Abschlussbericht

KIASH

KI-gestützte Anomalieerkennung für Smart Homes

FKZ: 16KIS1614

Bundesministerium
für Forschung, Technologie
und Raumfahrt

Zuwendungsempfänger:

KOBIL GmbH (FKZ: 16KIS1614)
August-Wilhelm Scheer Institut für digitale Produkte und Prozesse gGmbH (FKZ: 16KIS1614)
Cleopa GmbH (FKZ: 16KIS1614)
eBZ - Das eBusiness-KompetenzZentrum im Bau- & Ausbauhandwerk gUG (FKZ: 16KIS1614)
Hochschule Worms (FKZ: 16KIS1614)
Technische Universität Chemnitz (FKZ: 16KIS1614)

Berichtszeitraum: 01.07.2022 – 30.06.2025

Autoren:

Nikolai Kamenev	August-Wilhelm Scheer Institut für digitale Produkte und Prozesse gGmbH (AWSi)

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

I. Kurzdarstellung des Vorhabens

1. Aufgabenstellung

Die zunehmende Digitalisierung privater Haushalte führt zu einer wachsenden Zahl vernetzter IoT-Geräte, die häufig unzureichend abgesichert sind. [1] Ein einziges kompromittiertes Gerät kann Angreifern den Zugang zum gesamten Heimnetz eröffnen. [2] Insbesondere Handwerksbetrieben fehlen häufig die Ressourcen (Budget, Personal, Know-how), um ihren Kunden professionelles Security-Monitoring anzubieten. Ziel des Vorhabens KIASH – KI-gestützte Anomalieerkennung für Smart Homes ist es, Integratoren, Installateure, Elektrotechniker und Handwerksbetriebe in die Lage zu versetzen, ihren Kundinnen ein einfach nutzbares, DSGVO-konformes Security-Monitoring anzubieten, und ermöglicht damit neue digitalisierte Wertschöpfungsprozesse für KMU. Herzstück ist eine KIASH-Security-Box, die lokale Datenströme kontinuierlich überwacht. Ein Federated-Learning-Ansatz (föderiertes Lernen, bei dem ML-Modelle lokal trainiert und nur Modellparameter zentral aggregiert werden) aggregiert Modelle in einer Cloudplattform, sodass sich die Erkennungsqualität ständig verbessert, ohne dass personenbezogene Rohdaten das Heimnetz verlassen. Damit reagiert das Projekt auf den Bedarf an feingranularer, datenschutzsicherer Anomalieerkennung, der mit klassischen, regelbasierten Lösungen nicht zu decken ist.

2. Voraussetzungen des Vorhabens

Das Projekt KIASH wurde als Verbundvorhaben im Rahmen einer Fördermaßnahme des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) im Bereich Informations- und Kommunikationstechnologien (IKT) mit Schwerpunkt IT-Sicherheit und Datenwissenschaft durchgeführt. Es trägt damit zur Hightech-Strategie 2025 der Bundesregierung bei, insbesondere indem kleine und mittlere Unternehmen in der Spitzenforschung und im Wissens- und Technologietransfer gestärkt werden. KIASH wurde vom BMBFTR unter dem Förderkennzeichen 16KIS1614 gefördert. Die geplante Projektlaufzeit betrug 36 Monate, vom 01.07.2022 bis zum 30.06.2025, und das Vorhaben wurde innerhalb dieses Zeitrahmens abgeschlossen.

3. Planung und Ablauf des Vorhabens

Die Projektarbeit gliederte sich in sieben Arbeitspakete, die inhaltlich aufeinander aufbauten und parallel durchgeführt wurden. Nach der von Cleopa koordinierten Anforderungsanalyse (AP1), die eine Anwendertypologie mit fünf Personas, einen Anforderungskatalog und die Systemarchitektur-Spezifikation erarbeitete, entwickelten AWSi, Hochschule Worms und Kobil in AP2 einen Szenarienkatalog mit 17 Szenarien sowie ML-Modelle (Autoencoder, Graph Neural Network) auf Basis des Flower-Frameworks. Die Datenbasis kombinierte das HSW-Hardware-Testbed mit vom AWSi kuratierten Online-Datensätzen (CICIoT-23). Parallel entwickelte die TU Chemnitz in AP3 ein Datenschutzkonzept und evaluierte die DSGVO-Konformität aller Komponenten.

Die technische Umsetzung erfolgte in AP4 und AP5: In AP4 implementierte das AWSi die Cloud-Plattform samt FL-Backend, während KOBIL die Enduser-App entwickelte. In AP5 realisierte KOBIL darauf aufbauend die Security-Box (Raspberry Pi 5) inklusive der lokalen Anomalieerkennung. In AP6 entwickelte das eBZ ein Schulungskonzept mit digitaler Lernplattform, das AWSi unterstützte beim Modul Anomalieerkennung. AP7 umfasste die von Cleopa koordinierte Wissenschaftskommunikation sowie die Veröffentlichung zweier peer-reviewter AWSi-Publikationen zur strombasierten Cyberangriffserkennung.

4. Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Frühere Arbeiten adressierten einzelne Aspekte wie Haushaltsaktivitäten oder Daten-Marktplätze, berücksichtigten jedoch weder die Datensouveränität dezentraler Nutzer noch die Notwendigkeit, heterogene Protokolle (MQTT, Zigbee, Wi-Fi) gemeinsam zu analysieren. KIASH greift diesen Forschungsstand auf, verwendet Autoencoder-Modelle und Graph-Neural-Networks für semi-supervised Learning und verlagert das Training mittels Federated Learning komplett in die lokalen Boxen. Hierdurch wird einerseits eine robuste Erkennung auch bei nicht-IID-Daten erreicht, andererseits die Einhaltung der DSGVO gewährleistet.

5. Zusammenarbeit mit anderen Stellen

Das Vorhaben wurde in enger Zusammenarbeit mehrerer Partner aus Wissenschaft und Wirtschaft umgesetzt. Zum Konsortium gehörten die KOBIL GmbH (Konsortialführer), das August-Wilhelm Scheer Institut (AWSi), die Cleopa GmbH, das eBusiness-KompetenzZentrum (eBZ), die Hochschule Worms (HSW) sowie die Technische Universität Chemnitz (TUC).
KOBIL übernahm als Konsortialführer die Koordination des Verbundprojekts sowie die Entwicklung der Hardware-Plattform für die Security-Box und der Enduser-App. Das AWSi verantwortete die Entwicklung der KI-Verfahren zur Anomalieerkennung auf Basis von Federated Learning, die Realisierung der Cloud-Plattform sowie die Kuratierung von IoT-Datensätzen. Die Hochschule Worms verantwortete den Aufbau des Hardware-Testbeds, die experimentelle Datenerfassung sowie die Entwicklung des GNN-Modells und des Device-Fingerprinting für die lokale Anomalieerkennung. Die TU Chemnitz brachte ihre Expertise im Datenschutzrecht ein und entwickelte ein umfassendes Datenschutzkonzept. Das eBZ vermittelte den Kontakt zu Handwerksbetrieben und entwickelte das Schulungskonzept. Cleopa übernahm die Leitung der Anforderungsanalyse und koordinierte die Wissenschafts- und Ergebniskommunikation.
Halbjährige Projekttreffen und zweiwöchentliche Jour Fixe förderten den Wissensaustausch. Die Projektzusammenarbeit zeichnete sich durch eine interdisziplinäre und kooperative Arbeitsweise aus, die maßgeblich zum Erfolg des Vorhabens beitrug.

6. Ergebnisse

KIASH erreichte die wesentlichen Projektziele und legte einen funktionsfähigen Demonstrator vor, der die Kernfunktionalitäten in einer Testumgebung validiert.

Die ML-basierte Anomalieerkennung erzielte unter Laborbedingungen eine Genauigkeit von bis zu 92 Prozent, wobei das Autoencoder-Modell nach 30 Federated-Learning-Runden stabil konvergierte.
Der Praxiseinsatz offenbarte jedoch erhöhte Fehlalarmraten, die primär auf die Diskrepanz zwischen dem trainierten „Idle“-Zustand und aktivem Nutzerverhalten zurückzuführen waren. Die Analyse identifizierte als zentrale Verbesserungspfade die Erweiterung der Datenbasis um aktive Nutzungsszenarien sowie die Einführung adaptiver, haushaltsspezifischer Schwellenwerte.

Das Konsortium erarbeitete einen Best Practice Guide „Secure Smart-Home" als Alternative zur ursprünglich geplanten DIN SPEC. Das AWSi veröffentlichte zwei peer-reviewte Publikationen zur strombasierten Cyberangriffserkennung: Die erste (Energy Informatics 2023, mit HSW) dokumentierte Stromverbrauchsanomalien von 10-21% bei Angriffen, die zweite (EIA Nordic 2025) erreichte mit XGBoost-Modellen F1-Scores ≥ 0,80 für acht von zehn Gerätetypen. Das Projekt demonstriert die technische Machbarkeit KI-gestützter Anomalieerkennung für Smart Homes.

II. Eingehende Darstellung des Vorhabens

7. Ziele, Ergebnisse und Zuwendungsverwendung

7.1 Anforderungsanalyse - Arbeitspaket 1

Ziel und Ausgangssituation

Ziel von AP1

Ziel von AP1 war die systematische Anforderungsanalyse als Grundlage für die technische Umsetzung in AP2–AP7. Dies umfasste die Entwicklung einer Anwendertypologie (Personas), die Identifikation technischer, funktionaler und rechtlicher Anforderungen sowie die Spezifikation der Systemarchitektur. AP1 wurde von Cleopa koordiniert. Das AWSi unterstütze und brachte insbesondere Anforderungen für Cloud-Plattform-Schnittstellen und ML-Komponenten ein.

Ausgangssituation

Zum Projektstart (06/2022) erforderte die heterogene Smart-Home-Landschaft mit proprietären Kommunikationsstandards und uneinheitlichen Sicherheitsarchitekturen eine systematische Anforderungsanalyse. AP1 erhob technische, funktionale und rechtliche Anforderungen als Grundlage für die Entwicklung der KIASH-Komponenten (AP2–AP6).

Methodik und Ergebnisse

Methodik

Die Anforderungsanalyse erfolgte durch Literaturrecherche, iterative Stakeholder-Workshops (moderiert von Cleopa, mit Handwerksbetrieben und Konsortialpartnern) und Crowd-RE-Aktivitäten. Die Ergebnisse wurden in einem kontinuierlich gepflegten Living-Document (koordiniert von Cleopa) konsolidiert. Cleopa entwickelte parallel initiale Geschäfts- und Betreibermodelle.

Rollenzuordnung im Konsortium

Cleopa koordinierte AP1 und führte die allgemeine Anforderungserhebung, Stakeholder-Workshops und Persona-Entwicklung durch. Das AWSi wirkte mit, insbesondere durch:

- Teilnahme an Stakeholder-Workshops und Crowd-RE-Aktivitäten
- Einbringen von Security-Expertise (BSI-IT-Sicherheitskennzeichen)
- Identifikation von Schnittstellen für Cloud-Plattform (AP4) und ML-Komponenten (AP2)
- Spezifikation von Anforderungen für Federated Learning (Privacy-by-Design, GAIA-X-Kompatibilität) und ML-basierte Anomalieerkennung (Datenschutz, Echtzeitfähigkeit)

Die Hochschule Worms wirkte bei der technischen Anforderungsanalyse mit, die TU Chemnitz übernahm die rechtliche Bewertung (datenschutzrechtliche Vorgaben, Compliance-Anforderungen, regulatorische Rahmenbedingungen), und das eBZ erhob federführend die spezifischen Anforderungen von Handwerkern und Installationspartnern.

Deliverables

AP1 lieferte folgende Ergebnisse: Einen **Anforderungskatalog**, konsolidiert im Living-Document, der technische, funktionale und rechtliche Anforderungen umfasst; eine **Anwendertypologie** mit fünf

repräsentativen Personas (entwickelt von Cleopa und eBZ); eine **Systemarchitektur-Spezifikation** mit High-level Architektur, Hauptkomponenten und Schnittstellen; eine **Schnittstellenliste** zur Spezifikation der Schnittstellen zwischen KIASH-Komponenten; initiale **Geschäftsmodelle** als Business-Canvas-Modelle (Cleopa); sowie eine **ELSA-Analyse** zu rechtlichen Rahmenbedingungen (TU Chemnitz).

Die Hochschule Worms, Cleopa und eBZ entwickelten in enger Zusammenarbeit mit allen Konsortialpartnern fünf repräsentative Personas, die das gesamte Nutzerspektrum abbilden:

- **Tech-affine Early Adopter** (Ernst Blofeld): Modularer Expert-Modus, offene APIs, erweiterte Konfigurationsoptionen
- **Datenschutz-orientierte Professionals** (Elina Müller): Privacy-by-Design, intuitive UI, transparente Datenschutzmechanismen
- **Security-Experten** (Linus Informatikus): Vollständige Protokollierung, Pen-Testing-Fähigkeiten, Open-Source-Komponenten
- **Mainstream-Endnutzer** (Markus Bauer): Plug-and-Play-Installation, Secure-by-Default, vereinfachte Installationsprozesse
- **Handwerks-/Installationspartner** (Aileen Neuer): Schulungs-/Zertifizierungskonzepte, spezialisierte Dashboards

Systemarchitektur-Anforderungen

Die Systemarchitektur wurde als modulares Framework mit drei Hauptkomponenten spezifiziert:

KIASH-Security-Box: Anforderungen umfassen lokale Netzwerkanalyse in Echtzeit, integrierte Anomalieerkennung ohne Cloud-Abhängigkeit, optionale Geräte-Isolation bei erkannten Bedrohungen sowie stromsparende Hardware für Dauerbetrieb.

Enduser-App: Anforderungen umfassen plattformübergreifende Verfügbarkeit, Geräteübersicht und Status-Monitoring, manuelle Korrektur von Fehlklassifikationen sowie gesteuerten, einwilligungsbasierten Handwerkerzugriff.

Cloud-Backend: Anforderungen umfassen mandantenfähige Architektur, sichere Authentifizierung und Autorisierung, Orchestrierung des Federated Learning (GAIA-X-Kompatibilität, Privacy-by-Design), Persistenz von Nutzerkorrekturen sowie Schutz vor Poisoning-Angriffen.

Die Kommunikation zwischen den Komponenten erfordert gesicherte Schnittstellen (TLS, Authentifizierung), klar definierte APIs für Interoperabilität sowie DSGVO-konforme Datenübertragung. Die detaillierte Spezifikation der ML-basierten Anomalieerkennung und des Federated Learning erfolgte in AP2.

7.2 Machine Learning-basierte Anomalieerkennung auf heterogenen IoT-Daten - Arbeitspaket 2

Ausgangssituation

Die KI-basierte Anomalieerkennung für Smart-Home-Umgebungen erforderte die Abdeckung heterogener IoT-Protokolle und gleichzeitig die Einhaltung der strengen Datenschutzanforderungen durch dezentrales Lernen. Das AWSi brachte hierbei einschlägige Vorerfahrungen aus den Projekten VICAR, Preventive QA und DatEnKoSt im Bereich der LSTM-Autoencoder und Clustering-Verfahren ein.

Projektablauf und -ergebnisse

Ziel des Arbeitspakets 2 war die Entwicklung eines KI-Modells zur Anomalieerkennung in Smart-Home-Netzen. Der Ansatz sah zwei Stufen vor: Zunächst sollte die Anomalieerkennung lokal auf der KIASH-Box erfolgen, anschließend sollten die Modelle mittels Federated Learning datenschutzkonform verbessert werden, ohne dass Nutzerdaten das Heimnetz verlassen.

Hauptaufgaben des AWSi:

- Erstellung eines Szenarienkatalogs für Normal- und Anomalieverhalten gemeinsam mit der Hochschule Worms
- Aufbau einer Datenbasis durch Kuratierung des Online-Datensatzes (CICIoT2023) in Kombination mit den vom HSW-Hardware-Testbed generierten Daten
- Entwicklung der Federated-Learning-Infrastruktur
- Bereitstellung der Infrastruktur für bidirektionale Kommunikation zwischen KIASH-Boxen und Cloud (Flower-Server als Docker-Image, API-Spezifikation)

Projektphasen:

- **2022 - Explorative Phase:** Technologie-Entscheidung für PyTorch als Deep-Learning-Framework und Flower als Federated-Learning-Framework, Workshops mit HS Worms.
- **2023-2024 - Iterative Phase:** Entwicklung Autoencoder/GNN, Testzyklen, Integration in KIASH-Security-Box.
- **2025 - Konsolidierungsphase:** Pivot zu Autoencoder, Root-Cause-Analyse Live-FPR, finale Integration.

Erstellung des Szenarienkatalogs

Die Zielsetzung dieses Arbeitsschritts war die systematische Definition normaler versus anomaler Smart-Home-Betriebszustände als Grundlage für Modelltraining und Validierung. Das Hauptergebnis war ein vollständiger Szenarienkatalog, der eine systematische Kategorisierung in 14 netzwerkbasierte Szenarien wie Netzwerküberlastung und Sicherheitsverletzungen, ein gerätebasiertes Szenario (abnorme Batterieentladung) sowie zwei Benutzerszenarien wie nicht reagierende KIASH-Boxen und veränderte Sensorwerte umfasste.

Jedes Szenario wurde mit strukturierten Metadaten (Geräte- und Sensor-Typ, Netzwerk-Protokollen, Schweregrad, Handlungsempfehlungen) versehen, um eine rückverfolgbare Datenakquise und klare Labels für das ML-Training zu gewährleisten. Die methodische Basis bildete ein umfassender Literaturreview von mehr als 30 wissenschaftlichen Publikationen zu Anomalieerkennung und Federated Learning sowie intensive multilaterale Workshops zwischen AWSi, HSW und KOBIL zur Harmonisierung von Terminologie, Tool-Stack und Use Cases.

Generierung und Aufbereitung von Datensätzen

Die Zielsetzung dieses Arbeitsschritts war die Schaffung einer belastbaren, heterogenen Datenbasis für das ML Training. Hierfür setzte das Konsortium auf einen hybriden Ansatz: Das etablierte Hardware Testbed bei der Hochschule Worms lieferte authentische Netzwerk-Traces unter kontrollierten Laborbedingungen, während das AWSi den State-of-the-Art Datensatz CICIoT2023 kuratierte.

Vorausgegangen war eine umfassende Evaluierung von mehreren potenziellen Datenquellen, darunter IoT-23 [3], Edge-IIoTset [4] sowie Datensätze zur Geräteklassifizierung (Device Classification Dataset [5]) und Nutzerverkehrsanalyse (Residential Broadband Access Traffic Dataset [4]). Die Entscheidung fiel bewusst auf CICIoT2023 [6], da er mit 33 Angriffstypen und 105 integrierten IoT-Geräten (u.a.

Philips Hue, Amazon Echo, Somfy) die aktuell umfangreichste und realistischste Topologie für Smart-Home-Sicherheitsforschung bietet.

Ergänzend initiierte das AWSi die Erfassung von hochauflösende**n** Strommessdaten während simulierter Cyberangriffe, wofür das AWSi in Kooperation mit der Hochschule Worms entsprechende Messsensorik im Hardware-Testbed integrierte. Diese multimodalen Energiedaten ermöglichten die Entwicklung eines zusätzlichen ML-basierten Erkennungsansatzes über Stromverbrauchsanomalien (siehe AP7), der eine zweite Detektionsebene bietet. Die gemessenen Stromanomalien von 10-21% bildeten die Grundlage für XGBoost-Modelle mit F1-Scores ≥ 0,80. Diese Kombination ermöglichte einerseits protokolltreue PCAP-Aufzeichnungen mit gezielter Anomalie-Injection im Hardware-Testbed und andererseits systematisch gelabelte, heterogene Gerätedaten.

Modellbildung zur Anomalieerkennung

Die Zielsetzung dieses Arbeitsschritts war die Entwicklung und Integration der eigentlichen KI Logik in die Federated Learning Pipeline durch iterative Entwicklung, Testing und Optimierung. In Zusammenarbeit mit der Hochschule Worms entwickelte das AWSi zunächst einen 5 Layer Autoencoder mit ReLU Aktivierungen und MSE Loss, der eine belastbare Baseline lieferte (Details siehe Tabelle 1). AWSi fokussierte dabei auf die Implementierung des Autoencoder-Modells und des Federated Learning-Algorithmus, während die Hochschule Worms die GNN-Architektur entwickelte.

Im Vorfeld der Pipeline Implementierung wurden OpenFL und Flower als Orchestrierungs Frameworks für das Federated Learning evaluiert. Die Entscheidung fiel auf Flower, weil es (i) die Umsetzung von Federated Learning Anwendungen mit klaren Schnittstellen und anpassbaren Strategien (z. B. Round Robin/gewichtete Aggregation) deutlich vereinfacht, (ii) gängige ML Bibliotheken wie PyTorch und Keras nativ unterstützt, sodass bestehende Modelle (Autoencoder und GNN) ohne Portierungen eingebunden werden konnten, (iii) in verteilten Setups skalierbar und produktionsreif ist, inklusive stabiler Client /Server Kommunikation und solider Fehlerbehandlung, und (iv) plattformübergreifend läuft, was die Robustheit gegenüber Hardware und Softwareänderungen (KIASH Boxen und Cloud Instanzen) erhöhte. Diese Eigenschaften reduzierten Implementierungsrisiken, beschleunigten die Experimente und erleichterten die Integration sowie das Testen von verteilten Lernprozessen. Das AWSi implementierte einen robusten Proof of Concept für Federated Learning mit Flower, bei dem vier Clients lokal trainierten und der Server die Ergebnisse aggregierte. Parallel wurde das von der Hochschule Worms entwickelte GNN-Modell evaluiert.

Aufgrund einer in den ersten sechs FL-Runden beobachteten Divergenz der GNN-Architektur (siehe Tabelle 1) erfolgte ein methodischer Wechsel auf den vom AWSi bereits im Projektverlauf entwickelten Autoencoder, dessen Implementierung in die FL-Pipeline KOBIL unterstützte; zugleich führte das AWSi den adaptiven Serverparameter bestfound_mse anstelle eines starren Schwellenwerts ein, was die Flexibilität und Anpassungsfähigkeit an unterschiedliche Deployment Szenarien erhöhte.

Die ML-basierte Anomalieerkennung mit Federated Learning stand zur Integration in die KIASH-Security-Box und Cloud-Plattform bereit. Für den gemeinsamen Zugriff wurden GitLab Repositories bereitgestellt; zusätzlich stellte AWSi zwei Entwicklerkapazitäten für das Pipeline Tuning bereit. Zum Abschluss wurde ein lauffähiges Docker Image des Flower Servers inkl. Konfiguration und das entwickelte Autoencoder-Modell (Anomalieerkennung) als separater ML-Code an KOBIL zur Integration übergeben.

Die Modellarchitektur wurde bewusst ressourcenschonend gehalten, um den Betrieb auf der KIASH-Security-Box (Raspberry Pi 5, 8 GB RAM) ohne GPU-Unterstützung zu ermöglichen. (Details zur Validierung im Live-Betrieb und den Integrationstests finden sich im Bericht zu AP 5).

Quantitative Evaluationsergebnisse und Performance-Analyse

Die quantitative Evaluation zeigt den Trade-off zwischen Modellkomplexität, Trainingsmodus und Einsatzumgebung. **Tabelle 1** fasst die Kennzahlen der wichtigsten Konfigurationen zusammen; die nachfolgende Interpretation verweist auf diese Übersicht.

Modell	Konfiguration	Metriken	Bemerkungen
Autoencoder-Baseline	Lokal, 5-Layer, ReLU	AUC: 0,81 (MSE-Schwelle: 0,001993)	Solide Baseline-Performance
GNN (zentral)	GPU-Training, 23-Klassen	Lab-Accuracy: 70-74%	Vielversprechende Ausgangslage
GNN + Federated Learning	6 Runden, 4 Clients	Accuracy: <25%	Kritischer Performance-Drop
Autoencoder + FL	30 Runden, 4 Clients	Offline-Accuracy: 92%	Beste Lab-Performance

Tabelle 1: Performance-Vergleich der entwickelten Modellarchitekturen (Fokus: Modellauswahl)

Interpretation: Die Tabelle verdeutlicht die Sensitivität dezentraler Lernverfahren gegenüber Datenheterogenität und Schwellenwert Setups. Insbesondere der Vergleich zwischen zentralem Training und Federated Learning weist auf unterschiedliche Generalisierungseffekte hin.

Fazit

In gemeinsamer Arbeit von AWSi, Hochschule Worms und KOBIL wurden (a) eine belastbare Datenbasis aufgebaut, (b) eine funktionsfähige Federated-Learning-Pipeline auf Flower implementiert und (c) ein Docker-Image des Flower-Servers sowie das Autoencoder-Modell als separater ML-Code zur Integration übergeben. Die Laborergebnisse (siehe Tabelle 1) sind solide und zeigen, dass der gewählte Autoencoder-Ansatz im Offline-Training eine hohe Genauigkeit erreicht. Die methodische Grundlage für datenschutzkonformes, dezentrales Lernen wurde damit erfolgreich geschaffen. Die Validierung dieser Modelle unter Realbedingungen erfolgte im Rahmen der Integration in Arbeitspaket 5.

7.3 Betrachtung juristischer Aspekte – Arbeitspakete 3

Laut Teilvorhabenbeschreibung (TVB) und Gesamtvorhabenbeschreibung (GVB) war das August-Wilhelm Scheer Institut nicht an diesem Arbeitspaket beteiligt.

Trotzdem unterstützte das AWSi aus Datensicht: Gemeinsam mit der Hochschule Worms wurden für die TU Chemnitz die Datenströme und Datentransfers in der KIASH-Architektur analysiert. Diese Zuarbeit half bei der Erarbeitung des Datenschutz- und Datenwirtschaftskonzepts.

7.4 Umsetzung Cloud Service und Enduser-App – Arbeitspaket 4

Ausgangssituation

Das im Dezember 2022 gestartete Arbeitspaket 4 konzentrierte sich auf die Konzeption und Implementierung einer skalierbaren Cloud-Architektur sowie einer intuitiven Enduser-Applikation. Die in AP1 erarbeiteten funktionalen und nicht-funktionalen Anforderungen flossen unmittelbar in die Entwicklung der Cloud-Plattform-Architektur und die Entwicklung der Enduser-App mit ein.

Während Arbeitspaket 2 noch an der Entwicklung von Datensätzen, Szenarienkatalog und Federated-Learning-Prototyp arbeitete, begann AP4 bereits mit der Konzeption der bidirektionalen Kommunikationsschnittstelle zwischen KIASH-Security-Box und Cloud-Plattform. Die Architektur wurde dabei so gestaltet, dass sie flexibel auf die entstehenden Komponenten aus Arbeitspaket 2 reagieren konnte. Besonders wichtig war die Vorbereitung der Infrastruktur für die spätere Integration der Anomaliedetektion und des FL-Modells.

Zu Beginn von Arbeitspaket 4 verständigten sich AWS-Institut und KOBIL in einer gemeinsamen Abstimmung auf die Aufgabenteilung: AWSi übernahm die wissenschaftlich-technische Leitung von AP4 sowie die Entwicklung der Cloud-Plattform, KOBIL die Umsetzung der Enduser-App inklusive Anbindung an die KIASH-Security-Box.

Das cloudbasierte Backend wurde so konzipiert, dass es grundsätzlich mit einem Eclipse Dataspace Connector (EDC) sowie mit GAIA-X-kompatiblen Varianten des EDC verwendet werden kann. Gleichzeitig werden die spezifischen KIASH-Anforderungen für die Verwaltung von Anomalieerkennungsmodellen unterstützt. Dies erforderte eine Architektur, die Interoperabilität zwischen verschiedenen Cloud-Providern gewährleistet und flexible Schnittstellen für die später zu integrierenden Komponenten bereitstellt.

Projektergebnisse

Die Projektergebnisse des Arbeitspakets 4 wurden durch einen systematischen, zweiphasigen Entwicklungsansatz erarbeitet, der die Implementierung einer GAIA-X-kompatiblen Cloud-Komponenten sowie die Entwicklung einer Enduser-App zur Konfiguration, Visualisierung und Dienstleistungsbeauftragung umfasste.

Cloud-Plattform

Das AWSi begann die Entwicklung der Infrastruktur mit einer Technologie-Evaluation, bei der verschiedene Ansätze wie Container-basierte Lösungen mittels Docker, Serverless-Architekturen über Azure Functions und traditionelle VM-Ansätze verglichen wurden. Diese Evaluation berücksichtigte neben Skalierbarkeit und Wartungsaufwand auch die Kompatibilität mit dem bestehenden Tech-Stack des AWSi. Die Analyse ergab, dass eine Backend-Architektur auf Basis von Azure Functions optimal geeignet ist, um bedarfsgerechte Ressourcennutzung zu ermöglichen und gleichzeitig Kosten- und Wartungsoptimierung zu gewährleisten.

Komponente	Technologie	Begründung
Backend	Azure Functions	Serverless, Skalierung, Pay-per-Use-Kostenoptimierung
Identity Management	Keycloak (Docker/EC2)	Zentrale Authentifizierung, Standards (OAuth2 und OpenID Connect), DSGVO-Konformität, Open-Source
Datenbank	Azure Cosmos DB	Global verfügbare NoSQL-Infrastruktur, Multi-Region-Deployment
API-Dokumentation	Swagger auf GitHub	Standardisierte Schnittstellen, vereinfachte Integration
Deployment	CI/CD-Pipelines	Automatisierte Qualitätssicherung, schnelle Iteration

Tabelle 2: Technologie-Stack der Cloud-Plattform

AWSi implementierte ein skalierbares Backend auf Azure Functions-Basis, das eine hochverfügbare Cloud-Plattform mit automatischer Skalierung entsprechend der tatsächlichen Systemlast ermöglicht. Diese Architekturentscheidung berücksichtigt die

sporadischen, aber rechenintensiven Verarbeitungsanfragen für die Federated Learning-Aggregation (Zusammenführung der lokal trainierten Modelle), die von der bedarfsgerechten Ressourcennutzung cloudbasierter Architekturen profitieren.

Das AWSi führte das Identity- und Access-Management-Systems Keycloak als Docker-Container auf einer Amazon EC2-Instanz ein und etablierte damit eine zentrale Authentifizierungsinfrastruktur, die die Benutzerverwaltung durch KOBIL via Keycloak-API ermöglicht und gleichzeitig die DSGVO-konformen Anforderungen bezüglich Datenschutz und Benutzerrechte erfüllt. Diese Implementierung gewährleistet Single-Sign-On-Funktionalität über verschiedene KIASH-Komponenten hinweg und ermöglicht eine granulare Rechteverwaltung für verschiedene Benutzerrollen.

AWSi setzte Azure Cosmos DB als NoSQL-Datenbankinfrastruktur ein, um global verfügbare, latenzarme Datenspeicherung für FL-Modellparameter sowie Benutzerdaten bereitzustellen. Die Datenbank bietet Replikations- und Skalierungsmöglichkeiten für eine resiliente Infrastruktur.

AWSi veröffentlichte eine Swagger-API auf GitHub, die standardisierte Schnittstellen für die Kommunikation zwischen verschiedenen KIASH-Komponenten bereitstellt. Die API-Spezifikation dokumentiert verfügbare Endpunkte, Datenformate und Authentifizierungsverfahren und unterstützt die Integration neuer Services sowie vereinfacht die Einbindung weiterer Komponenten erheblich.

Verwaltungseinheit für das KIASH-System:

Diese Komponenten bilden gemeinsam die Verwaltungseinheit des KIASH-Systems: Azure Functions übernimmt Backend-Funktionen wie die Entgegennahme und Weiterverarbeitung eingehender Modellparameter sowie die Kommunikation mit der Enduser-App. Die eigentliche Federated-Learning-Orchestrierung wird containerisiert über Azure Container Instances ausgeführt, in denen der Flower-Server läuft. Cosmos DB persistiert sowohl lokale als auch aggregierte Modellparameter. Keycloak authentifiziert und autorisiert Zugriffe von Security-Boxen und der Enduser-App. Die Swagger-API dokumentiert sämtliche Schnittstellen für die bidirektionale Kommunikation. Gemeinsam ermöglichen diese Komponenten die zentrale Verwaltung des Systems sowie die Bereitstellung der Backend-Funktionalitäten.

Security-by-Design und Privacy-by-Design:

Die Cloud-Plattform-Entwicklung folgte den **Security-by-Design-** und **Privacy-by-Design**-Prinzipien:

- **Datensparsamkeit:** Nur trainierte ML-Modelle werden übertragen, keine Smart Home-Rohdaten
- **Anonymisierung:** Federated Learning verhindert Rückschlüsse auf individuelle Haushalte
- **Verschlüsselung:** Alle Kommunikationskanäle (Box ↔ Cloud, App ↔ Cloud) nutzen HTTPS/TLS
- **Zugriffskontrolle:** OAuth2-basierte Authentifizierung via Keycloak mit granularer Rechteverwaltung

Enduser-App-Entwicklung und Szenarienkatalog

Die Konzeption der Enduser-App wurde durch die gemeinsame Erarbeitung eines umfassenden Szenarienkatalogs durch KOBIL und AWSi angestoßen, wobei jeder

Anwendungsfall mit spezifischer Zielbeschreibung, Nutzerrolle und Erfolgsbedingung dokumentiert wurde. Diese systematische Herangehensweise ermöglichte die Priorisierung der Szenarien entsprechend ihrer Relevanz für die Endnutzer und etablierte eine strukturierte Grundlage für die Implementierungsreihenfolge der verschiedenen App-Funktionalitäten.

Die Priorisierung der Szenarien erfolgte durch eine detaillierte Analyse der Nutzeranforderungen und der technischen Komplexität der jeweiligen Implementierung. Registrierung, Dashboarding und Alarm-Management wurden als primäre Funktionalitäten identifiziert, die sowohl die Benutzerfreundlichkeit als auch die technische Realisierbarkeit innerhalb des verfügbaren Projektzeitraums berücksichtigten.

Die Erstellung eines interaktiven Mock-Ups durch KOBIL wurde durch strukturiertes Feedback von AWSi zur Ausgestaltung und Nutzerführung begleitet. Diese Kollaboration etablierte eine iterative Designmethodik, die sowohl technische als auch benutzerzentrierte Aspekte berücksichtigte und die frühzeitige Identifikation von Usability-Problemen ermöglichte.

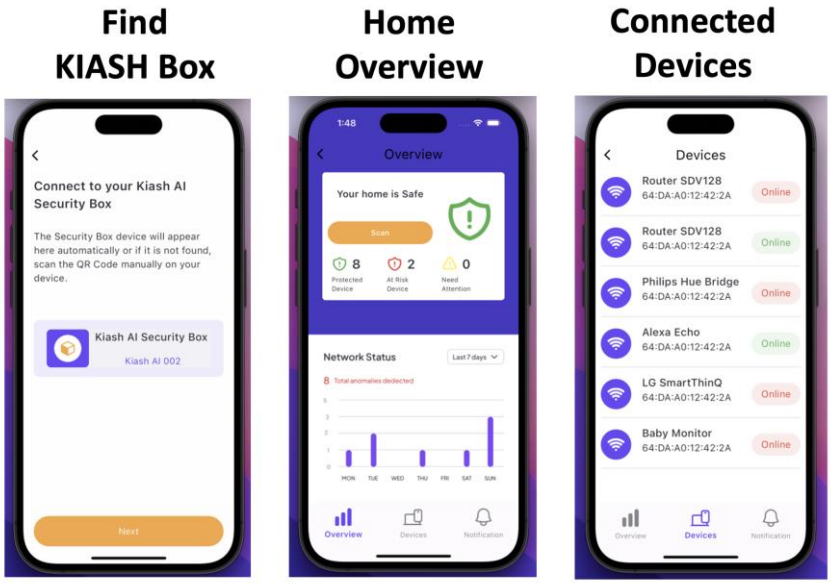

Abbildung 1: KIASH-App Auszug

Entwicklungsphasen der Enduser-App:

Die Einarbeitung des AWSi-Feedbacks sowie weiterer Rückmeldungen aus dem Konsortium führte zur Freigabe einer validierten Umsetzungsgrundlage, die als Basis für die App-Entwicklung diente. Diese iterative Herangehensweise gewährleistete, dass sowohl technische Anforderungen als auch Aspekte der Nutzererfahrung systematisch berücksichtigt wurden.

Auf dieser Grundlage entwickelte KOBIL eine erste voll funktionsfähige MVP-Version der Enduser-App, die lokal betrieben werden kann.

Funktionsumfang der MVP-Version:

Die von KOBIL auf Basis des **Flutter Frameworks** implementierte Enduser-App umfasst folgende Kernfunktionen:

1. **Registrierung und Setup:** Account-Erstellung, automatische KIASH-Box-Erkennung (QR-Code/Netzwerk-Scan)

2. **Dashboard:** Quantitative Übersicht (Anzahl verbundener Geräte), qualitative Einschätzung (grün/gelb/rot)
3. **Gerätemanagement:** Liste aller IoT-Geräte mit Detailansicht (MAC, IP, Status)
4. **Anomalie-Visualisierung:** Benachrichtigungen, Detailberichte, Empfehlungen
5. **Service-Request:** Handwerksdienstleistung auf Knopfdruck beauftragen
6. **Geräte-Isolation:** Option zum Aussperren unsicherer Geräte aus dem Netzwerk
7. **Privacy-Settings:** Konfiguration der Datenschutz-Einstellungen gemäß DSGVO

Die Umsetzung erfolgte unter Berücksichtigung von DSGVO-Vorgaben und responsive Design-Prinzipien für Desktop und Mobile.

Strategische Entscheidung für lokale Deployment-Variante

Die Entscheidung für eine **lokal ausführbare Enduser-App als Prototyp** (statt cloud-verbundener Produktivversion) wurde auf Basis einer gemeinsamen Zeit- und Risikoanalyse von KOBIL und AWSi getroffen. Die **Cloud-Plattform selbst** wurde hingegen vollständig auf Azure implementiert und ist cloud-basiert produktiv. Sie stellte eine pragmatische Antwort auf die engen zeitlichen Ressourcen und die technische Komplexität einer vollständigen Cloud-Integration dar.

Die lokale App-Variante ermöglichte die isolierte Entwicklung und Validierung zentraler ML-Komponenten (insbesondere Anomalieerkennung und Aggregationslogik für Federated Learning) ohne Abhängigkeit von produktiven Cloud-Ressourcen. Dies führte zu schnelleren Iterationen, testbaren Funktionalitäten sowie geringerer Komplexität und Risiken.

Eine direkte Cloud-Anbindung der App hätte zusätzliche Sicherheits- und Skalierungstests erfordert, deren Umsetzung den Projektzeitrahmen überschritten hätte. Der Fokus des Vorhabens lag auf den ML-Methoden, sodass sich das Konsortium bewusst für einen lokal lauffähigen Demonstrator entschied, der die Zielsetzungen des Projekts praxisnah abbildet und gleichzeitig Entwicklungsrisiken minimiert. Die Cloud-Plattform mit FL-Algorithmus, Parameter-Server und Verwaltungseinheit steht für spätere Integration bereit.

Fazit und Ausblick

Mit Arbeitspaket 4 wurde eine zentrale technologische Grundlage für das KIASH-System geschaffen: **AWSi entwickelte die Cloud-Plattform** mit FL-Algorithmus, Parameter-Server und Verwaltungseinheit, die grundsätzlich so ausgelegt wurde, dass sie mit einem Eclipse Dataspace Connector (EDC) bzw. GAIA-X-kompatiblen EDC-Varianten betreibbar wäre. Die lokal lauffähige MVP-Version der Enduser-App (entwickelt von KOBIL) setzt wesentliche Funktionalitäten wie Nutzerverwaltung, Visualisierung und Kommunikation mit der KIASH-Security-Box prototypisch um. Die enge Zusammenarbeit zwischen AWSi (wissenschaftlich-technische Leitung AP4, Cloud-Plattform) und KOBIL (App-Implementierung, Integration) sowie die klare Arbeitsteilung trugen wesentlich zur erfolgreichen, agilen Entwicklung bei.

Für eine künftige Weiterentwicklung empfiehlt sich die schrittweise Cloud-Anbindung der App-Komponenten sowie eine produktionsnahe Skalierung der Infrastruktur. Die hierfür bereits vorbereiteten Schnittstellen, Authentifizierungsverfahren und Datenmodelle bilden eine belastbare Basis, um das System über das Projekt hinaus in realen Anwendungsszenarien zu erproben und weiterzuentwickeln.

7.5 Umsetzung des Demonstrators der KIASH-Security-Box – Arbeitspaket 5

Ausgangssituation

Das von KOBIL geleitete Arbeitspaket 5 zielte auf die Entwicklung eines funktionsfähigen Demonstrators der KIASH-Security-Box. Der Fokus lag auf der Integration der IoT-Komponenten, der Implementierung der Anomalieerkennung sowie der Anbindung an die Cloud- und Service-Plattformen.

Projektergebnisse

Die Entwicklungsarbeiten konzentrierten sich auf die Umsetzung des lokalen Demonstrators. Dies ermöglichte die Validierung der Anomalieerkennung direkt auf der ressourcenbeschränkten Edge-Hardware. Die Security-Box wurde als lokaler Demonstrator erfolgreich validiert.

Deliverables und Technische Spezifikationen

Die API-Spezifikation für die Verwaltung der Security-Box wurde planmäßig fertiggestellt. Das AWSi erstellte in Kooperation mit KOBIL eine umfassende Swagger-Dokumentation, welche die Endpunkte für Geräteverwaltung, Modell-Updates und Monitoring spezifiziert.

Die Integrationstests der Federated-Learning-Schnittstelle und der lokalen Anomalieerkennung wurden planmäßig im Live-Betrieb durchgeführt. Das Testprotokoll belegt die vollständige Funktionsfähigkeit der FL-Prozesse auf der Zielhardware.

Durchgeführte Integrationstests und Validierung

Die technische Integration der ML-Komponenten auf der Raspberry Pi 5 Hardware (8 GB RAM) konnte erfolgreich nachgewiesen werden. Das abschließende Training des Autoencoders über 30 Runden konvergierte stabil.

Modell	Konfiguration	Metriken	Bemerkungen
Autoencoder-Baseline	Lokal, 5-Layer, ReLU	AUC: 0,81 (MSE-Schwelle: 0,001993)	Solide Baseline-Performance
GNN (zentral)	GPU-Training, 23-Klassen	Lab-Accuracy: 70-74%	Vielversprechende Ausgangslage
GNN + Federated Learning	6 Runden, 4 Clients	Accuracy: <25%	Kritischer Performance-Drop
Autoencoder + FL	30 Runden, 4 Clients	Offline-Accuracy: 92%	Beste Lab-Performance
Autoencoder (zentral)	300 Epochen, Full Dataset	Eval-Accuracy: 79%	Hohe Live-FPR >60%

Tabelle 3: Performance-Vergleich der entwickelten Modellarchitekturen (Integrationstest-Ergebnisse)

Die Validierung im Live-Betrieb offenbarte eine erhöhte False-Positive-Rate (>60%), deren Ursachen systematisch analysiert wurden:

1. **Repräsentativität des Nutzerverhaltens:** Abweichung zwischen dem in Testbeds trainierten "Idle"-Verhalten und dem aktiven Nutzungsverhalten von Smartphones im Realbetrieb.
2. **Schwellenwerte:** Statische MSE-Schwellen ignorierten haushaltsspezifische Dynamiken.
3. **Label-Qualität:** Verstärkung von Fehlern durch iteratives Pseudo-Labelling.
4. **Betriebsdrift:** Fehlende Erfassung von Firmware-Updates und Nutzungsänderungen.

Fazit und Verwertung

Die Fokussierung auf den lokalen Demonstrator erlaubte die Konzentration auf die forschungsrelevanten Aspekte der Edge-AI. Die durchgeführten Integrationstests bestätigten die technische Machbarkeit des Ansatzes. Die Hardware bewältigte die Last der lokalen Anomalieerkennung und der FL-Runden stabil. Die im Live-Betrieb gewonnenen Erkenntnisse zur False-Positive-Rate liefern essentielle Implikationen für die Weiterentwicklung der Datenbasis und Schwellenwert-Logik.

Ausblick

Basierend auf den Integrationsergebnissen wird für künftige Iterationen die Einführung von selektivem Federated Learning und adaptiver Drift-Detektion empfohlen, um die Robustheit im operativen Einsatz zu steigern.

7.6 Pilotphase, Demonstrator-Optimierung, Weiterbildung und Zertifizierung – Arbeitspaket 6

Ausgangssituation

Arbeitspaket 6 zielte auf eine praxisnahe Pilotphase und ein umfassendes Schulungskonzept für Handwerksbetriebe ab. eBZ koordinierte die Pilotphase mit vier Handwerksbetrieben, wobei AWSi fachliche Unterstützung zu Cloud- und Federated Learning-Komponenten leistete.

Zielsetzung und Neujustierung

Das übergeordnete Ziel von AP6 war die Entwicklung eines übertragbaren Weiterbildungs- und Zertifizierungskonzepts für die KIASH-Technologie. Dieses sollte sowohl technische als auch didaktische Anforderungen berücksichtigen, um die Technologie insbesondere für nicht-technische Zielgruppen zugänglich zu machen.

Das AWSi brachte seine Expertise in digitaler Bildung und didaktischer Konzeption gezielt in die Entwicklung der Schulungsplattform ein. Die Teilnahme an Pilotanwender-Workshops erfolgte in Form von fachlichem Input und Usability-Reviews für die Schulungsplattform.

Beitrag zur Schulungsplattform

Die Schulungsplattform *„Smart Home IT-Sicherheit“* basiert auf einem vierstufigen Weiterbildungskonzept, das in enger Zusammenarbeit mit dem Konsortium entwickelt wurde:

1. **Sensibilisieren**: Einführung in Smart-Home-Technologien, Datenschutz und potenzielle Risiken, ergänzt durch ein interaktives Quiz.
2. **Informieren**: Vermittlung technischer Grundlagen zur IT-Sicherheit und Netzwerkarchitektur anhand praxisnaher Fallstudien.
3. **Qualifizieren**: Praxisnahe Schulung zur Installation, Konfiguration und Nutzung der KIASH-Security-Box inklusive Anomalieerkennung.
4. **Vernetzen**: Aufbau eines digitalen Netzwerks für Erfahrungsaustausch und kontinuierliche Weiterbildung.

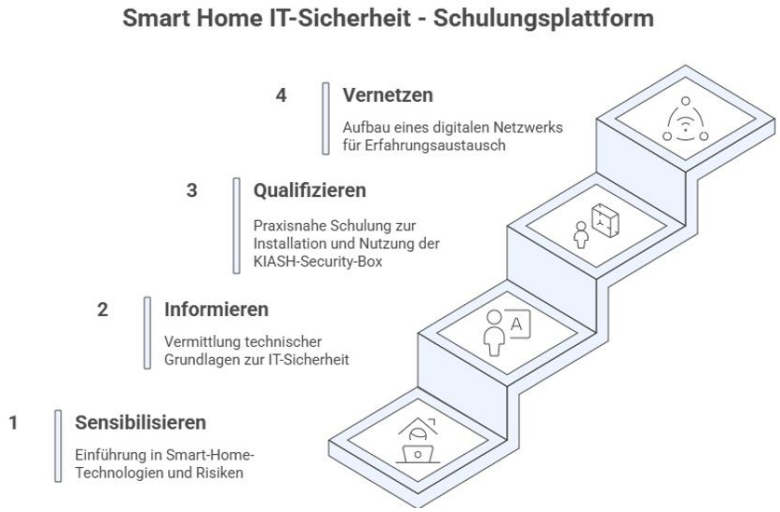

Abbildung 2: Smart Home IT-Sicherheit - Schulungsplattform Modularer Aufbau

Das AWSi entwickelte im Rahmen dieses Konzepts ein Fachmodul zur Anomalieerkennung im Smart-Home-Kontext. Zusätzlich unterstützte das AWSi die Plattform durch Usability-Reviews, didaktisches Feedback sowie Qualitätssicherung beim Einpflegen der Inhalte.

Einschätzung und Ausblick

Das entwickelte Fachmodul bietet eine fundierte, praxisnahe Schulungsgrundlage für Handwerksbetriebe (z. B. Elektrotechniker, Smart-Home-Integratoren), die auch ohne tiefgehende KI- oder Cloud-Vorkenntnisse verständlich ist. Die Pilotphase mit vier Betrieben lieferte wertvolles Feedback zur Plattform-Usability, das in die finale Version der Schulungsmodule einfloss.

Für eine nachhaltige Weiterentwicklung der Schulungsplattform empfiehlt sich, reale Nutzergruppen (z. B. Handwerksbetriebe, Fachschulen, Weiterbildungsträger) künftig aktiv in die Erprobung und Evaluation einzubinden. Damit kann sichergestellt werden, dass Inhalte, Formate und Anwendungsszenarien noch besser an den konkreten Bedarf angepasst und die langfristige Verbreitung der KIASH-Technologie unterstützt werden.

7.7 Normung und Wissenschaftskommunikation – Arbeitspaket 7

Ausgangssituation

Arbeitspaket 7 wurde konsortiumsweit unter Koordination von Cleopa bearbeitet. Alle Partner trugen zur Wissenschaftskommunikation und Öffentlichkeitsarbeit bei, das AWSi mit Schwerpunkt auf wissenschaftlicher Dissemination. Arbeitspaket 7 begleitete das KIASH-Vorhaben als Querschnittsaktivität von Beginn an. Ziel war es, Forschungsergebnisse kontinuierlich zu disseminieren, den Wissenstransfer sicherzustellen und die Sichtbarkeit des Projekts in der wissenschaftlichen Community zu erhöhen. Gleichzeitig sollten praxisnahe Erkenntnisse für eine spätere Standardisierung vorbereitet werden.

Ursprünglich war laut Gesamtvorhabenbeschreibung die Entwicklung einer DIN SPEC vorgesehen, um die Projektergebnisse in Form einer technischen Spezifikation zu verstetigen. Auf Empfehlung des Projektträgers wurde jedoch von der Erstellung verbindlicher technischer Dokumente abgesehen. Stattdessen entstand ein praxisorientierter Best Practice Guide, der freiwillige Handlungsempfehlungen zur sicheren Gestaltung von Smart-Home-Umgebungen zusammenfasst.

Wissenschaftliche Dissemination und Forschungsergebnisse

Das August-Wilhelm Scheer Institut (AWSi) trug mit zwei peer-reviewten Publikationen maßgeblich zur wissenschaftlichen Verbreitung der Projektergebnisse bei:

1. **Schorr V., Kamenev N., Bleistein T., Werth D., Wendzel S., Weigold T. (2023):** *„Power Consumption Analysis as a Detection Indicator for Cyberattacks on Smart Home Devices"*. In: Energy Informatics – Lecture Notes in Computer Science, Vol. 14468, pp. 224–239. Energy Informatics.Academy Conference 2023 (EI.A 2023), Campinas, Brasilien (Präsentation online). DOI: 10.1007/978-3-031-48652-4_15. Die Publikation entstand in Kooperation mit der Hochschule Worms (Ko-Autoren: Wendzel S., Weigold T.).

   Die Studie integrierte hochauflösende Energiesensorik in das Wormser Testbed und zeigte Stromverbrauchsanomalien von 10 – 21 % bei simulierten Cyberangriffen. Vier charakteristische Muster ermöglichten eine geräteübergreifende Angriffserkennung.

2. **Becker R. A., Kamenev N., Koelsch C., Kulkarni A., Bleistein T. (2025):** *„Machine Learning-Based Cyberattack Detection in Power Data"*. In: Energy Informatics – Lecture Notes in Computer Science, Part II, pp. 285–299. Nordic Energy Informatics Academy Conference 2025 (EIA Nordic 2025), Stockholm, Schweden (August 20–22, 2025, Präsentation vor Ort). DOI: 10.1007/978-3-031-74741-0_20. Publikationsdatum: 01 November 2025. Diese Publikation wurde ausschließlich vom AWSi-Team verfasst und baut auf den gemeinsamen 2023er-Vorarbeiten mit der Hochschule Worms auf.

   Aufbauend auf den 2023er-Daten entwickelte das AWSi eine Feature-Engineering-Methodik (Peaks > 3 W / 5 s + Varianz 30 s). XGBoost-Modelle erzielten F1-Scores ≥ 0,80 für acht von zehn Gerätetypen und behielten bei unbekannten Geräten ≥ 75 % ihrer Leistung.

3. **Kamenev N., Werth D. (2024):** *„Stand your digital ground – Wie Smart Homes sicher bleiben"*. IM+io – Magazin für digitale Transformation (Online-Fachbeitrag, 22.05.2024). Der Beitrag adressierte Fachpublikum und breitere Öffentlichkeit mit praxisorientierten Empfehlungen zur Smart-Home-Sicherheit.

Technologietransfer und Kommunikation

Cleopa koordinierte die Öffentlichkeitsarbeit des Konsortiums, einschließlich der Projekt-Website kiash.de und der LinkedIn-Kampagne. Das AWSi unterstützte diese Aktivitäten durch Bereitstellung von Bildmaterial, Abstracts und Kurzbeschreibungen der ML-Komponenten sowie durch Unterstützung bei der Erstellung von Präsentationsmaterial für Messepräsentationen. Das AWSi bediente den wissenschaftlichen Diskurs mit Publikationen und Konferenzen; Präsentationen auf der Energy Informatics.Academy erleichterten den Austausch mit internationalen Forschungsgruppen. Das AWSi trug mit Feedback zu technischen Kapiteln zum von Cleopa koordinierten Best Practice Guide bei, der unter Mitwirkung aller Konsortialpartner entstand und KMU sowie Integratoren praxisnahe Handlungsempfehlungen bietet.

Fazit

Das AWSi hat alle im Arbeitsplan vorgesehenen Aufgaben des Arbeitspakets 7 erfüllt. Die Publikationen erhöhen die wissenschaftliche Sichtbarkeit des KIASH-Projekts in der internationalen Forschungscommunity, während die Beiträge zum Best-Practice-Guide eine praxisorientierte Grundlage für künftige Produktentwicklungen und mögliche Standardisierungen schaffen. Die Unterstützung der von Cleopa koordinierten Öffentlichkeitsarbeit trug zur Verbreitung der Projektergebnisse bei. Damit trägt Arbeitspaket 7 wesentlich zur Verwertung der Projektergebnisse und zur Vorbereitung von Anschlussinitiativen im Bereich Smart-Home-Security bei.

8. Zahlenmäßiger Nachweis

Für den zahlenmäßigen Nachweis verweisen wir auf die partnerspezifischen Verwendungsnachweise.

9. Notwendigkeit und Angemessenheit der geleisteten Arbeit

Angesichts der wachsenden Zahl vernetzter Geräte in und der damit verbundenen Sicherheitsrisiken bestand ein klarer gesellschaftlicher Bedarf an vertrauenswürdigen Sicherheitslösungen. Bestehende Ansätze erforderten zentrale Datenverarbeitung und waren für KMU im Handwerk nicht praktikabel. Die vom AWSi im Rahmen von KIASH durchgeführten Arbeiten waren notwendig, um diese Lücke durch einen datenschutzkonformen Federated Learning-Ansatz zu schließen. Die gewählte Vorgehensweise war methodisch angemessen, um Datenschutz und technische Machbarkeit in Einklang zu bringen.

Dem Vorhaben KIASH lag ein interdisziplinärer Ansatz zugrunde, der informationstechnische, elektrotechnische und datenschutzrechtliche Fragestellungen gemeinsam adressiert, um eine innovative Lösung für die KI-gestützte Anomalieerkennung in Smart Homes zu entwickeln. Im Fokus stand die Kombination von maschinellem Lernen, insbesondere Federated Learning, mit einer sicheren Cloud-Infrastruktur und einem benutzerfreundlichen Endnutzer-Zugang. Das Vorhaben war dabei mit einem nicht unerheblichen Risiko behaftet, sowohl auf technischer als auch auf organisatorischer Ebene. Insbesondere die sichere Verarbeitung und Aggregation heterogener Smart Home-Daten in einem Federated Learning-System sowie die Entwicklung geeigneter Machine-Learning-Modelle für Anomalieerkennung auf Netzwerkdaten stellten technologische Herausforderungen dar. Eine limitierte Verfügbarkeit geeigneter und gelabelter Datensätze sowie die heterogene Datenstruktur führten zu zusätzlichem Forschungsaufwand.

Für die Datengenerierung setzte das Konsortium auf einen hybriden Ansatz aus kuratierten Online-Datensätzen und dem Hardware-Testbed der Hochschule Worms. Diese Kombination gewährleistete systematisch gelabelte Angriffsmuster, protokolltreue PCAP-Traces sowie zügige Verfügbarkeit im Projektzeitplan.

Der ursprünglich verfolgte Ansatz eines komplexen Klassifikators zur Unterscheidung verschiedener Angriffstypen im Federated Learning erwies sich als nicht praxistauglich, da die Modellgenauigkeit mit zunehmenden Lernrunden signifikant abnahm. Stattdessen wurde ein Autoencoder-basiertes Verfahren zur Anomalieerkennung in Kombination mit Federated Learning implementiert und optimiert. Diese Lösung stellte sich hinsichtlich der Generalisierbarkeit und Stabilität als vorteilhafter heraus.

Trotz der genannten Herausforderungen konnten wesentliche Komponenten, wie ein funktionaler Demonstrator der Cloud-Plattform sowie der Federated-Learning-Umgebung, erfolgreich umgesetzt und dem Industriepartner bereitgestellt werden.

10. Voraussichtlicher Nutzen und Verwertbarkeit

August-Wilhelm Scheer Institut

Die im Projekt KIASH entwickelten Konzepte zur KI-basierten Anomalieerkennung auf Basis von Energiedaten und Netzwerkverkehr sowie der Einsatz des Federated Learning (FL) bilden für das AWSi eine wichtige Grundlage für künftige Forschungs- und Transferprojekte im Bereich Smart Home Security und IoT-Datensicherheit. Insbesondere die sichere, datenschutzkonforme Verarbeitung von Smart-Home-Daten im FL-Ansatz unter Nutzung des Flower-Frameworks wird als Basis für die Weiterentwicklung datensouveräner KI-Anwendungen genutzt.

Der entwickelte FL-Prototyp und die dabei gewonnenen Erkenntnisse hinsichtlich Heterogenität der Daten, Client-Authentifizierung und Absicherung der Kommunikation werden in künftigen Forschungsprojekten des AWSi weiterverwendet und weiterentwickelt. Ziel ist es, FL-basierte Anomalieerkennungsmethoden auch in anderen Kontexten wie industriellen IoT-Umgebungen oder kritischen Infrastrukturen zu erproben und für den praktischen Einsatz zu optimieren.

Die gewonnenen Ergebnisse und Erfahrungen fließen zudem in wissenschaftliche Publikationen, Präsentationen auf Fachkonferenzen und in Qualifikationsarbeiten ein und stärken so das Forschungsportfolio des AWSi im Bereich Cybersicherheit und Privacy-Preserving Machine Learning. Überdies dienen die Konzepte als Ausgangspunkt für Beratungs- und Schulungsangebote rund um sichere KI-Architekturen und datenschutzgerechte Datenverarbeitung in verteilten Systemen. KIASH bildet damit die Grundlage für eine strategische Ausweitung des Themenfeldes am Institut.

11. Bekannt gewordener Fortschritt auf Gebiet des Vorhabens bei anderen Stellen

Die zunehmende Verbreitung von Smart-Home-Anwendungen, 46% der deutschen Haushalte nutzen 2024 mindestens eine solche Technologie, [7] hat zu verstärkten Forschungsaktivitäten im Bereich Smart-Home-Sicherheit geführt. Während der KIASH-Projektlaufzeit wurden parallel mehrere Forschungsprojekte durchgeführt, die verwandte Problemstellungen adressieren.

Das EU-Projekt SIFIS-HOME (2020-2023) entwickelte eine Sicherheits- und Privacy-Architektur für Smart-Home-Gateways mit Fokus auf Gateway-Ebene. [8] Das BMBF-Projekt IoTGuard (2023-2026) erforscht KI-basierte Angriffserkennung in Smart-Home-Netzen mit Schwerpunkt auf Verhaltensanalyse einzelner Geräte. [9] Das EU-Projekt MEDIATE (2024-2027) kombiniert Zero-Trust-Architekturen mit Federated Learning für unternehmensweite Threat-Intelligence-Systeme. [10]

KIASH unterscheidet sich von diesen Ansätzen durch die spezifische Ausrichtung auf Handwerks-KMU als Zielgruppe und die Integration von drei Komponenten in einer praxisorientierten Gesamtlösung: Federated Learning zur datenschutzkonformen Modellverbesserung, lokale Anomalieerkennung auf Edge-Geräten (Security-Box) und eine Cloud-Plattform für zentrale Dienste. Diese Kombination adressiert die besonderen Anforderungen kleiner Handwerksbetriebe, die weder über eigene IT-Infrastruktur noch über Sicherheitsexperten verfügen.

Der regulatorische Rahmen entwickelt sich parallel zur KIASH-Forschung: Der Cyber Resilience Act (ab 2027), die NIS2-Richtlinie und der AI Act formulieren erweiterte Sicherheits- und Transparenzanforderungen für vernetzte Geräte und KI-Systeme. [11] [12] Die im KIASH-Projekt entwickelten Ansätze zur datenschutzkonformen Anomalieerkennung und zum transparenten Federated Learning adressieren zentrale Anforderungen dieser Regulierungen.

12. Veröffentlichungen der Ergebnisse

Während der Forschungsarbeit am Projekt KIASH konnten mehrere Fachartikel, ein Fachbeitrag sowie Beiträge zu Leitfaden- und Normungsarbeiten erstellt werden. Zudem wurden die Ergebnisse des Forschungsprojekts im Rahmen von Konferenzen, Kongressen und Messeauftritten vorgestellt.

Veröffentlichungen

- Schorr V., Kamenev N., Bleistein T., Werth D., Wendzel S., Weigold T.: „**Power Consumption Analysis as a Detection Indicator for Cyberattacks on Smart Home Devices**“. In: *Energy Informatics* – Lecture Notes in Computer Science, Vol. 14468, pp. 224–239 (12 / 2023). DOI: 10.1007/978-3-031-48652-4_15
- Becker R. A., Kamenev N., Koelsch C., Kulkarni A., Bleistein T.: „**Machine Learning-Based Cyberattack Detection in Power Data**". Nordic Energy Informatics Academy Conference 2025 (EIA Nordic 2025), Stockholm, Schweden (20.-22. August 2025). DOI: 10.1007/978-3-032-03098-6_19
- Kamenev N., Werth D.: „**Stand your digital ground – Wie Smart Homes sicher bleiben**“. *IM+io – Magazin für digitale Transformation* (Online-Fachbeitrag, 22.05.2024), unter: https://www.im-io.de/stand-your-digital-ground/ (letzter Aufruf: 22.07.2025) IM+io
- Cleopa u. a.: „**Best Practice Guide »Secure Smart-Home« – Handlungsempfehlungen für Integratoren und Handwerksbetriebe**“ (in Vorbereitung, geplante Veröffentlichung Q3 / 2025).

Messen, Kongresse und Konferenzen

- E*nergy Informatics.Academy Conference 2023* (EI.A 2023), Campinas – Online-Vortrag & Paper (6.-8. Dezember 2023)
- *Nordic Energy Informatics Academy Conference 2025 (EIA Nordic 2025), Stockholm – Vortrag & Paper (20.-22. August 2025)*

Damit ist der Wissenstransfer in die wissenschaftliche Community, die Fachpresse und die Praxis sichergestellt und bildet zugleich eine solide Grundlage für die nachhaltige Verwertung der Projektergebnisse.

III. Verweise

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Die Lage der IT-Sicherheit in Deutschland 2024," Bonn, 2024.

[2] Federal Bureau of Investigation (FBI), „Home Internet Connected Devices Facilitate Criminal Activity," Washington, D.C., 2025.

[3] S. Garcia, A. Parmisano und M. J. Erquiaga, „IoT-23: A labeled dataset with malicious and benign IoT network traffic," Prag, 2020.

[4] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras und H. Janicke, „Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access,* Bd. 10, p. 40281–40306, 2022.

[5] L. Bai, L. Yao, S. S. Kanhere, X. Wang und Z. Yang, „Automatic Device Classification from Network Traffic Streams of Internet of Things," in *2018 43rd IEEE Conference on Local Computer Networks (LCN)*, Osaka, Japan, 2018.

[6] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu und A. A. Ghorbani, „CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors,* Bd. 23, Nr. 13, p. 5941, 2023.

[7] Bitkom Research, „Smart-Home-Anwendungen in fast jedem zweiten Zuhause," Berlin, 2024.

[8] CORDIS, „CORDIS," 2023. [Online]. Available: https://cordis.europa.eu/project/id/952652. [Zugriff am 31 7 2025].

[9] Bundesministerium für Bildung und Forschung (BMBF), „IoTGuard – Intelligente Erkennung von Angriffen gegen IoT Netzwerke in Smart Homes," 2024. [Online]. Available: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/iotguard. [Zugriff am 31 7 2025].

[10] Fundación Valenciaport, „Fundación Valenciaport," 11 2024. [Online]. Available: https://www.fundacion.valenciaport.com/en/news-events/2024/11/mediate-the-european-project-to-ensure-the-flow-and-security-of-information-in-freight-traffic-kicks-off/. [Zugriff am 31 7 2025].

[11] Europäische Kommission, „Shaping Europe's digital future," 06 03 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. [Zugriff am 31 7 2025].

[12] Europäische Kommission, „Shaping Europe's digital future," 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/de/policies/nis2-directive. [Zugriff am 31 7 2025].