendertypologie sowie erste Architekturentwürfe für die weitere Entwicklung.

2.3.2 AP2 – ML-basierte Anomalieerkennung auf heterogenen IoT-Daten

Szenarienkatalog

Für AP2 erstellte KOBIL einen Szenariokatalog mit 20 verschiedenen Gefährdungsszenarien. Die wichtigsten im Szenariokatalog vorgeschlagenen Szenarien lassen sich wie folgt zusammenfassen:

1. **Netzwerküberlastung** – Die KIASH-Box erkennt dauerhaft hohen Netzwerkverkehr und warnt den Benutzer vor einer möglichen Überlastung, einschließlich Vorschlägen zur Optimierung wie der Erhöhung der Bandbreite.
2. **Sicherheitsverletzungen** – Die KIASH-Box analysiert den Datenverkehr mittels KI und IDS-Systemen, um Sicherheitsvorfälle zu erkennen, und schlägt geeignete Gegenmaßnahmen vor.

3. **Unbenutzte Geräte** – Geräte, die über einen längeren Zeitraum inaktiv waren, werden erkannt und als potenziell unnötig markiert, mit Vorschlägen zum Trennen oder Überprüfen.
4. **Verbindungsprobleme** – Instabile Netzwerkverbindungen werden erkannt und dem Benutzer mit Lösungsvorschlägen (z. B. Neupositionierung des Routers) gemeldet.
5. **Geräteausfälle** – Die KIASH-Box erkennt ausgefallene oder fehlerhafte IoT-Geräte und gibt Hinweise zur Fehlerbehebung, wie z. B. Neustart oder Überprüfung der Verkabelung.
6. **Unbefugter Zugriff** – Verdächtige Zugriffs- oder Kommunikationsmuster werden erkannt und sofort gemeldet; es werden entsprechende Sicherheitsberichte generiert.
7. **Unerwarteter Netzwerkverkehr** – Unerwartete Datenübertragungen im isolierten Netzwerk werden erkannt, um Sicherheitsprobleme oder Fehlkonfigurationen aufzudecken.
8. **Unregelmäßiges Verhalten** – Abweichendes Verhalten (z. B. von Smart-Home-Geräten) wird automatisch analysiert und an den Benutzer gemeldet.
9. **Veraltete Hardware** – Alte oder nicht mehr unterstützte Geräte werden identifiziert, mit Empfehlungen zum Austausch oder Upgrade.
10. **Unerwartetes Geräte-Onboarding** – Neue, nicht autorisierte Geräte werden im Netzwerk erkannt, und der Benutzer wird zur Überprüfung aufgefordert.
11. **Unerwartete Geräteaktivität** – Aktivitäten außerhalb der geplanten Zeiten werden gemeldet, um mögliche Sicherheitskompromittierungen zu erkennen.
12. **Unsichere Kommunikation** – Unverschlüsselte oder schwach verschlüsselte Kommunikation wird erkannt, um Maßnahmen zur Verbesserung der Sicherheit anzuregen.

Datenbasis

Der für das jeweilige Modelltraining verwendete Datensatz wurde von AWSi und der Hochschule Worms definiert und ausgewählt. Die Hochschule Worms errichtete ein physisches IoT-Testbed, das eine typische Smart-Home-Umgebung abbildet. In der Testumgebung befinden sich 19 unterschiedliche IoT-Geräte verschiedener Hersteller, darunter Netatmo-Sensoren und -Kameras, Apple HomePod, Amazon Alexa, Google Nest Mini, iRobot Staubsauger, Philips Hue Lampen sowie Bosch und Homematic IP Smart-Home-Controller. Die Geräte wurden über einen OpenWRT-basierten Router (Xiaomi Mi Router 4A) vernetzt. Über einen Zeitraum von 136 Tagen – vom 28. September 2023 bis zum 15. Februar 2024 – wurden kontinuierlich Netzwerkverkehrsdaten im Leerlaufzustand aufgezeichnet. Insgesamt entstanden dabei rund 37 GB an Rohdaten, die sowohl LAN- als auch WAN-seitigen Verkehr umfassen.

Ergänzend zu den eigenen Testbed-Daten wurden öffentlich verfügbare Datensätze einbezogen, insbesondere der CIC-IoT-2023-Datensatz des Canadian Institute for Cybersecurity, der eine Vielzahl moderner IoT-Angriffsformen wie DDoS, Reconnaissance und Brute-Force-Angriffe enthält. Weitere berücksichtigte Datensätze waren IoT-23 (Botnet-Varianten wie Mirai und Hajime), TON_IoT sowie Edge-IIoTset.

Modellentwicklung

Auf Basis dieser Datensätze entwickelten AWSi und die Hochschule Worms die ML-Modelle zur Anomalieerkennung. Die Modellarchitektur experimentierte sowohl mit sogenannten „Autoencodern" [9] als auch mit „Graph Neural Networks" (GNN) [10]. Da künftig weitere, möglicherweise bessere Modellarchitekturen entstehen könnten, wurde die Infrastruktur

rund um das Modell architekturagnostisch aufgebaut, sodass ein Wechsel der Modellarchitektur problemlos möglich ist.

Folgende Modelle wurden entwickelt:

- **Autoencoder**: Ein Machine-Learning-Modell, das versucht, eingehende Datenpakete zu rekonstruieren. Schlägt die Rekonstruktion fehl (hoher Rekonstruktionsfehler), weist dies auf anomalen Datenverkehr hin. Das AWSi entwickelte dieses Modell mit Unterstützung der HSW.
- **Graph Neural Network (GNN)** zur Angriffserkennung: Dieser von der HSW entwickelte Modelltyp analysiert Beziehungen zwischen verschiedenen IoT-Geräten und Internetservern anhand der Menge und Art des ausgetauschten Datenverkehrs.
- **CNN-basiertes Device Fingerprinting**: Dieses ebenfalls von der HSW entwickelte Modell ermöglicht die Identifikation von Gerätetypen allein anhand ihres Netzwerkverhaltens im Leerlaufzustand.

Die detaillierte Evaluierung der Modelle ist im Abschlussbericht der Hochschule Worms dokumentiert.

Datenverarbeitungspipeline

Für die Echtzeit-Analyse des Netzwerkverkehrs entwickelte die HSW eine modulare Datenverarbeitungspipeline. Die zentrale Komponente – der sogenannte DataReader – erfasst Netzwerkpakete direkt von der Netzwerkschnittstelle und extrahiert in Echtzeit relevante Features. Diese Merkmalsvektoren werden anschließend den Analysemodellen übergeben. Die Ergebnisse werden sowohl lokal zwischengespeichert als auch an das Backend weitergeleitet. Die HSW stellte diese Pipeline als vollständig konfiguriertes Python-Environment sowie als Docker-Container bereit, um die Integration in die KIASH-Security-Box zu erleichtern.

Federated-Learning-Infrastruktur

Die Infrastruktur für Federated Learning wurde von AWSi entwickelt, einschließlich der Client/Server-Kommunikation und der Orchestrierung mittels des Flower-Frameworks. KOBIL unterstützte die Integration dieser Infrastruktur in die KIASH-Umgebung und testete das Systemverhalten während des Deployments.

Hardware-Anforderungen

Zu Beginn wurde angenommen, dass das Anomalieerkennungsmodell eine GPU sowohl für das Training als auch für die Inferenz benötigt. Im Verlauf des Projekts stellte sich jedoch heraus, dass lokales Training auf der KIASH-Box nur dann sinnvoll ist, wenn negative Beispiele (in Form von Anomalien) vorhanden sind – was im normalen Betrieb selten der Fall ist. Aufgrund der geringeren Last wurde daher festgestellt, dass eine GPU in der KIASH-Box nicht zwingend erforderlich ist, sofern die Inferenz in Echtzeit erfolgen kann.

2.3.3 AP3 – Betrachtung juristischer Aspekte

Arbeitspaket 3 behandelte die rechtlichen und datenschutzbezogenen Anforderungen des KIASH-Systems. Die TUC erarbeitete die vollständige juristische Analyse, einschließlich der Bewertung von Datenflüssen, Verarbeitungsschritten und datenschutzrechtlichen Vorgaben. Das eBZ steuerte praxisnahe Hinweise aus Workshops mit Handwerksbetrieben bei und brachte typische Nutzungssituationen und organisatorische Anforderungen ein, die in die rechtliche Bewertung einflossen. Cleopa leistete ergänzende Zuarbeiten im Rahmen der Abstimmungen. AWSi stellte technische Beschreibungen von Datenflüssen und

Kommunikationswegen bereit, die für die rechtliche Analyse relevant waren. Das Arbeitspaket führte zu einem umfassenden rechtlichen und datenschutzbezogenen Rahmen für die KIASH-Security-Box, die Cloud-Dienste und die zugehörigen Anwendungen.

2.3.4 AP4 – Umsetzung Cloud-Service und Enduser-App

Arbeitspaket 4 startete im Dezember 2022 und fokussierte die Konzeption einer skalierbaren Cloud-Architektur sowie die Enduser-App. AWSi übernahm die wissenschaftlich-technische Leitung und die Entwicklung der Cloud-Plattform, KOBIL die Umsetzung der Enduser-App inkl. Anbindung an die KIASH-Security-Box. Die in AP1 definierten Anforderungen flossen direkt in Architektur und App ein; parallel zu AP2 wurde die bidirektionale Schnittstelle zwischen KIASH-Box und Cloud vorbereitet, um Anomaliedetektion und Federated-Learning-Modell einzubinden.

Zentral für dieses Projekt ist die Kommunikation zwischen verschiedenen KIASH-Boxen, die mittels Federated Learning (FL) Modellupdates austauschen. Dies geschieht über eine zentrale Cloud-Plattform.

Die Aufgabe der Cloud-Plattform ist es, ein Identity Management für Nutzer und individuelle KIASH-Boxen zu betreiben, sodass diese eindeutig identifiziert und einem Haushalt zugeordnet werden können. Ebenso steuert die Cloud-Plattform den Federated-Learning-Prozess. Hierzu wird auf das sog. „Flower Framework“ [11] als Basis zurückgegriffen.

Abbildung 2 erklärt den Aufbau der KIASH Architektur schematisch.

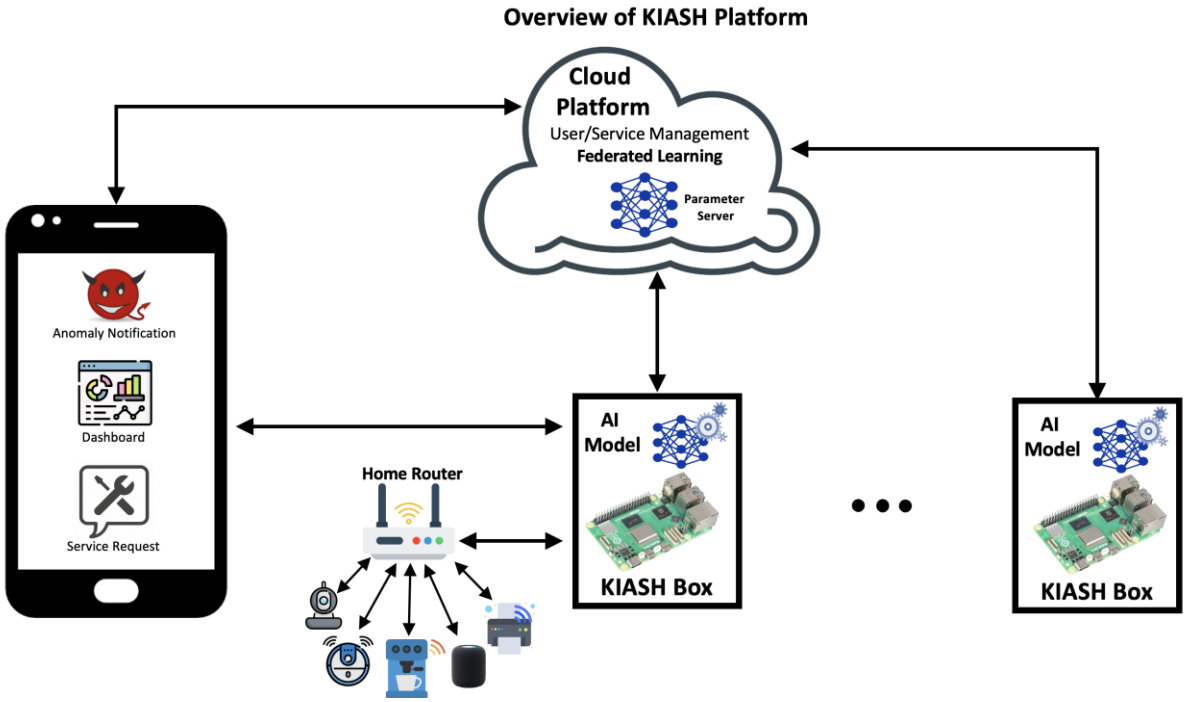


Abbildung 2: Überblick über die KIASH Plattform

Cloud-Plattform: Serverless Backend auf Azure Functions, containerisierter Flower-Server (Azure Container Instances) für die FL-Orchestrierung, Azure Cosmos DB für Modell- und Nutzungsdaten, Keycloak (Docker auf EC2) für Identity & Access Management, Swagger-API auf GitHub zur Schnittstellendokumentation. Ursprünglich war geplant, die KIASH-Plattform mit der Europäischen Gaia-X Infrastruktur kompatibel zu entwickeln. Allerdings kam es in der Zwischenzeit zu erheblichen Verzögerungen und Problemen in dessen Entwicklung und

Standardisierung. In der Presse wurde das Gaia-X Projekt von ehemalig Beteiligten als „tot“ bezeichnet. [12] Aus diesem Grund wurde nach gründlicher Evaluierung die GAIA-X-/EDC-Integration nicht umgesetzt. Die Architektur bleibt kompatibel, falls GAIA-X/EDC später benötigt wird.

Security/Privacy: HTTPS/TLS auf allen Kanälen (Box ↔ Cloud, App ↔ Cloud), OAuth2/OpenID Connect via Keycloak, datensparsam (nur Modelle, keine Rohdaten), FL verhindert Rückschlüsse auf Haushalte. Weitere Hardening- und Skalierungsmaßnahmen sind als Anschlussarbeiten vorgesehen, da der Projektschwerpunkt auf der ML/Federated-Learning-Integration lag.

ML-Integration: Schwerpunkt war die Einbindung der Federated-Learning-Pipeline samt Autoencoder-Experimenten, um schnelle Tests der Anomalieerkennung auf der KIASH-Box zu ermöglichen. Standard-Komponenten (Keycloak, HTTPS/TLS, Flutter) wurden dafür schlank konfiguriert.

Enduser-App: Als Interface für den Endnutzer dient eine eigens für dieses Projekt entwickelte App. KOBIL entwickelte eine MVP-Version, basierend auf dem Flutter Framework [13]. Wie in Abbildung 3 zu sehen ist, kann sich der Nutzer wie von anderen Apps gewohnt für die KIASH Plattform registrieren. Ist die KIASH Box bereits im Heimnetz vorhanden, wird diese im Regelfall direkt von der App gefunden.

Die MVP-App wurde im Projekt als lokal lauffähiger Demonstrator betrieben, um schnelle Iterationen ohne produktive Cloud-Abhängigkeit zu ermöglichen; die Azure-basierte Cloud-Plattform steht für die spätere Anbindung bereit. Zusätzliche Hardening- und Skalierungsmaßnahmen sind für eine mögliche Anschlussumsetzung vorgesehen, da sie außerhalb des Forschungsziels „ML-basierte Anomalieerkennung“ liegen.

Integrationstests: Aufgrund des Projektfokus auf die neuartige ML-Integration legten wir im Rahmen von AP4 den Schwerpunkt auf die Einbindung der Federated-Learning-Pipeline samt Autoencoder-Experimenten. Die Sicherheits- und Cloud-Komponenten (Keycloak, HTTPS/TLS, Flutter) wurden gezielt als Standardtechnologien konfiguriert, um die ML-Prototypen schnell testen zu können. Initiale Tests der FL-Schnittstelle und Anomalieerkennung auf der KIASH-Box (Raspberry Pi 5) wurden im Test-Betrieb durchgeführt und verliefen erfolgreich.

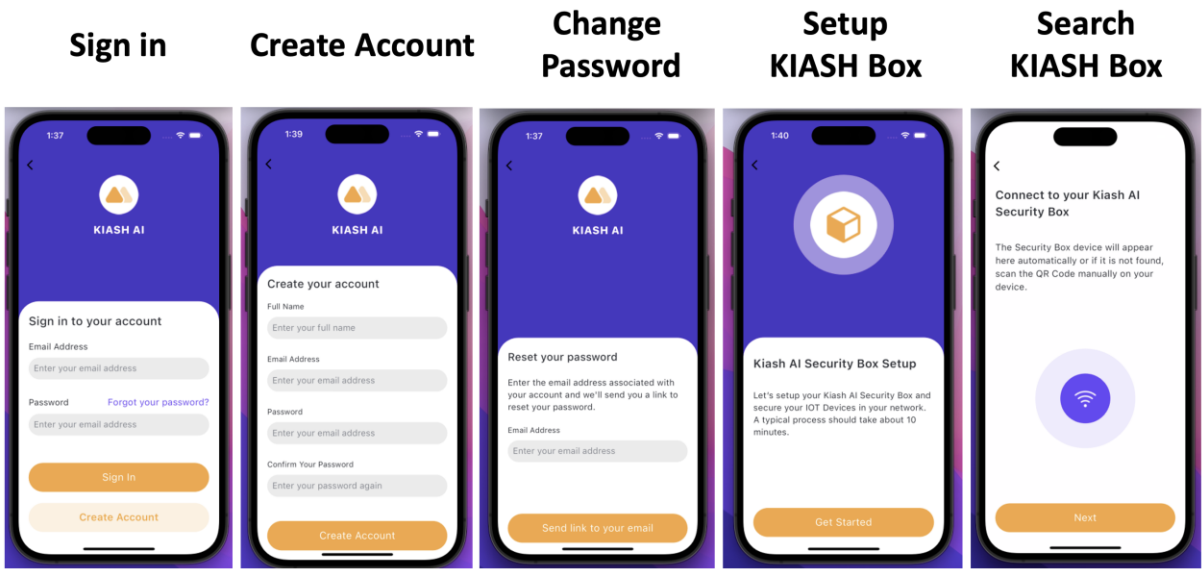


Abbildung 3: Registrierung und Einrichtung der KIASH-Box mit der KIASH-App

Abbildung 4 zeigt das Dashboard der KIASH-App. Der Homescreen gibt eine quantitative Auskunft über die Anzahl der mit dem Heimnetz verbundenen Geräte, sowie eine qualitative Einschätzung über deren Zustand: „Alles in Ordnung“ (grün), „Erfordert Aufmerksamkeit“ (gelb), oder „Gefahr“ (rot).

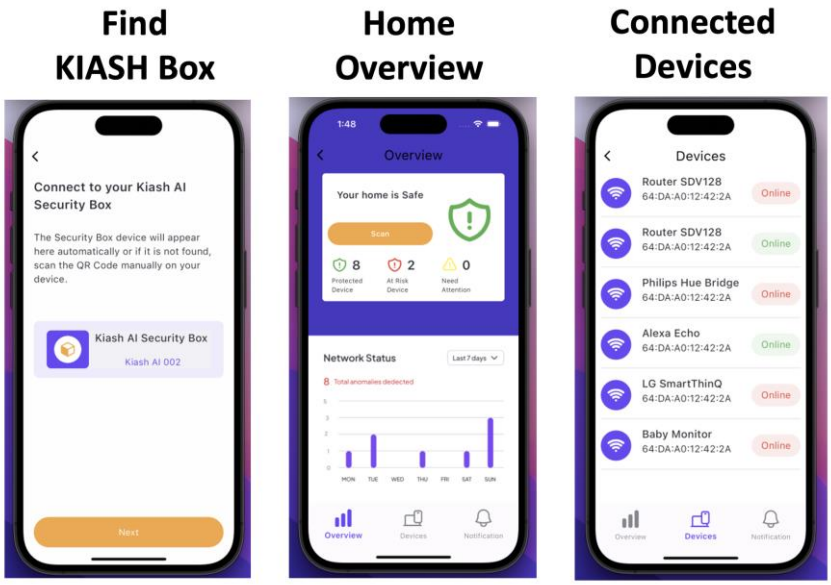


Abbildung 4: KIASH-App Dashboard und verbundene Geräte

Abbildung 5 veranschaulicht die Informationen über einzelne Geräte, die dem Endnutzer angezeigt werden, wenn er/sie auf ein Gerät in der Liste tippt. In dem unten gezeigten (fiktiven) Beispiel handelt es sich um eine Philips Hue Bridge, welche ein Problem aufweist. Der Nutzer hat nun die Option, sie aus dem lokalen Netzwerk auszusperren und auf Knopfdruck Dienstleistungen vom zuständigen Handwerksbetrieb anzufordern.

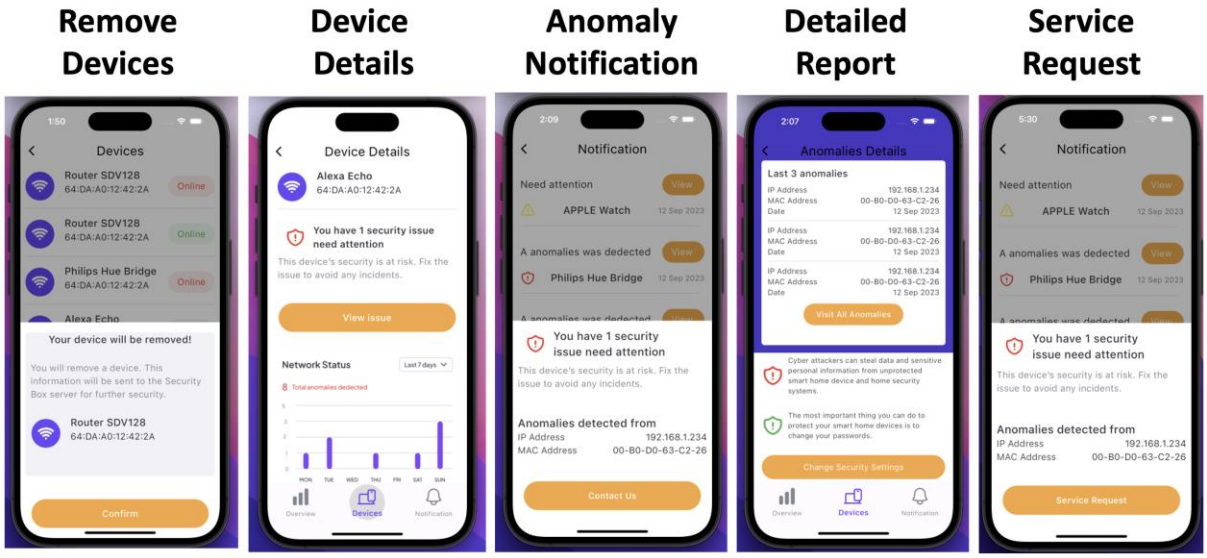


Abbildung 5: KIASH-App Statusanzeige von verbundenen Geräten und Aktionen

Die Kommunikation zwischen den jeweiligen Plattformkomponenten (ML-Modell, KIASH-Box, Cloud-Plattform, App) erfolgt branchentypisch über sogenannte APIs („Application Programming Interfaces“, dt. Programmierschnittstellen). Schematisch ist dies in Abbildung 6 dargestellt.

Im Speziellen wird die Kommunikation zwischen der KIASH-Box, der Cloud-Plattform und der App mittels einer HTTPS / TLS verschlüsselten Verbindung gesichert. Dies verhindert das Auslesen sensibler Informationen während des Austauschs durch Dritte und ermöglicht zugleich die Feststellung der Identität, insbesondere der Cloud-Plattform, mittels einer PKI („Public Key Infrastructure“, dt. öffentliche Schlüsselinfrastruktur.) Die versendeten Daten werden mit dem Flatbuffer Standard [14] encodiert.

Für die KIASH-Box wurde ein Dienst mit der Programmiersprache C++ entwickelt, welcher die Kommunikation der KIASH-Box mit dem ML-Modell auf der einen Seite und dem Cloud-Service auf der anderen Seite ermöglicht. Das ML-Modell, welches ebenfalls auf der KIASH-Box läuft, schreibt alle gefundenen Anomalien in eine lokale Datenbank (SQLite), welche kontinuierlich vom C++ Dienst ausgelesen wird. Gibt es einen neuen Fund, so werden umgehend alle lokal registrierten Apps per Broadcast-Message informiert und den Cloud-Dienst per API Call benachrichtigt, falls er in einer späteren Ausbaustufe zur Verfügung steht, welcher wiederum eine Eilmeldung an die registrierten Endnutzer-Apps schickt.

Abbildung 6: Kommunikation zwischen den jeweiligen Plattformkomponenten

2.3.5 AP5 – Umsetzung des Demonstrators und der KIASH-Security-Box

Da die Entwicklung einer maßgeschneiderten Hardware für die KIASH-Box den zeitlichen und finanziellen Rahmen des Projekts überstiegen hätte, wurde geprüft, ob sich die KIASH-Box auf Basis bereits existierender Hardware realisieren lässt. Ziel war es, eine leistungsfähige, zugleich aber kosteneffiziente Plattform zu finden, die den Anforderungen des Projekts gerecht wird.

Zunächst fiel die Wahl auf den **Nvidia Jetson Orin Nano** (Abbildung 7, links). Dabei handelt es sich um ein kompaktes System-on-Module, das für KI- und Edge-Computing-Anwendungen konzipiert ist. Es verfügt über eine integrierte Grafikeinheit (GPU) und bietet ausreichende Rechenleistung, um neuronale Netze effizient auszuführen. Zudem unterstützt es gängige ML-Frameworks wie TensorFlow und PyTorch und besitzt mehrere Schnittstellen zur Anbindung externer Komponenten.

Problematisch ist allerdings, dass der Stückpreis des Jetson bei etwa 500 EUR liegt. Auch wenn bei größeren Abnahmemengen mit Rabatten zu rechnen ist, übersteigt dieser Preis dennoch die Schmerzgrenze, die viele Verbraucher bereit wären, für eine KIASH-Box zu bezahlen.

Da zwischenzeitlich bekannt wurde, dass für das Anomaliemodell nicht zwingend eine GPU-Einheit benötigt wird, wurde im Laufe des Projektes auf einen **Raspberry Pi der 5. Generation** umgeschwenkt. Hierbei handelt es sich um einen Einplatinencomputer, der über eine leistungsfähige CPU, ausreichenden Arbeitsspeicher und vielseitige Schnittstellen verfügt. Er bietet genügend Rechenleistung, um das Anomaliemodell auszuführen, und stellt durch seine weite Verbreitung, gute Dokumentation und niedrigen Anschaffungskosten (ca. 70 EUR) eine praktikable und kosteneffiziente Alternative zum Jetson Orin Nano dar.

Zudem handelt es sich bei dem Raspberry Pi nicht um sonderlich spezialisierte Hardware, sodass jegliche Software auf dem Raspberry Pi (u.a. das Anomaliemodell) theoretisch in bereits beim Endnutzer vorhandene Heimrouter (z.B. FRITZ!Box) integriert werden könnte. Hierzu wäre allerdings die Kooperation des jeweiligen Herstellers nötig.

Dementsprechend wurde der Raspberry Pi als Basisplattform für den KIASH-Box Demonstrator ausgewählt.

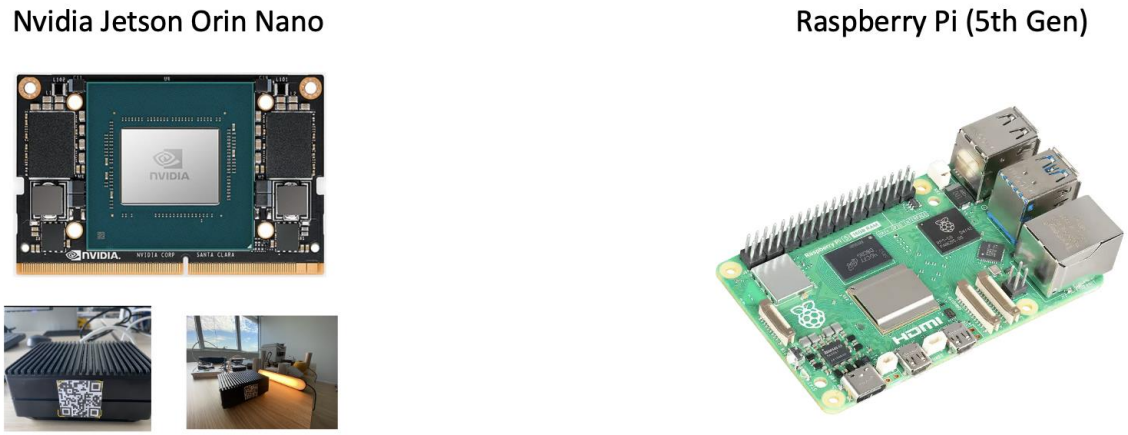


Abbildung 7: Hardware, die für den Demonstrator zur Auswahl stand: Nvidia Jetson Orin Nano (links), Raspberry Pi 5. Generation (rechts)

Damit die KIASH-Box den Datenverkehr des Heimnetzes analysieren kann, müssen sich alle IoT-Geräte im Haushalt mit der KIASH-Box verbinden. Hierzu stehen zwei Modi zur Auswahl:

1. **Bridge-Mode**: Hier fungiert die KIASH-Box selbst als neuer WLAN-Router im Haus. Alle IoT-Geräte verbinden sich direkt mit dem eingebauten WLAN Access Point der KIASH-Box und diese leitet den Datenverkehr über den eigentlichen Heimrouter (z.B. FRITZ!Box) ins Internet.
2. **DHCP-Mode**: Hierzu muss die DHCP-Konfiguration („Dynamic Host Configuration Protocol“) des existierenden Heimrouters (z.B. FRITZ!Box) derart abgeändert werden, dass die „Gateway-IP-Adresse“ auf die IP-Adresse der KIASH Box zeigt. Diese leitet dann den Datenverkehr über ein Ethernet Kabel zum Heimrouter.

Beide Modi haben jeweils Vor- und Nachteile. So ist der **Bridge-Mode** für einen unerfahrenen Nutzer wesentlich leichter einzurichten. Allerdings müssten dann alle sich bereits im Haushalt befindlichen IoT-Geräte mit dem neuen „Router“ verbunden werden. Des Weiteren ist fraglich, ob die KIASH-Box die gleiche WLAN-Sendeleistung aufweist wie gängige Heimrouter Modelle. Beim **DHCP-Mode** verhält es sich genau andersherum. Im Idealfall müssen existierende IoT-Geräte nicht neu verbunden werden und bleiben weiterhin mit der im Heimrouter verbauten WLAN-Antenne verbunden. Allerdings erfordert die DHCP Konfiguration einige Vorkenntnisse.

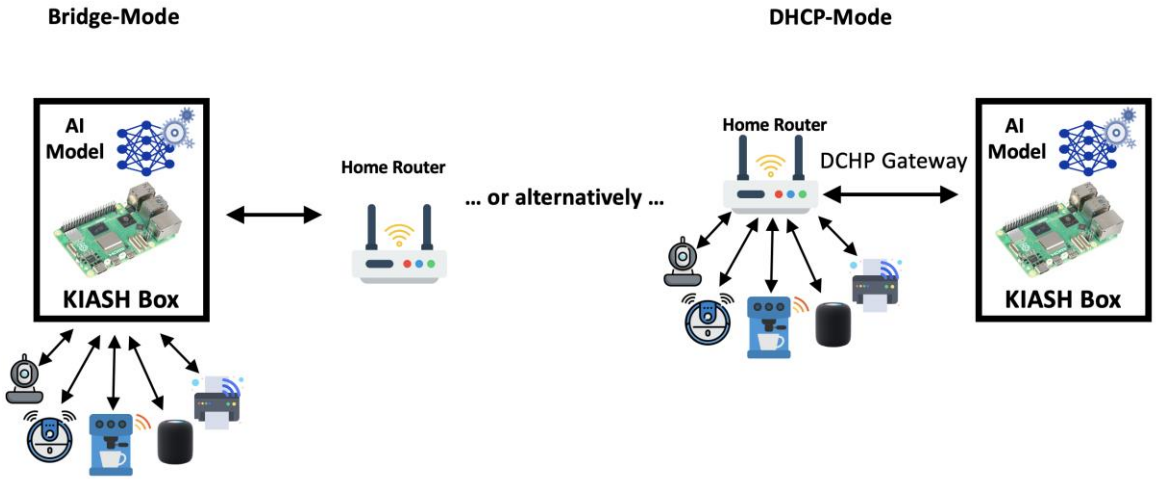


Abbildung 8: Illustration der beiden Verbindungsmodi der KIASH-Box, (links) Bridge-Mode, (rechts) DHCP-Mode

Während AP5 führte KOBIL die verschiedenen Projektkomponenten zusammen und führte unterschiedliche Testverfahren durch. Die Tests offenbarten eine erhöhte False-Positive-Rate, die auch von AWSi und der Hochschule Worms bestätigt wurde, und initiierten eine gemeinsame Analyse der drei Partner. Die Untersuchungen zeigten, dass insbesondere die Heterogenität des Netzwerkverkehrs und verschlüsselungsbedingte Einschränkungen die Klassifikation erschwerten. Die daraus gewonnenen Erkenntnisse bilden eine Grundlage für zukünftige Forschung und technische Verbesserungen im Bereich der Anomalieerkennung und des Federated Learning.

2.3.6 AP6 – Pilotphase, Demonstrator-Optimierung, Weiterbildung und Zertifizierung

Arbeitspaket 6 wurde vom eBusiness-KompetenzZentrum (eBZ) geleitet und konzentrierte sich auf die Erprobung der KIASH-Lösung unter realen Einsatzbedingungen. In diesem Zusammenhang wurden Rückmeldungen aus der praktischen Anwendung systematisch erfasst und zur kontinuierlichen Verbesserung der Systemkomponenten genutzt. Parallel dazu entwickelte das eBZ eine digitale Lern- und Schulungsumgebung, die Anwender bei der Einführung und Nutzung der Lösung unterstützt. Die Inhalte wurden schrittweise verfeinert und an das Feedback der Pilotbetriebe angepasst. Insgesamt leistete dieses Arbeitspaket einen wesentlichen Beitrag dazu, die Praxistauglichkeit, Benutzerfreundlichkeit und Qualifizierbarkeit der KIASH-Lösung sicherzustellen.

2.3.7 AP7 – Normung und Öffentlichkeitsarbeit

Zur öffentlichen Kommunikation des Projektes wurde eine Website (https://kiash.de/) eingerichtet, auf der regelmäßig über Neuigkeiten, die das Projekt betreffen, berichtet wurde.

Diese Website war erfolgreich darin, Aufmerksamkeit von externer Seite aus zu erlangen.

Zum Beispiel wurde auf dem Internetportal **BauNetz Wissen** in einem redaktionellen Artikel über KIASH berichtet. [15]

Ebenfalls gab es eine Einladung, das Projekt in einem Online Meetup des **Smart Home & Living Baden-Württemberg e.V.** vorzustellen. Die Vorstellung fand am 26.09.2024 in Form eines halbstündigen Vortrags statt. Die Resonanz war jedoch verhalten. So kam aus dem Publikum u.a. der Vorwurf auf, dass das KIASH Projekt auf „Angstmache“ vor unsicheren IoT-Geräten fuße.

3 Zahlenmäßiger Nachweis (wurde bei Profi-Online eingereicht)

4 Ergebnisse

4.1 Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Die im Rahmen von KIASH durchgeführten Arbeiten erwiesen sich als sinnvoll, um die gesteckten Ziele, namentlich die Entwicklung einer datenschutzkonformen, KI-basierten Lösung zur Anomalieerkennung in Smart Homes, zu erreichen. Angesichts der wachsenden Zahl vernetzter Geräte in Privathaushalten und der damit verbundenen Sicherheitsrisiken bestand ein klarer Bedarf an vertrauenswürdigen und für KMU praktikablen Sicherheitslösungen.

Das Projektteam hat diesen Bedarf auf mehreren Ebenen adressiert: technisch durch die Entwicklung der KIASH-Security-Box und der zugehörigen Cloud- und App-Infrastruktur, wissenschaftlich durch die Erstellung umfangreicher Datensätze im Testbed der Hochschule Worms (19 IoT-Geräte, 136 Tage Datenerfassung, ca. 37 GB Rohdaten) sowie strategisch durch die Einbettung in die förderpolitischen Zielsetzungen des BMBF und der Hightech-Strategie 2025. Die gewählte Vorgehensweise, damit gemeint der Einsatz von Federated Learning in Kombination mit „Privacy by Design“, war dabei methodisch angemessen, um Datenschutz, technische Machbarkeit und Wirtschaftlichkeit in Einklang zu bringen.

Die in Abschnitt 1.4 definierten Kernziele wurden weitgehend erreicht: Die KIASH-Security-Box wurde als funktionaler Demonstrator auf Basis eines Raspberry Pi 5 realisiert, eine Cloudplattform mit Federated-Learning-Infrastruktur wurde implementiert, und eine intuitive Enduser-App wurde entwickelt. Der im Szenarienkatalog definierte Umfang von 20 Gefährdungsszenarien bildete dabei eine solide Grundlage für die Anomalieerkennung.

Auch die intensive, interdisziplinäre Zusammenarbeit zwischen Forschung und Industrie erwies sich als wesentlicher Erfolgsfaktor. Der enge Austausch in regelmäßigen Jour fixe Meetings und Konsortialtreffen ermöglichte eine zielgerichtete Entwicklung, die sich an realen Anwendungsszenarien und praktischen Anforderungen orientierte. Damit wurde das Projekt seinem Anspruch gerecht, Wissenschaft mit gesellschaftlichem und wirtschaftlichem Nutzen zu verbinden.

4.2 Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse

Die Ergebnisse des Projekts besitzen erhebliches Verwertungspotenzial, welches sowohl technologisch als auch wirtschaftlich ist. Mit der KIASH-Security-Box, der Cloudplattform und der Endnutzer-App liegt ein funktionaler Demonstrator vor, der den Grundstein für marktfähige Produkte legt. Die technische Architektur ist modular und architekturagnostisch gestaltet, sodass künftige Modellarchitekturen problemlos integriert werden können. Perspektivisch kann die Lösung in kommerzielle Plattformen, Router (z. B. FRITZ!Box) oder Smart-Home-Systeme integriert werden.

Die Entscheidung für den Raspberry Pi 5 als Hardwarebasis (ca. 70 EUR gegenüber ca. 500 EUR für den ursprünglich vorgesehenen Nvidia Jetson Orin Nano) eröffnet zudem einen kosteneffizienten Weg zur Markteinführung und senkt die Einstiegshürde für Endverbraucher erheblich.

Für die KOBIL GmbH ergaben sich darüber hinaus weitere Mehrwerte: Durch das Projekt konnte ein erheblicher Erkenntnisgewinn für die eigenen Forschungs- und Entwicklungsaktivitäten sowie für gemeinsame Vorhaben mit Partnern erzielt werden, insbesondere im Hinblick auf die Weiterentwicklung des bestehenden Lösungs- und Produktportfolios. Zudem wurden die im Projekt entwickelten Verfahren gezielt so ausgelegt,

dass sie eine Integration in bestehende Systeme und die Anbindung zukünftiger Technologien ermöglichen. Schließlich trug das Projekt wesentlich zur Fortbildung der hausinternen KI-Abteilung bei, indem neue Anwendungsfelder von Künstlicher Intelligenz erschlossen wurden, die über das bisherige Kerngeschäft der Nutzer-Authentifizierung hinausgehen.

Darüber hinaus bietet KIASH eine Basis für zukünftige Standardisierungs- und Zertifizierungsprozesse, wie sie im Rahmen von AP7 angestoßen wurden.

4.3 Fortschritte anderer Akteure während der Projektlaufzeit

Ursprünglich war im Rahmen von KIASH vorgesehen, die entwickelte Cloudplattform vollständig GAIA-X-konform zu gestalten, um eine nahtlose Integration in die europäische Dateninfrastruktur zu ermöglichen. Im Verlauf des Projekts zeigte sich jedoch, dass sich die GAIA-X-Initiative erheblich verzögerte und von vielen beteiligten Akteuren als faktisch gescheitert beziehungsweise „tot“ bezeichnet wurde [12]. Daher wurde entschieden, von einer konkreten Implementierung der GAIA-X-Schnittstellen abzusehen, um die technische Entwicklung nicht zu behindern. Stattdessen wurde die KIASH-Cloudarchitektur cloud-agnostisch ausgelegt. Dadurch ist sie in der Lage, auf nahezu jeder gängigen Cloud-Infrastruktur (einschließlich europäischer und nationaler Plattformen) betrieben zu werden. Sollte GAIA-X oder eine vergleichbare Initiative künftig an Bedeutung gewinnen, bleibt die Architektur kompatibel.

4.4 Gesamtbewertung

Zusammenfassend lässt sich festhalten, dass KIASH ein erfolgreiches und zukunftsorientiertes Forschungsprojekt war. Die erarbeiteten Konzepte, Prototypen und Leitfäden bilden eine solide Grundlage für eine technische und wirtschaftliche Weiterentwicklung. Besonders hervorzuheben ist die integrative Verknüpfung von Forschung und Praxis sowie die enge Zusammenarbeit aller Konsortialpartner.

Die in Abschnitt 1.4 formulierten Kernziele – Entwicklung der KIASH-Security-Box, Realisierung einer Cloudplattform, Implementierung von KI-Verfahren zur Anomalieerkennung, Entwicklung einer Enduser-App sowie Aufbau eines Schulungsmodells – wurden erreicht. Die gewonnenen Erkenntnisse über die technische Umsetzbarkeit, wirtschaftliche Verwertbarkeit und datenschutzgerechte Anwendung von KI-Technologien in vernetzten Systemen leisten einen wertvollen Beitrag zur Stärkung der technologischen Souveränität deutscher KMU.

KIASH verdeutlicht, dass die Verbindung von Künstlicher Intelligenz, Datenschutz und Vertrauenswürdigkeit nicht nur technologisch möglich, sondern auch wirtschaftlich sinnvoll und gesellschaftlich wünschenswert ist. Die Projektergebnisse bieten Anknüpfungspunkte für weiterführende Forschungs- und Industrievorhaben, etwa im Kontext von Smart Cities oder energieeffizienten Gebäuden.

5 Literaturverzeichnis

[1] Avast, „Avast - Pressezentrum“, Februar 2019. [Online]. Available: https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf.

[2] IT-Daily, „IT-Daily: Avast auf der IFA”, September 2018. [Online]. Available: https://www.it-daily.net/analysen/19429-smart-home-schon-ein-verwundbares-geraet-ist-ein-einfallstor-fuer-cyberangriffe.

[3] BMFTR, „Fortschrittsbericht zur Hightech-Strategie 2025”, Januar 2022, Available: https://www.bmftr.bund.de/SharedDocs/Publikationen/DE/1/31522_Fortschrittsbericht_zur_Hightech_Strategie_2025.pdf

[4] R. Trimananda, J. Varmarken, A. Markopoulou und B. Demsky, „PINGPONG: Packet-Level Signatures for Smart Home Device Events”, Network and Distributed Systems Security, 23-26 Februar 2020

[5] T. OConnor, R. Mohamed, M. Mettinen, W. Enck, B. Reaves und A.-R. Sadeghi, „HomeSnitch: behavior transparency and control for smart home IoT devices“, WISec '19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, pp. 128-138, Mai 2019.

[6] U. M. Aïvodji, S. Gambs und A. Martin, „IOTFLA : A Secured and Privacy-Preserving Smart Home Architecture Implementing Federated Learning“, 2019 IEEE Security and Privacy Workshops (SPW), pp. 175-180, 2019.

[7] C. Fu, Q. Zeng und X. Du, „HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes“, 30th USENIX Security Symposium (USENIX Security 21), pp. 4223-4240, 2021.

[8] CIC IoT dataset 2023, Canadian Institute for Cybersecurity, https://www.unb.ca/cic/datasets/iotdataset-2023.html

[9] Autoencoder, Wikipedia, https://de.wikipedia.org/wiki/Autoencoder

[10] Graph Neural Network, Wikipedia (Englisch), https://en.wikipedia.org/wiki/Graph_neural_network

[11] „Flower A Friendly Federated AI Framework”, https://flower.ai/

[12] „Nextcloud-Chef Frank Karlitschek: ‚Gaia-X ist tot‘”, WirtschaftsWoche, https://www.wiwo.de/technologie/digitale-welt/europaeische-cloud-initiative-nextcloud-chef-frank-karlitschek-gaia-x-ist-tot/30198440.html

[13] „Flutter - Build for any screen”, https://flutter.dev/

[14] „Flatbuffers”, https://flatbuffers.dev/

[15] „KI-gestützte Sicherheitslösung für Smart Homes”, BauNetz Wissen, https://www.baunetzwissen.de/elektro/tipps/news-produkte/ki-gestuetzte-sicherheitsloesung-fuer-smart-homes-9912204

[16] „VDC TZ Meetup am 26.09.2024 zum Thema Smart Home & Living – heute und morgen (online)”, Smart Home & Living Baden-Württemberg e.V., https://www.shl-bw.de/home/aktuelles/detail-veranstaltungen/news/detail/vdc-tz-meetup-am-26092024-zum-thema-smart-home-living-heute-und-morgen-online/

6 Abbildungsverzeichnis

Abbildung 1: Arbeitspakete (APs) des Projekts mit jeweiliger Zuständigkeit 6
Abbildung 2: Überblick über die KIASH Plattform 12
Abbildung 3: Registrierung und Einrichtung der KIASH-Box mit der KIASH-App 14
Abbildung 4: KIASH-App Dashboard und verbundene Geräte 14
Abbildung 5: KIASH-App Statusanzeige von verbundenen Geräten und Aktionen 15
Abbildung 6: Kommunikation zwischen den jeweiligen Plattformkomponenten 15
Abbildung 7: Hardware, die für den Demonstrator zur Auswahl stand: Nvidia Jetson Orin Nano (links), Raspberry Pi 5. Generation (rechts) 16
Abbildung 8: Illustration der beiden Verbindungsmodi der KIASH-Box, (links) Bridge-Mode, (rechts) DHCP-Mode 17

7 Anhang

- Anhang A: Szenarienkatalog zur Anomalieerkennung aus AP2
- Anhang B: Wissenschaftliche Veröffentlichung der Hochschule Worms: „Power Consumption Analysis as a Detection Indicator for Cyberattacks on Smart Home Devices" (Springer, 2024) – https://link.springer.com/chapter/10.1007/978-3-031-48652-4_15

Kobil GmbH

Pfortenring 11

67547 Worms

Worms 22.12.2025 Ismet Koyun Geschäftsführer