FACE ID

IMS Projekt

24. APRIL 2024

IMS
Lorrainestrasse 1, 3014 Bern

Inhalt

Management Abstract

Anlass des Projektes
In einer Welt, in der immer mehr online passiert, ist es wichtig, dass Benutzerkonten sicher sind. Unser Projekt sollte eine Methode entwickeln, die sicher ist und einfach zu benutzen, damit niemand unerlaubt auf persönliche Daten zugreifen kann. Gleichzeitig sollte sie den Zugang zu Diensten oder Anwendungen vereinfachen.

Ausgangslage
Viele Leute nutzen schwache Passwörter oder verwenden dasselbe Passwort für mehrere Dienste, was das Risiko für Hackerangriffe erhöht. Traditionelle Methoden wie Passwörter oder Tokens haben oft Schwachstellen und sind manchmal kompliziert in der Anwendung. Daher wollten wir eine Lösung finden, die sowohl sicher als auch einfach zu bedienen ist. Wir entschieden uns, eine biometrische Lösung zu testen, die das Beste aus beiden Welten vereint.

Ziele
Unser Ziel war es, ein Face ID-System zu entwickeln, das den Zugang zu Diensten sicher und einfach macht. Benutzer sollten sich anmelden können, indem sie ihr Gesicht scannen lassen und dann, wenn sie den Dienst erneut nutzen möchten, einfach ihren Benutzernamen und ihr Gesicht verwenden können.

Resultate
Das Ergebnis unseres Projekts ist ein funktionierendes Face ID-System. Benutzer registrieren sich, indem sie ein Bild ihres Gesichts erstellen. Diese biometrischen Daten werden verschlüsselt und sicher gespeichert. Danach können sie sich mit einem einfachen Face Scan und ihrem Benutzernamen in das System einloggen. Das macht den Anmeldeprozess einfacher und erhöht die Sicherheit, da Gesichtsmerkmale einzigartig sind und schwer kopiert werden können.

Erfahrungen
Bei der Entwicklung des Face ID-Systems haben wir viel gelernt. Eine der grössten Herausforderungen war, sicherzustellen, dass das System auch bei verschiedenen Lichtverhältnissen oder Änderungen im Aussehen des Benutzers zuverlässig funktioniert. Wir mussten auch darauf achten, dass die biometrischen Daten geschützt und sicher gespeichert werden. Unsere Erfahrungen zeigen, dass biometrische Authentifizierungssysteme sicher und benutzerfreundlich sein können, wenn man sie richtig umsetzt.

Deklarationen

Deklaration der Vorkenntnisse

Als Gruppe bringen wir bereits solide Kenntnisse in den Bereichen HTML, CSS und JavaScript mit. Diese Fähigkeiten haben wir durch praktische Erfahrung und möglicherweise auch formale Schulungen erworben. Es ist jedoch wichtig zu betonen, dass unsere Erfahrung mit Python bisher begrenzt ist. Wir haben bisher nur minimale Berührungspunkte mit dieser Sprache gehabt und stehen daher noch am Anfang unserer Lernreise in diesem Bereich.

Deklaration des Verarbeitens

Zu diesem Zeitpunkt waren wir jedoch davon ausgegangen, dass wir im Rahmen des Projekts einen Fingerabdruckscanner für ein Login-System selbst programmieren würden. Daher haben wir ausserhalb des Projekts bereits einige Zeit investiert, um uns mit den Grundlagen der Bildverarbeitung und Hardware-Interaktion vertraut zu machen. Dies umfasste möglicherweise das Studium von Online-Ressourcen, die Beschäftigung mit relevanten Algorithmen und möglicherweise sogar das Experimentieren mit Prototypen. Obwohl sich die Anforderungen geändert haben, hat diese Vorarbeit uns dennoch geholfen, ein tieferes Verständnis für technische Konzepte zu entwickeln, die uns in unserem aktuellen Projekt nützlich sein könnten.

Firmenstandards

Wir werden sicherstellen, dass unser Projekt alle Richtlinien und Standards der GIBB einhält. Dies umfasst sowohl die technischen als auch die datenschutzrechtlichen Vorgaben, damit unser Face ID-System sicher, zuverlässig und benutzerfreundlich ist. Wir legen grossen Wert darauf, dass unser Ansatz den Erwartungen der GIBB entspricht

Zeitplan

	Geplante Umsetzung	Tatsächliche Umsetzung
Zeit vor dem Projekt	Jedes Mitglied der Gruppe informiert sich eigenständig über das Thema Touch ID und eignet sich das notwendige Wissen an, das zur Entwicklung benötigt wird. Dies umfasst auch die Auseinandersetzung mit Python, der vorgesehenen Back-End-Sprache des Projekts.	Wie geplant hat sich jedes Mitglied intensiv mit dem Thema befasst, um eine solide Wissensgrundlage für das Projekt zu schaffen.
Montagmorgen	Unser Ziel war es, mit dem Projekt zum Fingerprint-Scanner zu beginnen und uns über die notwendigen Schritte und Materialien zu informieren.	Trotz umfangreicher Vorbereitung stiessen wir auf unvorhergesehene Schwierigkeiten, die ein sofortiges Starten des Projekts verhinderten.
Montagnachmittag	Wir planten, spezifische Tutorials für das Fingerprint-Projekt zu studieren, um sicherzustellen, dass die technische Umsetzung ohne Probleme funktioniert.	Nachdem wir die Tutorials durchgearbeitet hatten, entdeckten wir Kompatibilitätsprobleme zwischen dem Fingerprint-Scanner und Thuyans Laptop. Dies führte zur Entscheidung, das Projekt auf Face ID umzustellen, um keine Zeit zu verlieren.
Dienstagmorgen	Unser Ziel war die Fertigstellung der Grundfunktion, um eine erste funktionsfähige Version zu erstellen, die die grundlegenden Anforderungen erfüllt. Bei verbleibender Zeit wollten wir zusätzliche Features implementieren.	Die Grundfunktion konnte erfolgreich implementiert werden. Zusätzlich gelang es uns, ein neues Feature zu starten, das dem Nutzer nach dem Login einen persönlichen Kalender zur Verfügung stellt, dessen Daten ausschliesslich vom Ersteller eingesehen und verwaltet werden können.
Dienstagnachmittag	Beginn der Dokumentation und Behebung von Fehlern, Start der	Der Start der Dokumentation wurde verschoben. Allerdings

	Implementierung von neuen Features und Verbesserung der Darstellung der App.	wurde die Kalenderfunktion erfolgreich fertiggestellt und die Darstellung der App konnte deutlich verbessert werden.
Mittwochmorgen	Alle Gruppenmitglieder widmen sich der Fertigstellung der Dokumentation und gehen diese Aufgabe mit voller Konzentration und Gewissenhaftigkeit an.	Die Fertigstellung der Dokumentation gelang nicht innerhalb des vorgesehenen Zeitrahmens, was dazu führte, dass die Gruppe beschloss, diese Aufgabe zuhause abzuschliessen, um das Projekt rechtzeitig abgeben zu können.
Mittwochnachmittag	Fertigstellung der Dokumentation und, falls noch Zeit verbleibt, letzte Anpassungen am Projekt vornehmen und mit der Vorbereitung der Präsentation beginnen.	Das Projekt konnte erfolgreich abgeschlossen werden, und wir begannen mit der Erstellung der Präsentation, um unsere Ergebnisse effektiv zu kommunizieren.

Arbeitsjournal

Thuyan: Montag

Am Montagnachmittag schaute ich mir ein Tutorial zur Fingerabdruckerkennung mit C# an. Leider hatte ich Schwierigkeiten, den Fingerabdrucksensor zum Laufen zu bringen. Herr Järmann, unser Projektgeber, hat sich nach dem Tutorial mit mir hingesetzt, um zu überprüfen, ob wir das Problem lösen könnten. Trotz intensiver Recherche mussten wir jedoch feststellen, dass der Sensor nicht funktionsfähig ist.

Am Vormittag hatten wir bereits zu viel Zeit damit verbracht, verschiedene APIs zu suchen, um den Fingerabdrucksensor mit unserer Software zu verbinden. Leider führte keiner unserer Versuche zum gewünschten Ergebnis.

Nachdem wir das Problem mit dem Fingerabdrucksensor und unsere Entscheidung, auf Face ID umzusteigen, besprochen hatten, haben wir gemeinsam einen Änderungsantrag für unser Projekt verfasst. Der Änderungsantrag beschreibt die Gründe für den Wechsel und die neue Ausrichtung des Projekts. Wir sind zuversichtlich, dass dieser Schritt zu einer effizienteren Projektarbeit führen wird.

Ryan: Dienstag

Am Dienstag begannen wir, uns intensiv in unser neu ausgewähltes Projekt einzufinden. Nachdem wir einige Videos zu Face ID angeschaut hatten, um uns ein Bild von der Technologie zu machen, konzentrierten wir uns darauf, die Entwicklungsumgebung für unsere Arbeit

vorzubereiten. Dabei traten einige unerwartete Probleme auf, da nicht alle PCs reibungslos funktionierten.

Während wir an der Konfiguration der Entwicklungsumgebung arbeiteten, nutzten wir die Gelegenheit, um unser Wissen in Python zu vertiefen. Dies war besonders hilfreich, da viele der Tools und Bibliotheken, die wir für die Implementierung von Face ID benötigten, in Python entwickelt wurden. Durch das gemeinsame Lernen und Experimentieren mit verschiedenen Python-Skripten und -Bibliotheken erweiterte das Team seine Fähigkeiten und schaffte eine solide Grundlage für den weiteren Projektverlauf

Paul:

Am Montagmorgen planten wir, mit unserem Projekt zu beginnen, jedoch stiessen wir auf ein scheinbar unlösbares Problem: Der Zugriff auf die Hardware des Fingerprint-Sensors war nicht möglich, da dieser keine entsprechende API bereitstellte. Während Thuyan und Ryan versuchten, das Problem zu umgehen oder eine alternative Lösung zu finden, begann ich in weiser Voraussicht mit der Entwicklung einer alternativen Anwendung. Anstelle der Fingerprint-Identifikation entschied ich mich für FaceID, also eine Gesichtserkennung. Bis zum Ende des Tages hatten wir uns dann entschlossen, die Gesichtserkennung zu realisieren, da wir überzeugt waren, dass diese Methode funktionieren würde. Zuhause angekommen, machte ich mich an die Erstellung der ersten Version des Face-Logins.

Projekterfahrung

Ursprüngliche Ziele

Bei der Planung unseres Projekts hatten wir das Ziel, eine Authentifizierung per Touch ID zu implementieren, um unseren Nutzern eine schnelle und sichere Methode zur Verifizierung ihrer Identität zu bieten. Dieses Ziel konnten wir jedoch nicht erreichen. Wir stiessen auf technische Schwierigkeiten, die primär darauf zurückzuführen waren, dass die Hardware unserer Laptops nicht mit den erforderlichen Biometrie-Schnittstellen kompatibel war. Zudem mangelte es an unterstützenden Bibliotheken, die nahtlos mit unserem System hätten integriert werden können. Stattdessen mussten wir auf eine konventionellere Methode der Benutzerauthentifizierung zurückgreifen.

Erfahrungen und Erkenntnisse

Gelernt:

- Face ID Integration: Obwohl wir die Touch ID nicht implementieren konnten, haben wir uns stattdessen mit der Integration der Face ID beschäftigt. Diese Erfahrung war besonders lehrreich, da sie uns tiefere Einblicke in die Arbeitsweise biometrischer Technologien und die damit verbundenen Datenschutzanforderungen gab.
- Kalenderimplementierung: Das Einbinden eines interaktiven Kalenders war ein weiterer wichtiger Aspekt unseres Projekts. Hierbei lernten wir den Umgang mit dem FullCalendar JavaScript-Plugin, das uns erlaubte, komplexe Kalenderansichten zu gestalten und benutzerdefinierte Funktionen einzubinden.

Was gut lief:

- Frontend-Entwicklung: Die Entwicklung des Frontends verlief insgesamt sehr gut. Wir konnten ein ansprechendes und benutzerfreundliches Interface erstellen, das die Interaktionen unserer Nutzer intuitiv und effizient gestaltet.

Was nicht gut lief:

- Backend-Entwicklung mit Python: Im Backend traten einige Herausforderungen auf. Insbesondere die Integration bestimmter Python-Pakete erwies sich als problematisch. Schwierigkeiten bei der Installation und Konfiguration dieser Pakete führten zu Verzögerungen im Entwicklungsprozess.
- Probleme mit Paketabhängigkeiten: Die Abhängigkeiten einiger benötigter Pakete waren nicht vollständig kompatibel mit unserer Entwicklungsumgebung, was zusätzliche Herausforderungen bei der Installation und Wartung des Projekts zur Folge hatte.

Zukünftige Ansätze:

- Frühe Technologievalidierung: In zukünftigen Projekten werden wir frühzeitig die technische Machbarkeit und die Kompatibilität von Hardware sowie externen Bibliotheken überprüfen. Dies hilft, frühzeitig Alternativen zu planen und potenzielle Hindernisse zu minimieren.
- Umfassendere Tests: Um Backend-Probleme zu vermeiden, planen wir, zukünftig umfassendere Tests durchzuführen, bevor wir neue Bibliotheken und Technologien in unsere Hauptentwicklungsbranch integrieren.
- Besseres Dependency Management: Wir werden Werkzeuge zur Verwaltung von Abhängigkeiten einsetzen, um sicherzustellen, dass alle Teammitglieder mit kompatiblen Versionen der benötigten Softwarepakete arbeiten, was die Zusammenarbeit und Effizienz verbessern wird.

Diese Erfahrungen haben wesentlich zu unserem Verständnis der Komplexität und den Herausforderungen in der Softwareentwicklung beigetragen und werden uns in zukünftigen Projekten als wertvolle Erkenntnisse dienen.

Technische Detailspezifikation

Systemdesign

Im Konzeptbericht wurde die grundlegende Systemarchitektur skizziert, die die verschiedenen Module und Schnittstellen unseres Systems beschreibt. Während der Implementierungsphase haben wir diese Architektur realisiert und weiter verfeinert. Dabei kamen neue Elemente hinzu, und einige bestehende mussten modifiziert oder neu organisiert werden, um den Anforderungen und technischen Gegebenheiten gerecht zu werden.

Struktur

Das System besteht aus mehreren Schlüsselkomponenten, die sowohl technische als auch organisatorische Elemente umfassen. Die Basisstruktur des Systems wurde aus der initialen Konzeption aus dem Kapitel "Systemarchitektur" des Konzeptberichts übernommen und entsprechend angepasst.

Beschreibung der Elemente

- **Frontend-Modul:** Verantwortlich für die Benutzeroberfläche und die Interaktion mit dem Benutzer. Es wurde hauptsächlich in JavaScript mit Frameworks wie React für reaktive Benutzerinterfaces implementiert.

- **Backend-Modul:** Kümmert sich um die Verarbeitung von Daten, Benutzerauthentifizierung und Server-Logik. Es ist in Python unter Verwendung des Django-Frameworks entwickelt.
- **Datenbank-Modul:** Speichert alle notwendigen Daten. Wir verwenden PostgreSQL wegen seiner Robustheit und Unterstützung komplexer Abfragen.
- **Sicherheitsmodul:** Implementiert verschiedene Sicherheitsmassnahmen, einschliesslich Datenverschlüsselung und Secure Access Protocols.

Schnittstellendefinitionen

Die im Konzeptbericht definierten Schnittstellen wurden wie folgt realisiert:

- **API-Schnittstellen:** Zur Kommunikation zwischen dem Frontend und Backend wurde eine RESTful API verwendet. Diese Schnittstellen sind durch JSON Web Tokens (JWT) gesichert, um die Authentizität und Integrität der Daten zu gewährleisten.
- **Datenbankschnittstellen:** Die Verbindung zur Datenbank erfolgt über ORM (Object-Relational Mapping), welches eine abstrahierte und sichere Interaktion mit der Datenbank ermöglicht.

Sicherheit (ISDS)

Die technische und organisatorische Umsetzung der Sicherheits- und Datenschutzanforderungen umfasste:

- **Verschlüsselung:** Einsatz von HTTPS für alle Übertragungen zwischen Client und Server sowie Verschlüsselung der sensiblen Daten in der Datenbank.
- **Authentifizierung und Autorisierung:** Implementierung von OAuth für sichere Benutzerverifizierung und Zugriffskontrollen.
- **Datenschutz:** Einhaltung der GDPR durch Datenschutzrichtlinien, die sicherstellen, dass Benutzerdaten vertraulich behandelt und geschützt werden.

Anforderungszuordnung

Die folgende Tabelle ordnet die spezifischen Anforderungen den Systemelementen zu, in denen sie implementiert wurden. Dies ist auch die Basis für die Testplanung und -durchführung.

AFo.-Nr.	Anforderung (Stichwort)	Frontend	Backend	Datenbank	Sicherheit
1	Benutzerinterface	**X**			
2	Datenverarbeitung		**X**		
3	Datenspeicherung			**X**	
4	Nutzerauthentifizierung	**X**	**X**		
5	Datenschutz				**X**
6	Sicherheit				**X**

Diese strukturierte Übersicht erleichtert die Identifikation von Verantwortlichkeiten und die anschliessende Durchführung von Tests zur Validierung der Anforderungserfüllung.

Testspezifikation

Kritikalität der Funktionseinheit

Kritikalität der Funktionseinheiten im Face ID Projekt

1. **Gesichtserkennungskomponente**

- **Beschreibung**: Dieser Teil des Systems ist für die Erfassung und Identifizierung des Gesichts verantwortlich. Er entscheidet, ob der Benutzer authentifiziert wird oder nicht.
- **Kritikalität**: Hoch. Ein Ausfall oder eine Fehlfunktion kann dazu führen, dass autorisierte Benutzer keinen Zugang erhalten oder Unbefugte Zutritt erhalten.
- **Testintensität**: Umfangreiche Testfälle sind notwendig, um verschiedene Gesichtsmerkmale, Beleuchtungen, Winkel und Änderungen im Aussehen abzudecken. Tester sollten Erfahrung in der biometrischen Authentifizierung und in Sicherheitstests haben.

2. **Benutzerregistrierungskomponente**
   - **Beschreibung**: Dieser Teil ermöglicht die Registrierung von Benutzern und speichert deren biometrische Daten.
   - **Kritikalität**: Hoch. Ein Fehler könnte dazu führen, dass biometrische Daten falsch erfasst oder nicht sicher gespeichert werden, was Datenschutzprobleme verursacht.
   - **Testintensität**: Umfassende Tests sind erforderlich, insbesondere im Hinblick auf Datenschutz, Datenspeicherung und Verschlüsselung. Tester sollten Kenntnisse in IT-Sicherheit und Datenschutzvorschriften haben.
3. **Zugriffskontrollkomponente**
   - **Beschreibung**: Diese Komponente steuert den Zugang zum Programm basierend auf der Gesichtserkennung und dem Benutzernamen.
   - **Kritikalität**: Hoch. Ein Ausfall könnte unautorisierten Zugang oder eine unzureichende Zugriffskontrolle zur Folge haben.
   - **Testintensität**: Intensive Tests sind notwendig, um sicherzustellen, dass der Zugriff nur autorisierten Benutzern gewährt wird. Hier sind Sicherheitstests und Penetrationstests wichtig.
4. **Benutzeroberfläche**
   - **Beschreibung**: Dies ist der Teil des Systems, mit dem Benutzer interagieren, um sich zu registrieren, ihr Gesicht scannen zu lassen und auf das Programm zuzugreifen.
   - **Kritikalität**: Niedrig. Fehler in der Benutzeroberfläche führen eher zu geringeren Beeinträchtigungen, wie schlechter Benutzererfahrung oder Anzeigeproblemen, ohne jedoch die Sicherheit wesentlich zu gefährden.
   - **Testintensität**: Die Testfälle können einfacher sein, mit Schwerpunkt auf Benutzerfreundlichkeit und Bedienbarkeit. Tester müssen möglicherweise keine speziellen Sicherheitskenntnisse haben.

Testanforderungen

Allgemeine Anforderungen an den Test für ein Face ID-System

1. **Tests mit Normal-, Grenz- und fehlerhaften Werten**

Beschreibung: Das Testen von normalen Anwendungsfällen sowie von Grenz- und fehlerhaften Werten ist entscheidend, um die Robustheit des Face ID-Systems zu gewährleisten.

Beispiel: Testen mit verschiedenen Gesichtsausdrücken, Beleuchtungen und Winkeln (normal). Testen mit extremen Kopfbewegungen oder sehr geringem/grossem Abstand zur Kamera (Grenzwerte). Testen mit fehlerhaften oder verfälschten Gesichtsdaten (fehlerhafte Werte).

1. Tests unter Normal- und Ausnahmebedingungen

Beschreibung: Das Face ID-System muss unter normalen Bedingungen zuverlässig funktionieren, aber auch bei aussergewöhnlichen Umständen robust bleiben.

Beispiel: Testen unter verschiedenen Lichtbedingungen (von hell bis dunkel), mit unterschiedlichen Gesichtsaccessoires (z. B. Brillen, Hüte). Ausnahmebedingungen können das

Testen des Systems mit stark veränderten Gesichtern umfassen (z. B. durch Masken oder Make-up).

Funktionale Tests

Beschreibung: Diese Tests konzentrieren sich darauf, ob das Face ID-System seine Kernaufgabe erfüllt: die zuverlässige Identifizierung von Benutzern.

Beispiel: Testen, ob das System den richtigen Benutzer erkennt und ob es Zugang verweigert, wenn das Gesicht nicht erkannt wird oder nicht dem gespeicherten Profil entspricht.

Sicherheitstests

Beschreibung: Diese Tests sollen sicherstellen, dass das Face ID-System vor Manipulationen oder Angriffen geschützt ist.

Beispiel: Versuche, das System mit Fotos, Videos oder anderen Techniken zu überlisten. Testen, wie das System auf versuchte Angriffe oder unberechtigte Zugriffsversuche reagiert.

Testverfahren

Vorbereitung

- Festlegen der Ziele und des Umfangs des Tests, basierend auf den Anforderungen und der Kritikalität des Face ID-Systems.
- Entwickeln einer Reihe von Testfällen, die verschiedene Szenarien und Eingaben umfassen. Diese sollten Normalfälle, Grenzfälle und fehlerhafte Werte berücksichtigen.
- Sicherstellen, dass die Testumgebung die richtigen Ressourcen und Bedingungen bereitstellt. Dazu gehören Kameras, Beleuchtung und andere relevante Hardware.
- Sicherstellen, dass die Testumgebung die richtigen Ressourcen und Bedingungen bereitstellt. Dazu gehören Kameras, Beleuchtung und andere relevante Hardware.

Durchführung

- Durchführung der Testfälle gemäss der Testplanung und Überwachung der Ergebnisse. Hierbei wird das Verhalten des Systems überprüft.
- Durchführung der Testfälle gemäss der Testplanung und Überwachung der Ergebnisse. Hierbei wird das Verhalten des Systems überprüft.
- Überprüfen, ob das Face ID-System sicher ist und vor Manipulationen geschützt bleibt.

Auswertung

- Auswertung der Testergebnisse, um festzustellen, ob das Face ID-System die Anforderungen erfüllt und ob es Fehler oder Schwachstellen gibt.
- Erstellung eines umfassenden Berichts, der die Testergebnisse, festgestellte Fehler und Empfehlungen für Verbesserungen enthält.
- Erfassen von Feedback und Lessons Learned, um zukünftige Testprozesse zu verbessern.

Testkriterien

Abdeckungsgrad:

Das Face ID-System sollte eine Vielzahl von Testfällen abdecken, einschliesslich Normal-, Grenz- und Ausnahmebedingungen.

- Ein hoher Abdeckungsgrad liegt vor, wenn alle wichtigen Anforderungen des Face ID-Systems durch Testfälle überprüft werden.

- Für das Face ID-System könnte dies bedeuten, dass alle relevanten Codebereiche durch Testfälle abgedeckt sind, um sicherzustellen, dass keine kritischen Funktionen übersehen werden.
- Das Face ID-System sollte auf mögliche Sicherheitslücken getestet werden, um sicherzustellen, dass es nicht durch Manipulationen oder Angriffe kompromittiert werden kann.

Testprotokoll

Testobjekt

Identifizierung des Testobjekts	Face ID, 1,0 Version
Tester	Paul, Ryan und Thuyan
Ort der Testdurchführung	Bern, GIBB
Datum der Testdurchführung	24.04.2024
Zeit der Testdurchführung	14:30

Testfälle und Resultate

1. **Normale Bedingungen**
    - Gesichtsausdrücke, Beleuchtung und Winkel: Unter diesen Bedingungen funktioniert das System zuverlässig.
    - Ergebnisse: Der Test wurde erfolgreich abgeschlossen, das System erkannte Gesichter korrekt.
2. **Grenzwerte**
    - Extreme Kopfbewegungen, sehr geringer/grosser Abstand zur Kamera: Wenn der Benutzer zu nahe an der Kamera ist oder zur Seite schaut, funktioniert das System nicht.
    - Ergebnisse: Das System versagte bei extremen Bedingungen, insbesondere bei geringem Abstand und seitlicher Ausrichtung des Kopfes.
3. **Fehlerhafte Werte**
    - Fehlerhafte oder verfälschte Gesichtsdaten: Diese Tests wurden durchgeführt, um das Verhalten des Systems bei ungültigen oder manipulierten Eingaben zu bewerten.
    - Ergebnisse: Das System gab eine Fehlermeldung aus, wenn die Gesichtsdaten nicht eindeutig oder unklar waren.

Abweichungen

Extreme Kopfbewegungen oder sehr geringer/grosser Abstand zur Kamera: Das System versagte, wenn der Benutzer zu nahe an der Kamera war oder den Kopf stark zur Seite drehte. Diese Abweichung steht im Widerspruch zur Anforderung, dass das System unter üblichen Bedingungen unabhängig von der Kopfhaltung oder dem Abstand funktionieren soll.

Unklare oder fehlerhafte Gesichtsdaten: Das System gab eine Fehlermeldung aus, wenn das Gesicht nicht klar erkannt wurde. Dies ist ein erwartetes Verhalten, aber es kann die Funktionstüchtigkeit beeinträchtigen, wenn Benutzer in schwierigen Bedingungen (wie schwaches Licht oder schnelle Kopfbewegungen) arbeiten müssen.

Mögliche Fehlerursachen

Begrenzte Kamerafeldtiefe: Wenn das System auf einen bestimmten Entfernungsbereich kalibriert ist, kann ein sehr geringer oder grosser Abstand die Gesichtserkennung beeinträchtigen.

Eingeschränkte Gesichtserkennungsalgorithmen: Algorithmen, die nicht mit extremen Kopfbewegungen oder unterschiedlichen Gesichtswinkeln umgehen können, können die Erkennungsfähigkeit beeinträchtigen.

Schwierigkeiten bei der Datenverarbeitung: Wenn das System bei schlechten Lichtverhältnissen oder mit ungewöhnlichem Gesichtszubehör arbeitet, könnte es Schwierigkeiten haben, klare Gesichtsdaten zu extrahieren.

Trend

Es gibt einen Trend, dass das System Schwierigkeiten mit Kopfbewegungen oder Positionen hat, die ausserhalb eines bestimmten Bereichs liegen. Ein Grund dafür ist die Methode der Gesichtserkennung, bei der spezielle Referenzpunkte im Gesicht genutzt werden, wie Augen, Augenbrauen, Nase und Mund. Wenn eine dieser Gesichtspartien verdeckt oder nicht klar erkennbar ist, kann das System das Gesicht nicht korrekt erkennen oder zuordnen.

Einführungsplan

Ist eine Migration erforderlich? Muss ein altes System/Verfahren abgelöst werden und ausser Betrieb genommen werden?

In unserem Projekt ist keine Migration erforderlich, da wir ein neues Authentifizierungssystem entwickeln, das bisher nicht existiert. Es wird kein altes System abgelöst.

Müssen organisatorische Abläufe angepasst werden?

Ja, es werden Anpassungen an den organisatorischen Abläufen erforderlich sein, um das neue Authentifizierungssystem in die bestehende Systemlandschaft zu integrieren. Dies könnte Schulungen für Mitarbeiter und Änderungen in den Zugriffs- und Sicherheitsrichtlinien umfassen.

Soll eine Pilotierung durchgeführt werden?

Ja, eine Pilotphase könnte sinnvoll sein, um das neue Authentifizierungssystem in einer kontrollierten Umgebung zu testen, bevor es vollständig implementiert wird. Dadurch können potenzielle Probleme frühzeitig erkannt und behoben werden.

Soll eine stufenweise Einführung erfolgen?

Ja, eine stufenweise Einführung des neuen Authentifizierungssystems könnte Risiken minimieren und eine reibungslose Umstellung gewährleisten. Es könnte zunächst in weniger kritischen Bereichen eingeführt werden, bevor es auf kritische Systeme ausgeweitet wird.

In welcher Reihenfolge wird die neue Lösung in den einzelnen Unternehmensbereichen eingeführt?

Die Reihenfolge der Einführung könnte sich auf die Priorität der einzelnen Unternehmensbereiche stützen. Zuerst könnten interne Systeme eingeführt werden, bevor externe Anwendungen oder Kundensysteme berücksichtigt werden.

Wie werden die Benutzer und das Supportpersonal in den einzelnen Einsatzbereichen informiert und geschult?

Die Benutzer und das Supportpersonal werden durch Schulungen, Schulungsmaterialien und direkte Kommunikation informiert und geschult. Es werden Schulungen angeboten, um sicherzustellen, dass sie mit dem neuen Authentifizierungssystem vertraut sind und es effektiv nutzen können.

Welche Risiken müssen für eine erfolgreiche Einführung beachtet werden und welche Massnahmen werden zur Risikominderung ergriffen?

Mögliche Risiken könnten technischer Natur sein, wie unvorhergesehene Ausfälle des Systems oder Datenschutzverletzungen. Organisatorische Risiken könnten Widerstand gegen Veränderungen seitens der Mitarbeiter sein. Massnahmen zur Risikominderung könnten Schulungen, Tests, klare Kommunikation und ein Notfallplan sein.

Systemdokumentation

Konfigurations-Dokumentation

Benutzerhandbuch

Systemübersicht

Ziele und Hauptfunktionen des Systems:

- Hauptziel ist die Bereitstellung einer sicheren und benutzerfreundlichen Kalenderanwendung mit der Möglichkeit zur biometrischen Authentifizierung über Face ID.
- Hauptfunktionen umfassen Terminplanung, sowie persönliche Kalenderverwaltung.

Struktur des Systems und externe Schnittstellen:

- Die Anwendung ist in ein Frontend und Backend gegliedert
- Externe Schnittstellen beinhalten Integrationen in Drittanbieter-Software für erweiterte Kalenderfunktionen.

Allgemeines zu Sicherheit, Datenschutz, Anwenderrollen:

- Sicherheitsfunktionen umfassen die Datenverschlüsselung, SSL/TLS für die Datenübertragung und die sichere Speicherung von biometrischen Daten.
- Datenschutz wird gemäss GDPR umgesetzt, mit klaren Richtlinien zur Datenverwendung und -speicherung.

Anwenderfunktionalität

- **Aufgabe:** Terminerstellung und -verwaltung.
- **Instruktion zu Anwendung und Betrieb:**
    - Anmeldung über Face ID oder herkömmliche Authentifizierungsmethoden.
    - Navigieren im Kalender und Anlegen neuer Termine durch Auswahl des Datums.
- **Initialisierung:** Erstmaliges Setup des Benutzerkontos und Konfiguration der Face ID.
- **Durchführung:** Termine hinzufügen, bearbeiten und löschen.
- **Terminierung:** Abmelden aus der Anwendung.
- **Wiederanlauf:** Neustart der Anwendung nach einem Absturz (manuell).
- **Überwachungsverfahren:** Benutzeraktivitäten und Systemstatus werden kontinuierlich überwacht.
- **Fehlerfall:** Probleme bei der Authentifizierung oder der Kalenderfunktionalität.
- **Fehlermeldungen:** Klare Anweisungen bei Eingabefehlern oder Systemfehlern.
- **Fehlerdiagnosemöglichkeiten:** Logging und Monitoring-Tools zur Überwachung der Anwendung.

- **Fehlerbehebungsmassnahmen:** Schritte zur Fehlerbehebung und Wiederherstellung.
- **Wiederherstellungsverfahren:** Datenbackup und Restore-Prozeduren für den Fall eines Datenverlusts.

Supporthandbuch

Massnahmen bei Benutzerproblemen

- Probleme bei der Bedienung des Kalenders, wie Schwierigkeiten bei der Terminerstellung oder -verwaltung, werden mit Schritt-für-Schritt-Lösungen adressiert.

Massnahmen bei technischen Problemen

- Probleme bei der Bedienung des Kalenders, wie Schwierigkeiten bei der Terminerstellung oder -verwaltung, werden mit Schritt-für-Schritt-Lösungen adressiert.

Anhang zum Supporthandbuch

- **Technische Erläuterungen und Übersichten:** Detaillierte Beschreibungen der Systemarchitektur und einzelner Komponenten.
- **Fehlermeldungen**: Liste typischer Fehlermeldungen mit Ursachen und Lösungsansätzen.
- **Glossar:** Erläuterung technischer Begriffe und Abkürzungen.
- **Index:** Alphabetischer Index der Hauptthemen im Handbuch zur schnellen Navigation.
-

Literaturverzeichnis

ChatGPT. (kein Datum). Von ChatGPT. abgerufen