

WearPrivate

Kurzbericht zum Teilvorhaben (I. Kurze Darstellung)

Zuwendungsempfänger: WearHealth GmbH

Förderkennzeichen: 16KIS1514

Vorhabenbezeichnung: WearPrivate

Teilvorhaben: Anonymisierte Wearables-basierte Analytics für HSE

Laufzeit des Vorhabens: 01.09.2021 – 30.11.2024



1. Aufgabenstellung und Zielsetzung

Unternehmen wollen Arbeitssicherheit und Gesundheit fördern, ohne Mitarbeitende zu überwachen. Bestehende Verfahren zur Beurteilung von Arbeitsbelastung sind jedoch häufig subjektiv und reaktiv. Ziel des WearHealth-Teilvorhabens in WearPrivate war daher die Entwicklung und Validierung eines DSGVO-konformen Cloud-Services, der Daten aus Wearables über eine mobile App erfasst, on-the-fly verarbeitet und daraus a) Risikobenachrichtigungen, b) individuelle arbeitsbelastungsbezogene Empfehlungen sowie c) anonymisierte Team-Einblicke für HSE-Verantwortliche ableitet. Zentrale Leitplanken waren End-to-End-Anonymisierung, Transparenz und Selbstbestimmung der Beschäftigten, umgesetzt in Architektur, APIs, Dashboard und einem mit Stakeholdern abgestimmten Evaluationsplan.

2. Wissenschaftlich-technischer Stand

Das Verbundvorhaben baute auf datenschutzfreundlicher Systemarchitektur mit strikter Rollentrennung auf, verankerte Datennutzungskontrolle (MYDATA/XACML-Prinzipien) und kombinierte Anonymisierungs-/Aggregationsverfahren mit benutzbaren Interaktionskonzepten (z. B. Privacy-Dashboard, Ereignisprotokoll, zeit-/ortabhängige Erfassung). Für individuelles Feedback wurden Differential-Privacy-(DP)-Ansätze untersucht und die Auswirkung des Schutzparameters ϵ auf die Analysequalität (Sensitivität) evaluiert. Diese Bausteine wurden so gestaltet, dass sie auch Nicht-IT-Fachleuten vermittelbar sind und die freiwillige Teilnahme fördern.

Zusätzlich stützte sich die Entwicklung der KI-basierten Belastungsalgorithmen auf biomedizinische biomedizinischer Literatur und orientierte sich an einschlägigen Industriestandards, u. a. ISO 10075-1:2017, ISO 10075-2:1996, ISO 10075-3:2004, ISO 8996:2004 und ISO 6385:2016.

3. Ablauf des Vorhabens

Das Teilvorhaben lief planmäßig über die Gesamtprojektlaufzeit (01.09.2021–31.08.2024) und folgte einer iterativen Roadmap von der Anforderungserhebung über Architektur/Implementierung bis zu Integration, Demonstrator und Evaluation.

Anforderungsphase (AP1): WearHealth erhob und dokumentierte technische Datenschutzerfordernisse als Grundlage der Software-/Cloud-Architektur. Die Umplanung durch den Partnerwechsel (ambiotex → neusta mobile solutions) beeinträchtigte die Zielerreichung nicht.

Architektur & Prototyping (AP2–AP4): Beim Jahrestreffen am 12.10.2022 in Bremen wurden Sensorik, App-Architektur und Cloud-Analytics abgestimmt. Auf AWS wurde die Zielarchitektur validiert, Kommunikationsprotokolle und Echtzeit-Analysedienste aktiviert, Datenspeicher nach Verwendungszweck separiert und ein Secure Software Development Lifecycle (SSDLC) etabliert. Parallel wurden Konzepte für Transparenz und Selbstbestimmung mit den Partnern ausgearbeitet.

Integration, Demonstrator & Evaluation (AP3–AP6): Beim Jahrestreffen am 23.–24.08.2023 in Kaiserslautern wurden Umsetzungsstand und Demonstratoren zusammengeführt. Die Cloud-API wurde freigeschaltet, App-Integration umgesetzt und getestet; Verschlüsselung und Schutzmechanismen ergänzt. Für HSE-Manager entstand ein Web-Dashboard (Node.js) zur Darstellung anonymisierter Trends. Die Cloud-Prozesse (inkl. Protokolle/Interaktion mit der App) wurden evaluiert/optimiert; Nutzergruppen und Validierungsschritte wurden gemeinsam festgelegt.

4. Wesentliche Ergebnisse

- a) Funktionsfähiger, DSGVO-konformer Cloud-Service mit API und App-Anbindung. Die Plattform erfasst Wearable-Daten über die mobile App, verarbeitet sie in nahezu Echtzeit und stellt – ausschließlich nach Einwilligung – anonymisierte Analysen und Trends bereit. Die Architektur und Dienste wurden auf AWS entworfen, abgesichert und in Betrieb genommen.
- b) Datenschutz „by design“ mit Datennutzungskontrolle und klarer Transparenz. Die Verbundkonzepte zu Datennutzungskontrolle (Policy-basierte Steuerung der Verarbeitung/Nutzung/Weitergabe) bilden das Rückgrat der Lösung. Auf Nutzerseite wurden Privacy-Einstellungen und Nachvollziehbarkeit (z. B. Ereignisprotokoll, Visualisierung von

Datenflüssen, Speicherbegrenzung) realisiert, damit Beschäftigte die Datennutzung verstehen und steuern können.

- c) Differential Privacy für individuelles Feedback – mit geprüfter Sensitivität. Für vitale und kontextuelle Daten wurden DP-Mechanismen konzipiert und im Verbund evaluiert. Die Sensitivitätsanalyse zeigt, wie sich unterschiedliche ϵ -Werte auf Klassifikations-/Erkennungsqualität auswirken – eine Grundlage, um Schutz und Nützlichkeit zielgruppengerecht auszubalancieren.
- d) Dashboard für HSE-Manager mit anonymisierten Team-Einblicken. Das Web-Dashboard (Node.js) stellt aggregierte Belastungsindikatoren und Trendverläufe teambezogen dar. Gruppenberichte unterstützen das betriebliche Gesundheitsmanagement dabei, Überlastungen zu erkennen und präventive Maßnahmen abzuleiten, ohne individualisierbare Leistungsdaten offenzulegen.
- e) Integration, Tests und Optimierungen. Die Cloud-API wurde für die App geöffnet, Datenübertragung und -verarbeitung getestet und Sicherheitsmechanismen (u. a. Verschlüsselung, Protokollhärtung) ergänzt. In der Evaluation wurden Kommunikationsprotokolle, Cloud-Prozesse und die App-Interaktion überprüft und iterativ verbessert; Nutzergruppen und Validierungsszenarien wurden gemeinsam mit den Partnern festgelegt.
- f) KI-getriebene Workload-Algorithmen (HR/HRV). Die Analytik wurde dahingehend erweitert, dass aus Herzfrequenz (HR) und Herzratenvariabilität (HRV) des über die App verbundenen Wearables ein Belastungsindex sowie Belastungsklassen (z. B. MENTAL, PHYSICAL, MIXED, RECOVERY) in nahezu Echtzeit abgeleitet und als Hinweise in der App bzw. als Trends im Dashboard bereitgestellt werden. Bei aktivierter Differential Privacy zeigt sich eine systematische Unterschätzung der Belastung (durch tendenziell erhöhte HRV-Werte); dies kann durch DP-bewusstes Training der KI kompensiert werden.

5. Zusammenarbeit mit anderen Forschungseinrichtungen

Das Teilvorhaben profitierte von enger, arbeitsteiliger Kooperation: Fraunhofer IESE verantwortete u. a. Sicherheitsarchitektur, bedrohungsgeleitete Anforderungserhebung und die Systematik der Datennutzungskontrolle; Universität des Saarlandes (UdS) entwickelte Anonymisierungs-/Aggregationskonzepte und bewertete rechtlich-ethische Aspekte; neusta mobile solutions (NMS) verantwortete die mobile App und trug zur Gesamtintegration des Demonstrators bei. Die gemeinsame Ausgestaltung von Transparenz-/Selbstbestimmungskonzepten, die Jahrestreffen 2022 (Bremen) und 2023 (Kaiserslautern) sowie fortlaufende Abstimmungen stellten Konsistenz von Architektur, Datenschutz und Usability sicher.

6. Kurzfazit

Das WearHealth-Teilvorhaben liefert einen pragmatisch einsetzbaren, abgesicherten Cloud-Service mit App-Schnittstelle und anonymisiertem HSE-Dashboard, verankert in Datennutzungskontrolle und Differential Privacy. Damit ist eine allgemein verständliche, datenschutzfreundliche Nutzung von Wearables im Arbeitskontext möglich mit unmittelbarem Mehrwert für Mitarbeitende (Feedback/Empfehlungen) und Arbeitgeber (präventive Team-Einblicke), ohne Leistungsüberwachung zu ermöglichen.