INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Masterarbeit

Anforderungsanalyse und Konzeption für ein System zur sicheren computergestützten Abnahme von Prüfungen

Muhibullah Nasari

INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Masterarbeit

Anforderungsanalyse und Konzeption für ein System zur sicheren computergestützten Abnahme von Prüfungen

Muhibullah Nasari

Aufgabensteller:	Prof. Dr. Dieter Kranzlmüller
Betreuer:	Dr. Thomas Schaaf Robert Kuhlig (mITSM GmbH)
Abgabetermin:	22. Januar 2018

Hiermit versichere ich, dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 22. Januar 2018

. . . . . .

(Unterschrift des Kandidaten)

Abstract

Das wachsende Prüfungsaufkommen im Zuge der Bologna Reform führt zu einem erheblichen Mehraufwand für die Organisation, Durchführung und Korrektur von Prüfungen. Hinzu kommt die stetig steigende Zahl von immatrikulierten Studenten an deutschen Hochschulen. Diese Umstände führen dazu, dass sich ein einzelner Hochschullehrer um immer mehr Studenten kümmern müssen und sich so die Betreuungssituation an den Hochschulen verschlechtert. Gleichzeitig haben die Hochschulen Probleme damit ausreichend große Räumlichkeit für die Prüfungsabnahme zu Verfügung zu stellen.

Ein Ansatz, um dieses Problem zu lösen, ist die Verlagerung der Prüfungsabnahme ins Internet. Online Prüfungen können nicht nur Organisations-, Durchführungs- und Korrekturaufwände senken, sondern auch eine skalierbare Teilnehmeranzahl unabhängig vom Ort bedienen. Jedoch birgt sie auch gewisse Risiken. Einer der größten Bedrohung stellen Täuschungen dar. Prüflinge könnten bei der Prüfung schummeln. In dieser Arbeit soll ein modulares System für die sichere Abnahme von Online Prüfung konzipiert und beispielhaft implementiert werden, um das Risiko für Täuschungen zu reduzieren.

Inhaltsverzeichnis

1 Einführung

Diese Arbeit ist im Rahmen einer Kooperation der Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung des Instituts für Informatik der Ludwig-Maximilians-Universität München und des Munich Institute for IT Service Management entstanden.

In diesem Kapitel werden zuerst Motivation und Notwendigkeit für die Erstellung dieser Arbeit aufgezeigt. Danach werden die Ziele der Arbeit festgelegt und der Aufbau der Arbeit beschrieben. Die Grundlagen werden im folgenden Kapitel behandelt.

1.1 Motivation

Das wachsende Prüfungsaufkommen im Zuge der Bologna Reform führt zu einem erheblichen Mehraufwand für die Organisation, Durchführung und Korrektur von Prüfungen. Hinzu kommt die stetig steigende Zahl von immatrikulierten Studenten an deutschen Hochschulen. Vom Wintersemester 2014/15 auf das Wintersemester 2015/16 stieg die Zahl der eingeschriebenen Studenten um 48.300 auf über 2,8 Millionen (vgl. [Bun17]). Diese Umstände führten dazu, dass sich ein einzelner Hochschullehrer um immer mehr Studenten kümmern musste und sich so die Betreuungssituation an den Hochschulen verschlechterte. Laut den Daten des Statistischen Bundesamtes (vgl. [Bun16]) kamen 2015 auf einen Hochschulprofessor 64 Studenten. Vier Jahre zuvor waren es noch 58. Schließt man private und fachlich spezialisierte Hochschulen aus und betrachtet alle anderen, an denen immerhin 90 Prozent der Studenten immatrikuliert sind, liegt das Verhältnis von Professor zu Studenten sogar bei 1 zu 70 (vgl. [Wie16]). Gleichzeitig haben die Hochschulen Probleme damit ausreichend große Räumlichkeit für die Prüfungsabnahme zu Verfügung zu stellen, wie ein Bericht des Bundeslands Nordrhein-Westfalen, das im deutschen Vergleich die meisten Hochschulen besitzt, zeigt (vgl. [MfI16]).

Ein Ansatz, um dieses Problem zu lösen, ist die Verlagerung der Prüfungsabnahme ins Internet. Online Prüfungen können nicht nur Organisations-, Durchführungs- und Korrekturaufwände senken, sondern auch eine skalierbare Teilnehmeranzahl unabhängig vom Ort bedienen. Jedoch birgt sie auch gewisse Risiken. Einer der größten Bedrohung stellen Täuschungen dar. Prüflinge könnten bei der Prüfung schummeln. Diesem Thema haben sich in der Vergangenheit einige Online Proctoring Unternehmen gewidmet und speziell abgesicherte cloud-basierte Prüfungsabnahmesysteme auf den Markt gebracht. Allerdings ist die Nutzung eines solchen Systems mit einigen Nachteilen für die Bildungseinrichtungen verbunden. Pro Prüfung und Prüfling muss eine Gebühr an das Unternehmen gezahlt werden, wodurch nicht nur die Teilnehmerzahl, sondern auch die Kosten skalieren. Des Weiteren muss sich die Bildungseinrichtung auf das maximale Sicherheitsniveau des Procotoring Systems beschränken. Besondere Anforderungen an die Sicherheit werden nur nach vorheriger Beauftragung implementiert, was wiederum Kosten und Wartezeit mit sich bringt. Außerdem

muss die Bildungseinrichtung u.U. die eigenen sowie die Daten der Teilnehmer ausländischen Datenschutzgesetzen unterwerfen, da sich die größten Online Proctoring Unternehmen im Ausland befinden. PearsonVue (vgl. [Pea17]), Software Secure (vgl. [Sec17]), und ProctorU (vgl. [Pro17]) haben ihren Standort in den USA und Questionmark (vgl. [Que17]) in Großbritannien. Ein ähnliches Problem besteht bei Online Kursen, die von deutschen Universitäten in Zusammenarbeit mit ausländischen Organisationen angeboten werden. Hier wird von Seiten deutscher Datenschützer bemängelt, dass gesammelte Studentendaten nicht ausreichend geschützt und von den ausländischen Partnern an Dritte weitergegeben werden (vgl. [Tag15]). Ein weiteres Problem kann es aufgrund von fehlender Schnittstellenkompatibilität bei der Integration der neuen Komponenten mit bestehenden Systemen, wie z.B. Learning Management Plattformen, die von vielen Bildungseinrichtungen eingesetzt werden (vgl. [OG16]). geben. Aus den genannten Gründen hat es sich diese Masterarbeit zum Ziel genommen eine alternative Lösung für die Absicherung von Online Prüfungen anzubieten.

1.2 Zielsetzung

Das Ziel dieser Arbeit ist es ein Konzept für ein sicheres System für die Abnahme von Online Prüfungen (im Folgenden SSAOP) zu erstellen. Der Begriff „sicher“ bezieht sich auf die Reduzierung von Täuschung bezieht und nicht auf die Systemsicherheit. Mit Hilfe des Konzepts soll eine Organisation in der Lage sein ein SSAOP nach ihrem Schutzbedarf zu implementieren. Daher werden organisatorische und technische Maßnahmen erarbeitet, um die Anforderungen an die Sicherheit zu erfüllen. Die einzelnen technischen Komponenten des SSAOP soll die Organisation selbst auswählen können. Grundlage für die Anforderungen sind die Aspekte der Informationssicherheit, Prüfungsordnungen von Universitäten, typische Anwendungsfälle und Täuschungsszenarien. Die Umsetzungsfähigkeit des Konzepts soll mit Hilfe einer beispielhafte Implementierung demonstriert werden.

1.3 Related Work

Cluskey, Ehlen und Raiborn haben in ihrer Arbeit acht Maßnahmen erarbeitet, um die Möglichkeiten der Täuschung bei Online Prüfungen zu reduzieren. Allein durch die Begrenzung der Prüfungszeit, des Zugriffs auf die Prüfung und durch die Veränderung des Tests sollen Studenten am Täuschen gehindert bzw. dabei beeinträchtigt werden. (vgl. [CJER11]). Die Autoren formulieren keine Maßnahmen zur Authentifizierung und Überwachung des Prüflings während der Prüfung.

Sarrayrih und Ilyas befassen sich in ihrer Arbeit mit den Herausforderungen von Online Prüfungen von Universitäten. Sie beschreiben einen Prozess, der die Sicherheit von Online Prüfungen steigern soll. Dabei gehen sie insbesondere auf die Authentifizierung des Prüflings am Anfang einer Prüfung mittels biometrischen Daten ein, um dadurch den Abgleich des Ausweisfotos mit dem Gesicht des Prüflings bei traditionellen Prüfungen zu simulieren (vgl. [SI13]). Jedoch fehlt in ihrem Prozess die kontinuierliche Authentifizierung während der gesamten Prüfung, wodurch es möglich wäre, den Prüfling nach der erfolgreichen initialen Authentifizierung für den Rest der Klausur durch eine andere Person zu ersetzen und so bei der Prüfung zu täuschen.

Karim und Shukur gehen einen Schritt weiter und untersuchen in ihrem Werk Möglichkeiten, um die Authentizität der Prüflinge kontinuierliche zu überprüfen. Dazu analysieren sie 54 Arbeiten zu diesem Thema und kommen zu dem Ergebnis, dass die biometrische Authentifizierung im Gegensatz zur Authentifizierung durch Wissen oder Besitz, die zuverlässigste und beliebteste Methode ist (vgl. [KS15]).

Kombiniert man mindestens zwei biometrische Authentifizierungsmethoden, so kann man die Zugverlässlichkeit bei der kontinuierlichen Authentifizierung weiter erhöhen, wie eine Studie von Aguila, Rua und Castro zeigt (vgl. [ARC09]). In ihrer Studie haben sie Studenten mit der Methode der Gesichtserkennung überwacht. Ziel war es, herauszufinden, ob es nötig ist eine weitere biometrische Methode hinzuzunehmen für den Fall, dass alleine die Gesichtserkennung für die Authentifizierung nicht ausreichend ist. Sie kommen zu dem Ergebnis, dass das System bei 3 von 16 Studenten eine weitere Überprüfung, bswp. durch Stimmerkennung oder Fingerabdruck, angefordert hat. Wurde die zusätzliche Überprüfung durchgeführt, so konnten alle Studenten authentifiziert werden.

1.4 Annahmen in dieser Arbeit

Für Online Prüfungen gibt es viele Anwendungsbereiche. So kann man sie im klassischen Bildungswesen, wie in Schulen und Universitäten einsetzen. Aber auch Erwachsenenbildung, wie Schulungen und Weiter- bzw. Fortbildungen können mit einer Onlineprüfung abschließen. In dieser Arbeit wird die Online Prüfung an einer Hochschule als Beispiel herangezogen.

Die Arbeit konzentriert sich des Weiteren auf die Abwehr vor Täuschungen bei Prüfungen. Die technische Sicherheit der IT-Systeme wird nicht betrachtet. Es wird angenommen, dass sie ausreichend gegen Angriffe von Hackern geschützt und durch Penetrationstests gehärtet sind.

Eine Online Prüfung besteht aus vielen Unterprozesse, wie bspw. Planung, Erstellung, Durchführung und Korrektur der Prüfung. Die für die Arbeit nicht relevanten Unterprozesse werden nicht bzw. nur rudimentär in dieser Arbeit behandelt. Falls nicht anders beschrieben, wird davon ausgegangen, dass diese Unterprozesse bereits implementiert sind. Der Fokus liegt hier vor allem bei dem Prozess der Prüfungsabnahme (s. 1.1).

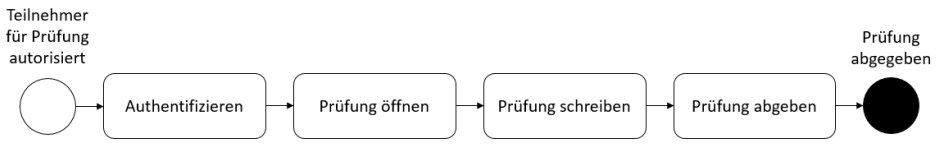


Abbildung 1.1: Prozess der Prüfungsabnahme aus Sicht des Prüfungsteilnehmers

1.5 Aufbau der Arbeit

Im Folgenden wird der Aufbau der Masterarbeit kapitelweise erläutert. Das Werk gliedert sich, ausgenommen von diesem Kapitel, in sieben weitere Kapitel.

Im nächsten Kapitel werden die Grundlagen für diese Arbeit dargelegt. Begriffe wie „Online Prüfung“, „Learning Management System“ und „Authentifizierung“ werden definiert.

Im dritten Kapitel werden Täuschungsszenarien analysiert, Anti-Täuschungsmaßnahmen definiert und daraus organisatorische und technische Anforderungen an ein sicheres Prüfungsabnahmesysteme abgeleitet. Des Weiteren werden Anwendungsfälle bei einer Online Prüfung zusammengetragen und Prüfungsordnungen von Universität nach Anforderungen untersucht.

Die Anforderungsanalyse wird in Kapitel vier mit Hilfe einer Expertenumfrage mit 17 Teilnehmern evaluiert.

Die Anforderungen aus dem dritten Kapitel dienen im fünften Kapitel als Grundlage für die Konzeption des sicheren Prüfungsabnahmesystems und dessen Komponenten. Neben der Architektur des Systems wird das Framework für die Implementierung von Modulen zur Überwachung der kontinuierlichen Authentifizierung entworfen. Zusätzlich werden beispielhaft zwei Module zur Gesichtserkennung und zum Tippverhalten konzipiert.

Im sechsten Kapitel geht es um die Implementierungen des Konzepts. Dabei wird die Umsetzung des Frameworks und der Authentifzierungsmodule dargestellt.

In Kapitel sieben wird die Implementierung mit Hilfe eines Probandentest evaluiert, um die Funktionsfähigkeit des Systems zu überprüfen.

Im letzten Kapitel werden die Erkenntnisse der Arbeit zusammengefasst und mögliche Folgearbeiten skizziert.

2 Grundlagen

In diesem Kapitel werden die Grundlagen für diese Arbeit dargestellt. Dazu wird als erstes geklärt, was eine Online Prüfung ist und wie sie sich von der Präsenzprüfung und der E-Klausur abgrenzt. Danach werden die Aspekte der Informationssicherheit und die biometrische Authentifizierung erklärt. Zum Schluss wird ein Einblick in das Thema „Learning Management System“ gegeben.

2.1 Online Prüfung

Im Gegensatz zur papierbasierten Prüfung setzen die Studenten bei einer computergestützten Prüfung Computer, Tastatur und Maus statt Papier und Stift als Arbeitsmittel ein. Elektronische Prüfungen können entweder als E-Klausur in den Räumen der Bildungseinrichtung oder als Online Prüfung von einem entfernten Ort abgelegt werden. Über zwei Drittel der Hochschulen in Deutschland setzen bereits E-Klausuren ein bzw. prüfen deren Einsatz (vgl. [IUB16]). Aber auch die Nachfrage nach Online Prüfungen steigt stetig. Eine Studie der Internationalen Hochschule Bad Honnef aus dem Jahr 2016 zeigt, dass sich über 70% der befragten Studenten den Einsatz von Online Prüfungen wünschen (vgl. [Wan16]).

Ein Vorteil von Online Prüfungen gegenüber E-Klausuren und papierbasierten Prüfungen ist, dass sie die Anwesenheit des Prüflings an einem bestimmten Ort nicht voraussetzen. So kann der Student selber entscheiden, von wo er die Prüfung ablegen will. Das erleichtert vor allem Menschen mit eingeschränkter Mobilität oder Personen mit langer Anreise die Teilnahme an der Prüfung. Außerdem können Prüfungen, aufgrund der elektronischen Verarbeitung, automatisiert korrigiert werden. Der Einsatz von Computern erlaubt auch neue Fragetypen, wie z.B. Zuordnungen per Drag & Drop. Das bietet neue Möglichkeiten bei der Wissensabfrage.

Es gibt jedoch auch Nachteile bei der Einführung von elektronischen Prüfungen. Es können hohe Erstinvestitionskosten entstehen. Die Universität Mainz hat für die Einführung der E-Klausur im Jahr 2008 insgesamt sechs Server und 230 PCs angeschafft. Die Kosten hierfür beliefen sich auf 200.000 Euro. Für die Betreuung des Systems sind zwei wissenschaftliche Mitarbeit in Teilzeit und zwei studentische Hilfskräfte angestellt worden. Andererseits hat die Online Prüfung gegenüber der E-Klausur den Vorteil, dass die Prüflinge ihre eigene Hardware einsetzen können, wodurch eine große Kostenkomponente entfällt. Ein andere Nachteil ist die Störungsanfälligkeit von IT-Systemen. Daher muss ein Entstörungs-, Problem-, Verfügbarkeits- und Ressourcenmanagement sowie eine Qualitätssicherung etabliert werden, um einen möglichst reibungslosen Ablauf der Prüfung zu gewährleisten. Aber auch der Verlust der Kontrolle über den Prüfling und die dadurch entstehende Gefahr der Täuschung ist ein Nachteil, der in Kapitel 3.10 thematisiert wird.

2.2 Informationssicherheit

Die Informationssicherheit befasst sich mit der Gewährleistung und den Erhalt der Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, die als Voraussetzung für sichere Systeme gelten (vgl. [Eck12]). Zusätzlich werden weitere Attribute wie Authentizität, Zurechenbarkeit, Verbindlichkeit und Zuverlässigkeit betrachtet. Im Folgenden werden die Aspekte der Informationssicherheit erläutert (vgl. [mIT16]).

Vertraulichkeit bedeutet, dass Informationen nur für Berechtigte einsehbar sind. Unberechtigte Dritte dürfen dagegen keinen Zugriff auf die Informationen haben. So können nur der Sender und Empfänger einer Nachricht die enthaltenen Informationen lesen.

Integrität von Informationen bezieht sich auf den Schutz der Informationen vor unbefugter Manipulation. Dazu gehören unberechtigte Löschung, Veränderung und Erweiterung von Informationen.

Verfügbarkeit von Informationen bezieht sich darauf, dass autorisierte Parteien zu vereinbarten Zeiten auf Informationen zugreifen können.

Authentizität ist die Echtheit von Informationen oder Identitäten. Durch Authentisierung und Authentifizierung wird diese Echtheit nachgewiesen und überprüft.

Zurechenbarkeit bedeutet die Übernahme von Verantwortung, Rechenschaft und/oder Haftung für Handlungen oder Entscheidungen.

Verbindlichkeit ist zugleich Nicht-Abstreitbarkeit und bedeutet die Nachweisbarkeit von Ursprung und Auslieferungsziel einer Information.

Zuverlässigkeit wird durch die Sicherstellung eines konsistenten Verhaltens und Lieferung vorgesehener intendierter Ergebnisse erreicht.

2.3 Biometrische Authentifizierung

Biometrische Authentifizierung scheint heutzutage omnipräsent zu sein. Moderne Smartphone und Laptops nutzen biometrische Authentifizierungsmethoden, um den Nutzer das Entsperren des Geräts zu erleichtern. Hierbei werden bspw. Fingerabdruck-Leser, Gesichtserkennung oder Iris-Scanner genutzt, die biometrische Merkmale des Bedieners erkennen und diese nutzen, um dessen Authentizität zu überprüfen. Damit das Gerät einen Abgleich machen kann, muss der berechtigte Nutzer seine biometrischen Daten, ein sogenanntes Referenzmodell seines Gesichts, auf dem Gerät hinterlegen.

2.4 Learning Management System

Ein Learning Management System (kurz: LMS) ist eine Applikation, die das Verwalten von Kursen und Kursmaterialien ermöglicht. Man kann damit Studenten für Kurse anmelden und ihnen Material wie Skripte, Software und Umfragen zu Verfügung stellen. Der Funkti-

onsumfang der meisten LMS lässt sich durch Plugins erweitern. Zwei der bekanntesten LMS sind Moodle und ILIAS. Sie werden von den meisten deutschen Universitäten eingesetzt (vgl. [OG16]). Einige der LMS stellen auch umfangreiche Funktionen für die Abnahme von Online Prüfungen zu Verfügung, jedoch ohne der Überwachung des Prüflings. Diese Art von Systemen eigenen sich, um sie als Grundsystem für das SSAOP einzusetzen, da ein paar der essentiellen Anforderungen an das SSAOP von den meisten LMSs auf dem Markt bereits umgesetzt werden.

3 Anforderungsanalyse

In diesem Kapitel werden die Anforderungen an das SSAOP analysiert. Die Anforderungsanalyse ist ein systematischer Ansatz zur Spezifikation von Anforderungen. Hierbei sind die Ziele, die relevanten Anforderungen zu identifizieren sowie dokumentieren und die Wünsche und Bedürfnisse der Stakeholder zu verstehen, um das Risiko zu minimieren, dass das System nicht den Wünschen und Bedürfnissen der Interessensgruppen entspricht. Mit Hilfe von Artefakten, Rollen und Anwendungsfällen sollen Anforderungen, die für die Konzeption des Systems notwendig sind, abgeleitet werden. Da der Fokus dieser Arbeit auf die Konzeption eines Frameworks gegen Täuschungsversuche liegt, werden die grundsätzlichen Anforderungen an ein Prüfungsabnahmesystem, wie das Anmelden oder Teilnehmen an einer Prüfung, lediglich in einem rudimentären Umfang erläutert. Danach werden die Anforderungen an die Informationssicherheit erfasst. Im Anschluss dazu werden anhand von Täuschungsszenarien Bedrohungen aufgezeigt und anschließend Maßnahmen formuliert, die diesen entgegenwirken. Dadurch ergeben sich Anforderungen an das SSAOP, die kategorisiert und nummeriert erfasst werden. Schließlich werden die Prüfungsordnungen der Universitäten analysiert.

3.1 Stakeholder

Die Hauptstakeholder des SSAOPs sind alle Organisationen, die Prüfungen durchführen und diese in Zukunft sicher über das Internet anbieten wollen sowie Studenten, Schulungsteilnehmer und weitere Person, die eine Prüfung online ablegen werden. Daneben gibt es noch weitere Stakeholder wie die Prüfungskommission, Gesetzgeber, die operative IT und die Forschung, die nicht direkt das SSAOP nutzen, jedoch Einfluss auf das System haben bzw. von den Auswirkungen des Systems betroffen sind. In den folgenden Abschnitten, sollen die Anforderungen der Stakeholder nach nach dem Requirements Engineering Framework IREB (vgl. [ire17]) identifiziert und analysiert werden.

3.2 Systemkontext

Der Systemkontext ist der Teil der Umgebung eines Systems, der für die Definition und das Verständnis der Anforderungen des betrachteten Systems relevant ist.

Typen von Aspekten im Systemkontext:

- Personen (Stakeholder und/oder Stakeholdergruppen)
- Systeme im Betrieb (andere technische Systeme oder Hardware)
- Prozesse (technisch oder physikalisch, Geschäftsprozess)
- Ereignisse (technisch oder physikalisch)

- Dokumente (z.B. Gesetze, Richtlinien)

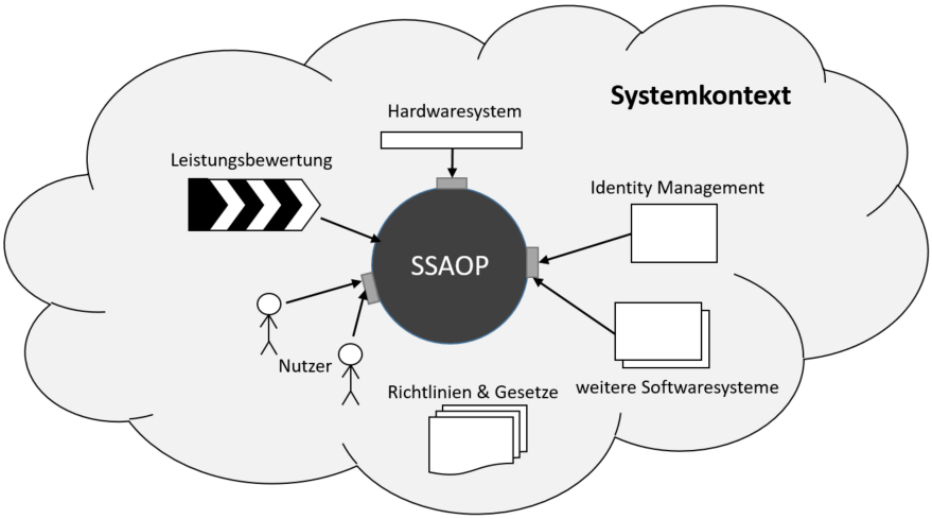


Abbildung 3.1: Der grobe Systemkontext des SSAOP

Abbildung 3.1 visualisiert das System, die Systemgrenze, sowie Aspekte und ihre Schnittstellen. Hier kann man erkennen, welche Aspekte bei der Anforderungsanalyse berücksichtigt werden müssen. Diese Aspekte gelten für den Zeitpunkt, zu dem diese Arbeit veröffentlicht wurde. Künftige neue Aspekte müssen ggf. bei der Umsetzung des SSAOPs berücksichtigt werden. Im Folgenden wird dies weiter erläutert.

3.3 Systemgrenze

Die Systemgrenze separiert das geplante System von seiner Umgebung. Sie grenzt den im Rahmen des Entwicklungsprozesses gestaltbaren und veränderbaren Teil der Realität von Aspekten in der Umgebung ab, die durch den Entwicklungsprozess nicht verändert werden können. Alles innerhalb der Systemgrenze ist gestaltbar und alles darüber hinaus nicht. Dies bedeutet, dass es Gegebenheiten gibt, die die Konzeption und Implementierung des SSAOPs einschränken. Dazu gehören die Prüfungsordnung, bestehende Prozesse, bspw.. für die Leistungsbewertung, die Kompetenzen der Nutzer des SSAOP und bereits bestehende Software- sowie Hardwaresysteme.

Schnittstellen, die über die die Aspekte mit dem SSAOP kommunizieren, müssen identifiziert werden. Dies geschieht durch Betrachtung von Quellen, die Eingaben für das System liefern und Senken, die Ausgaben vom System erwarten.

Quellen und Senken für das SSAOP:

- ein existierendes Identity Management System
- SSAOP Nutzer, wie bspw. Prüflinge oder Prüfungsersteller
- die genutzte Infrastruktur

Die Grauzone der Systemabgrenzung enthält alle Aspekte, von denen zu einem bestimmten Zeitpunkt nicht klar ist, ob sie vom zu entwickelnden System implementiert bzw. unterstützt werden sollen oder nicht. Sie wird erst bei der tatsächlichen Implementierung des SSAOP in die Zielumgebung bekannt.

Die Kontextgrenze separiert den relevanten Teil der Umgebung eines geplanten Systems vom irrelevanten Teil, d.h. den Teil der Umgebung, der keinen Einfluss auf das geplante System und damit auch keinen Einfluss auf die Anforderungen dieses Systems hat. Die Grauzone der Kontextabgrenzung enthält alle Aspekte, von denen zu einem bestimmten Zeitpunkt unklar ist, ob diese das geplante System beeinflussen oder nicht. Eine vollständige und präzise Kontextabgrenzung ist für das SSAOP praktisch nicht möglich. Die irrelevante Umgebung beinhaltet die „Restwelt“ außerhalb von System und Systemkontext und ist somit nicht endlich. So können neue Gesetze, die heute nicht bekannt sind, die Konzeption bzw. Implementierung des Systems einschränken. Daher muss vor der Implementierung des SSAOPs die Kontextgrenze erneut überprüft werden, um herauszufinden, ob neue Einflüsse zu beachten sind. Daraus folgt, dass es nicht möglich und auch nicht notwendig, die aktuelle Grauzone der Kontextabgrenzung vollständig aufzulösen.

3.4 Anforderungskategorien

Für die Anforderungsanalyse werden drei Anforderungskategorien definiert. Im Folgenden werden sie jeweils erklärt.

3.4.1 Funktionale Anforderungen

Eine funktionale Anforderung ist eine Anforderung bezüglich des Ergebnisses eines Verhaltens, das von einer Funktion des Systems bereitgestellt werden soll. Funktionale Anforderungen legen die Funktionalität des Systems fest.

3.4.2 Qualitätsanforderungen

Eine Qualitätsanforderung ist eine Anforderung, die sich auf ein Qualitätsmerkmal bezieht, das nicht durch funktionale Anforderungen abgedeckt wird. Qualitätsanforderungen definieren die Qualität des Systems und beeinflussen häufig stärker als funktionale Anforderungen die Systemarchitektur. Sie werden oft auch als „nicht-funktionale Anforderungen“ klassifiziert. „Nicht-funktionale Anforderungen“ können auch Randbedingungen sein.

Kategorien von Qualitätsanforderungen:

- Performanz des Systems
- Sicherheitsaspekte
- Zuverlässigkeit der Funktionalität, insbes. in Bezug auf Robustheit, Fehlertoleranz und Wiederherstellbarkeit

- Benutzbarkeit des Systems, insbes. hinsichtlich Verständlichkeit, Erlernbarkeit und Bedienbarkeit
- Änderbarkeit des Systems, insbes. in Bezug auf Analysierbarkeit, Modifizierbarkeit, Stabilität und Prüfbarkeit
- Übertragbarkeit des Systems, insbes. hinsichtlich Anpassbarkeit, Installierbarkeit und Austauschbarkeit

3.4.3 Randbedingungen

Eine Randbedingung ist eine Anforderung, die den Lösungsraum jenseits dessen einschränkt, was notwendig ist, um die funktionalen Anforderungen und die Qualitätsanforderungen zu erfüllen. Randbedingungen können inhaltlicher oder prozessualer Art sein und werden nicht umgesetzt, sondern schränken die Umsetzungsmöglichkeiten des Systems ein und sind nicht beeinflussbar.

3.5 Artefakte

Vor der Anforderungsanalyse wird definiert, welche Artefakte vom SSAOP bzw. SSAOP Nutzer erstellt und/oder genutzt werden. Artefakte sind Produkte, die Eingaben bzw. Ausgaben von Anwendungsfällen darstellen. Im Folgenden werden die Artefakte Prüfung, Prüfungsfrage, Musterlösung, Bewertungsergebnis, Prüfungstermin, Fragenkatalog und Überwachungsdaten erläutert.

3.5.1 Prüfung

Eine Prüfung soll die Kenntnisse und Leistung einer Person feststellen. Sie ist ein Leistungsnachweis und besteht aus einer oder mehreren Fragen, die sich auf die im Kurs vermittelten Lerninhalte beziehen. Eine Prüfung unterliegt einem Lebenszyklus (s. Abbildung 3.2). So wird eine Prüfung in der Regel erstellt, getestet bevor sie freigegeben und bei Bedarf überarbeitet wird. Nach der Einsatzphase wird die Prüfung eingezogen.

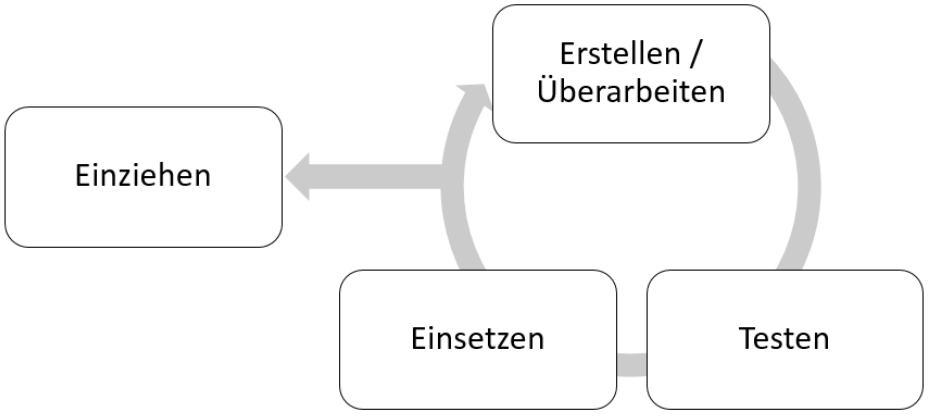


Abbildung 3.2: Lebenszyklus einer Prüfung

3.5.2 Prüfungsfrage

Prüfungsfragen sind Teil einer oder mehrerer Prüfungen. Es gibt unterschiedliche Arten von Fragestellungen. In dieser Arbeit wird unterschieden zwischen offenen Fragen, bei denen der Prüfling in Form von Freitext antworten kann und geschlossenen Fragen (auch Multiple-Choice Fragen genannt), bei denen dem Prüfling eine eingeschränkte Auswahl an Antworten vorgegeben wird und er hieraus die richtige Antwort bzw. Antworten auswählen muss.

3.5.3 Musterlösung

Die Musterlösung bezieht sich auf eine Prüfungsfrage und stellt die richtige Beantwortung dieser dar. Bei offenen Fragen besteht die Musterlösung aus Schlüsselworten, die im Text des Prüflings enthalten sein müssen, damit dieser die jeweiligen Punkte erlangt. Bei Multiple Choice Fragen enthält die Musterlösung die richtigen Antwortmöglichkeiten. Weitere Fragetypen sind möglich, werden aber in dieser Arbeit nicht betrachtet.

3.5.4 Bewertungsergebnis

Das Bewertungsergebnis ist das Resultat der Beurteilung einer Prüfungsfrage. Es ergibt sich durch den Abgleich der Musterlösung mit der vom Prüfling abgegebenen Lösung. Das Ergebnis wird in Punkten dargestellt.

3.5.5 Prüfungstermin

Der Prüfungstermin ist die Uhrzeit und das Datum an dem eine konkrete Prüfung stattfindet. Prüflinge (s. Kap. 3.7.13) können sich zu einem Prüfungstermin anmelden. Auch der Prüfungsort kann ggf. zu einem Termin gehören. Einem Prüfungstermin muss auch ein Prüfungsbewerter (s. Kap. 3.7.15) zugeteilt werden, der die Prüfung korrigieren muss.

3.5.6 Fragenkatalog

Ein Fragenkatalog ist eine Datenbank, die die Prüfungsfragen zu einem bestimmten Themenbereich zentral bereitstellt, unabhängig davon, ob sie Teil einer Prüfung sind oder nicht. Wenn Fragen formuliert werden landen sie als erstes im Fragenkatalog und werden dann einzelnen Prüfungen zugeordnet. Dadurch ist es möglich eine Frage mehreren Prüfungen zuzuordnen. Außerdem wird die Verwaltbarkeit der Fragen vereinfacht, da Änderung, wie z.B. die Verbesserung eines Rechtschreibfehlers, zentral im Fragenkatalog durchgeführt werden können und nicht in jeder einzelnen Prüfung, die diese Frage beinhaltet.

3.5.7 Überwachungsdaten

Die Überwachungsdaten werden vom SSAOP generiert, um Täuschungsversuche erkennen zu können. Zu den Überwachungsdaten können Webcam Bilder, Ergebnisse zum kontinuierlichen Gesichtsabgleich, Ergebnisse zum Tippverhalten und weitere Authentifizierungsdaten gehören.

3.6 Rollen

An der Erstellung, Organisation, Durchführung und Korrektur der Prüfung sind unterschiedliche Rollen beteiligt. So gibt es beispielsweise einen Prüfungsersteller, der eine Prüfung erstellt, die dann von einem Prüfungsplaner terminiert wird, damit Prüflinge die Prüfung zu einem gegebenen Datum ablegen können. Oder die Prüfungsaufsicht, die Prüflinge überwacht, um zu erkennen, ob sie bei der Prüfung getäuscht haben. Im Folgenden werden die Anwendungsfälle der einzelnen Rollen beschrieben und davon Anforderungen abgeleitet. Der Umfang dieses Kapitels beschränkt sich auf die wesentlichen Rollen und Anwendungsfälle. Die Beschreibung der Anwendungsfälle erfolgt in einem für die Konzeption erforderlichen Umfang und Detailtiefe.

Jeder Nutzer kann mehrere Rollen innerhalb des Systems annehmen. Manche Aktivitäten, wie z.B. das Abrufen des Ergebnisses, können von mehr als einem Nutzer getätigt werden. Für das SSAOP wurden 17 mögliche Rollen identifiziert und wie folgt gruppiert:

Rollen, die sich auf System, Nutzer und Gruppen beziehen:

1. Der System Administrator installiert und wartet das System und fügt Nutzermanager dem System hinzu.
2. Der Nutzermanager fügt dem System Nutzer hinzu und weist ihnen Rollen zu.
3. Der Gruppenmanager teilt Nutzer Gruppen zu.

Rollen, die sich auf Fragen beziehen:

4. Der Fragenersteller kreiert neue Fragen und Fragenkataloge.
5. Der Fragenbetrachter hat die Möglichkeiten Fragen anzuschauen.
6. Der Fragenvalidierer prüft die Qualität der erstellten Fragen, bevor sie in die Prüfungen übernommen werden.

Rollen, die sich auf Prüfungen beziehen:

7. Der Prüfungsersteller kombiniert Fragen zu einer Prüfung und bestimmt das Bewertungsschema sowie die Dauer der Prüfung.
8. Der Prüfungsbetrachter hat die Möglichkeit eine Prüfung anzuschauen.
9. Der Prüfungsvalidierer prüft die Qualität der Prüfung, bevor sie den Prüflingen vorgelegt werden.

Rollen, die sich auf Prüfungssitzungen beziehen:

10. Der Prüfungsplaner lädt eine Gruppe von Prüflingen zu einer Prüfung ein und bestimmt wann sie stattfindet.
11. Die Prüfungsaufsicht überwacht die Prüfung und meldet Täuschungsversuche.
12. Der Prüfling nutzt das System, um an Prüfungen teilzunehmen und die Prüfungsergebnisse anzuzeigen.

Rollen, die sich auf Antworten und Ergebnisse beziehen:

13. Der Antwortüberwacher kontrolliert die von den Prüflingen abgegebene Antworten. Dieser Rolle kann dem Fragenersteller zugeteilt werden, falls er sehen will, wie seine Fragen beantwortet werden.

14. Der Prüfungsbewerter bewertet Freitext- oder andersartige Antworten, die nicht vom System maschinell bewertet werden können.

15. Der Bewertungsüberwacher kontrolliert die Endergebnisse von Prüflingen und die Überwachungsdaten. Diese Rolle kann z.B. dem Zweitkorrektor zugeteilt werden.

16. Der Notenkorrektor kann Ergebnisse verändern, falls z.B. falsch bewertet wurde oder ein Prüfling getäuscht hat.

17. Der Forscher nutzt die Statistiken des Systems, um Trends zu erkennen bspw. bei häufigen Fehlmessungen.

In einer Universität können beispielsweise folgende Rollen realen Personen zugeteilt werden:

- Ein Mitglied des Prüfungsamts könnte Gruppenmanager, Prüfungsplaner und Bewertungsüberwacher sein.

- Der Tutor, die Person, die oft Prüflinge in Übungen auf Prüfungen vorbereitet, könnte Prüfungsbetrachter, Antwortüberwacher und Prüfungsbewerter sein.

3.7 Anforderungen aus Anwendungsfällen

Zuerst werden die grundsätzlichen Anforderungen für alle SSAOP Nutzer definiert. Danach werden die speziellen Anforderungen der 17 Rollen identifiziert, indem deren typischen Anwendungsfällen analysiert werden.

3.7.1 SSAOP Nutzer

Eine grundsätzliche Voraussetzung für alle Nutzer des SSAOPs ist es, dass es eine intuitive Bedienung anbietet und keine bzw. eine kurze Schulung erfordert. Der Nutzer muss keine Programmiersprache beherrschen sowie kein spezielles IT-Wissen aufweisen. Das SSAOP unterstützt außerdem aktuelle Windows und MacOS Betriebssysteme. Es bietet auch die Möglichkeit das Look and Feel der Prüfungsorganisation zu übernehmen, um es an die restlichen Benutzeroberflächen anzupassen. Die Nutzerverwaltung kann an ein vorhandenes Identity Management System angebunden werden, sodass Nutzer bereits vorhandene Zugänge verwenden können.

Sicherheit und Belastbarkeit sind auch essentiell für alle Nutzer des SSAOPs und für die Erhaltung des Rufs der Prüfungsorganisation. Alle Prüfungen und Daten sind nur für Nutzer zugänglich, denen die entsprechenden Rechte von Nutzermanager zugewiesen wurden. Die Nutzer sollten darauf vertrauen können, dass alle Daten verschlüsselt über das Netzwerk kommuniziert werden. Sie sollte sich auch sicher, dass auf dem Server gelagerte Daten nicht von unautorisierten Dritten gelesen, verändert oder gelöscht werden können.

Außerdem ist das System robust und ausreichend vor Abstürzen sowohl auf Server- als auch auf Client-Seite geschützt. Komplizierte und zeitaufwändige Anmeldeprozeduren können ebenfalls die Akzeptanz bei den Nutzern senken. Die Erstellung von Prüfungsfragen und Prüfungen kann auch teilweise erfolgen und muss nicht in einem Guss abgeschlossen werden.

Nutzer aller Art können bei Bedarf Inhalte einbinden, so wie das auf üblichen Webseiten möglich ist. Beispiele für solche Inhalte sind Chart oder Bilder.

Alle Nutzeraktionen werden protokolliert, so dass es möglich ist bspw. die IP Adresse eines Prüflings anzuschauen oder die Vergabe einer Bewertung durch einen Prüfungsbewerter nachzuvollziehen.

Letztendlich kann das SSAOP auch Hilfestellung bei der Bedienung des Systems leisten. Abhängig von der aktiven Rolle werden Tipps und Anleitung zu Verfügung gestellt.

Funktionale Anforderungen des Nutzers:

Funktionale Anforderung 1: Bei der Einrichtung muss das SSAOP dem Systemadministrator die Möglichkeit bieten das User Interface an das Corporate Design der Prüfungsorganisation anzupassen.

Funktionale Anforderung 2: Das SSAOP muss eine integrierbare Nutzerverwaltung besitzen.

Funktionale Anforderung 3: Das SSAOP muss dem Nutzer die Möglichkeit bieten Änderungen auch teilweise abzuspeichern.

Funktionale Anforderung 4: Das SSAOP muss alle Nutzeraktionen protokollieren.

Qualitätsanforderungen des Nutzers:

Qualitätsanforderung 1: Das SSAOP muss dem Nutzer die Möglichkeit bieten das System intuitiv zu bedienen.

Qualitätsanforderung 2: Das SSAOP muss eine verschlüsselte Datenübertragung über das Netzwerk sicherstellen.

Qualitätsanforderung 3: Das SSAOP muss robust sein gegen Abstürze auf der Client- sowie Server-Seite.

Qualitätsanforderung 4: Das SSAOP muss dem Nutzer eine intelligente Hilfestellung bieten.

Randbedingungen des Nutzers:

Randbedingung 1: Das SSAOP muss dem Nutzer die Möglichkeit bieten von einem Windows bzw. einem MacOS Betriebssystem aus das System zu bedienen.

3.7.2 Systemadministrator

Die primäre Anforderung des Systemadministrators ist es, dass die Software auf dem Server einfach zu installieren ist. Das System läuft sowohl auf Windows als auch auf UNIX Betriebssystemen. Es benötigt minimalen Wartungsaufwand und Nutzersupport. Falls neue Fragentypen hinzukommen, ist es möglich diese ohne Neuinstallation hinzuzufügen. Das System kann eine angemessene Anzahl von gleichzeitigen Nutzern bedienen und ist skalierbar.

Daten können in zeitgemäßen Datenbanken, wie SQL oder NoSQL, abgelegt werden. Es ist möglich bereits vorhandene Datenbanken mit minimalen Anpassungsaufwand für die Speicherung von Fragen, Prüfungen, Antworten und Nutzerdaten zu verwenden. Der Systemadministrator ist auch zuständig für die Browsersoftware, die der Prüfling für das Ablegen der Prüfung einsetzt. Dieser Browser reduziert die Möglichkeiten der Täuschung, indem er manche Funktionen eines Standardbrowsers deaktiviert. Das SSAOP setzt daher einen Browser ein, der u.a. Druck-, Navigation-, Screenshot-, Chat- und Speicher-Funktionalitäten einschränkt.

Eine andere wesentliche Aufgabe des Systemadministrators ist das Hinzufügen von neuen Nutzermanagern, so dass das Hinzufügen von neuen Nutzer an andere Personen delegiert werden kann. Er kann außerdem Nutzermanagerinformationen bearbeiten sowie entfernen.

Funktionale Anforderungen des Systemadministrators:

Funktionale Anforderung 5: Das SSAOP muss über einen speziell gegen Täuschungen abgesicherten Browser für die Prüfungsabnahme verfügen.

Funktionale Anforderung 6: Das SSAOP muss dem Systemadministrator die Möglichkeit bieten Nutzermanager hinzuzufügen, zu entfernen und zu bearbeiten.

Qualitätsanforderungen des Systemadministrators:

Qualitätsanforderung 5: Das SSAOP muss auf allen Systemen leicht zu installieren sein.

Qualitätsanforderung 6: Das SSAOP muss dem Systemadministrator die Möglichkeit bieten neue Funktionalitäten ohne Neuinstallation umzusetzen.

Qualitätsanforderung 7: Das SSAOP muss eine große Anzahl von gleichzeitigen Nutzern unterstützen.

Randbedingungen des Systemadministrators:

Randbedingung 2: Das SSAOP muss auf einem Windows Server der aktuellen Generationen installierbar sein.

Randbedingung 3: Das SSAOP muss auf einem UNIX Server der aktuellen Generationen installierbar sein.

Randbedingung 4: Das SSAOP muss bereits existierende Datenbanksysteme unterstützen.

Randbedingung 5: Das SSAOP muss Daten in einer SQL oder NoSQL Datenbank ablegen können.

3.7.3 Nutzermanager

Das SSAOP kann eine vorhandene zentrale Nutzerverwaltung einbinden. Falls dies nicht erwünscht ist, ist es dem Nutzermanager möglich neue Nutzer wie Prüflinge oder andere Nutzer außer Systemadministratoren über die Nutzeroberfläche hinzuzufügen.

Nutzermanager sind des Weiteren dafür zuständig Nutzer, die einen Zugang zum SSAOP nicht mehr benötigen, zu entfernen. Das System unterstützt auch die Entfernung aller Nutzer, die einer Gruppe zugeordnet sind. Außerdem kann er für einzelne Nutzer den Zugang zum SSAOP für eine bestimmte Zeit sperren.

Funktionale Anforderungen des Nutzermanagers:

Funktionale Anforderung 7: Das SSAOP muss dem Nutzermanager die Möglichkeit bieten Nutzer hinzuzufügen, zu bearbeiten und zu entfernen.

Funktionale Anforderung 8: Das SSAOP muss dem Nutzermanager die Möglichkeit bieten alle Nutzer einer Gruppe zu entfernen.

Funktionale Anforderung 9: Das SSAOP muss dem Nutzermanager die Möglichkeit bieten Nutzer vorübergehend zu sperren.

3.7.4 Gruppenmanager

Der Gruppenmanager definiert Prüfungsgruppen und teilt diesen Prüflinge zu. Das Entfernen von Prüflingen von einer Gruppe wird ebenfalls vom Gruppenmanager durchgeführt. Eine Gruppe besteht aus einem oder mehreren Prüflingen, die an der gleichen Prüfung teilnehmen. Nur Gruppen können einer Prüfung zugewiesen werden, nicht jedoch einzelnen Prüflinge. Im Allgemeinen entspricht eine Gruppe der Menge von Studenten, die an einer Vorlesung teilnehmen. Der Gruppenmanager kann Informationen zu einer Gruppe in das SSAOP einstellen und entfernen.

Funktionale Anforderungen des Gruppenmanagers:

Funktionale Anforderung 10: Das SSAOP muss dem Gruppenmanager die Möglichkeit bieten Gruppen zu erstellen und Prüflinge diesen Gruppen hinzuzufügen.

Funktionale Anforderung 11: Das SSAOP muss dem Gruppenmanager die Möglichkeit bieten alle Prüflinge von einer Gruppe zu entfernen.

Funktionale Anforderung 12: Das SSAOP muss dem Gruppenmanager die Möglichkeit bieten Informationen zu Gruppen einzustellen.

3.7.5 Fragenersteller

Der Fragenersteller kreiert Fragen. Er könnte außerdem Fragenbetrachter sein, weswegen er Zugang zum Fragenkatalog erhalten muss, um bereits veröffentlichte Fragen anzuschauen und bspw. deren Fragenstil zu übernehmen.

In dieser Arbeit werden die unterschiedlichen Fragentypen nicht diskutiert, trotzdem sollte das System fähig sein eine breite Auswahl von möglichen Fragetypen anzubieten. Der Fragenersteller kann außerdem Hinweise zu Fragen hinzufügen, um den Prüfling bei komplexen Fragen zu unterstützen. Auch multimediale Inhalte wie Bilder, Audio und Video können in die Frage integriert werden. Fragen, die offline z.B. in einer XML Datei erstellt werden, können in das System importiert werden.

Es ist möglich Fragen vor der Veröffentlichung in einer Vorschau, die sehr nahe an der Sicht des Prüflings ist, zu begutachten. Fragenersteller können Fragen, die bereits von Prüflingen beantwortet wurden, nachträglich nicht mehr verändern. Dies ist aus Gründen der Nachvollziehbarkeit zu unterbinden. Es ist ihnen aber möglich Fragen zu kopieren und im Anschluss die Kopie zu verändern, um eine Wiederverwendbarkeit von Inhalten zu gewährleisten. Diese Funktion ist des Weiteren hilfreich, um Fragen in alternativen Versionen abzufassen.

Erstellten Fragen wird eine eindeutige Nummer zur Identifikation zugewiesen. Dies ist auch der Fall, falls eine weitere Frage mit dem gleichen Text erzeugt wird.

Funktionale Anforderungen des Gruppenmanagers:

Funktionale Anforderung 13: Das SSAOP muss dem Fragenersteller die Möglichkeit bieten Fragen zu erstellen.

Funktionale Anforderung 14: Das SSAOP muss dem Fragenersteller die Möglichkeit bieten Fragen zu betrachten und zu adaptieren.

Funktionale Anforderung 15: Das SSAOP muss dem Fragenersteller die Möglichkeit bieten Fragen in nicht proprietären Formaten zu importieren bzw. exportieren.

Funktionale Anforderung 16: Das SSAOP muss einer Frage automatische eine eindeutige Identifikationsnummer zuweisen.

3.7.6 Fragenbetrachter

Eine Vielzahl von Nutzer können einen Zugriff auf einzelne Fragen oder Fragenkataloge benötigen. Der Zugriff wird auf Grundlage des Themenbereichs oder der ID der Frage zugewiesen. Gründe für diese Aktion könnten sein, dass Fragen, die von anderen Nutzer eingestellt wurden, begutachtet werden müssen oder Fragen aus älteren Prüfungen als Vorlage dienen sollen. Nutzermanager geben Fragenbetrachtern Zugriff auf Fragen oder Fragenkataloge.

Funktionale Anforderungen des Fragenbetrachters:

Funktionale Anforderung 17: Das SSAOP muss dem Fragenbetrachter die Möglichkeit bieten Fragen anzuschauen.

3.7.7 Fragenvalidierer

Oft werden Fragen von jemand anderem als dem Autor validiert bevor sie den Studenten vorgelegt werden. Der Fragenvalidierer erhält den Status eines Fragenbetrachters für einen ausgewählten Fragenkatalog. Er kann einzelne Fragen des Fragenkatalogs freigeben bzw. ablehnen und bei Bedarf einen Kommentar hinterlassen. Diese Informationen werden dem Fragenersteller automatisch mitgeteilt.

Funktionale Anforderungen des Fragenvalidierers:

Funktionale Anforderung 18: Das SSAOP muss dem Fragenvalidierer die Möglichkeit bieten Fragen freizugeben bzw. abzulehnen.

Funktionale Anforderung 19: Das SSAOP muss dem Fragenvalidierer die Möglichkeit bieten Fragen zu kommentieren.

Funktionale Anforderung 20: Das SSAOP muss dem Fragenersteller die Kommentare des Fragenvalidierers automatisch mitteilen.

3.7.8 Prüfungsersteller

Prüfungsersteller kombinieren Fragen, die bereits von Frageerstellern kreiert wurden. Sie können einzelnen Fragen unterschiedliche Bewertungskriterien zuordnen, wie z.B. die Anzahl der Punkte bei richtiger oder Negativpunkte bei falscher Beantwortung der Frage. Er kann die Darstellung der Prüfung konfigurieren. So kann er bspw. einstellen, dass die gesamte Prüfung auf einer Seite bzw. eine Frage pro Seite dargestellt wird. Außerdem kann er Fragen nach Themen gruppieren. Auch die Bestimmung des Layouts gehört zu den Fähigkeiten des Prüfungserstellers. Um das Ergebnis seiner Arbeit begutachten zu können, ist er in der Lage eine Vorschau der Prüfung testweise anzeigen zu lassen.

Um die Konsistenz der Daten zu gewährleisten, kann der Prüfungsersteller eine Prüfung, die Prüflinge bereits angetreten haben, nicht löschen. Jedoch kann er diese als Vorlage für die Generierung einer Kopie nutzen, um bspw. eine Variation der Prüfung zu erstellen.

Der Prüfungsersteller kann einstellen, ob die Prüfungsfragen zufällig angeordnet oder nach Theme gruppiert werden sollen. Er kann des Weiteren die Reihenfolge der Antwortmöglichkeiten bestimmen und diese auch zufällig verteilen lassen.

Vom Prüfungsersteller wird ebenfalls entschieden, ob eine Prüfung für die formale Beurteilung oder für die Selbsteinschätzung verwendet wird. Sollte eine Prüfung der formalen Beurteilung dienen, so kann der Prüfungsersteller unterstützende Funktionen, wie das Anzeigen von Hinweisen oder Rückmeldungen deaktivieren. Er kann auch bestimmen, wie viele Versuche der Prüfling für die Beantwortung der Frage hat.

Alle Prüfungen haben eine eindeutige ID und können bei Bedarf exportiert werden, um in einem anderen System eingesetzt zu werden.

Funktionale Anforderungen des Prüfungserstellers:

Funktionale Anforderung 21: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten Fragen zu einer Prüfung zu kombinieren.

Funktionale Anforderung 22: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten Fragen Bewertungskriterien zuzuweisen.

Funktionale Anforderung 23: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten die Darstellung der Fragen zu bestimmen.

Funktionale Anforderung 24: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten die Reihenfolge der Fragen zu bestimmen bzw. diese zufällig zu verteilen.

Funktionale Anforderung 25: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten Reihenfolge der Antworten zu bestimmen bzw. diese zufällig zu verteilen.

Funktionale Anforderung 26: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten eine Vorschau der Prüfung zu betrachten.

Funktionale Anforderung 27: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten Hilfestellungen und Rückmeldungen über Ergebnisse zu aktivieren bzw. deaktivieren.

Funktionale Anforderung 28: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten die Anzahl der Antwortversuche zu bestimmen.

Funktionale Anforderung 29: Das SSAOP muss einer Prüfung automatische eine eindeutige Identifikationsnummer zuweisen.

Funktionale Anforderung 30: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten Prüfungen in nicht proprietären Formaten zu importieren bzw. exportieren.

3.7.9 Prüfungsbetrachter

Ein Prüfungsbetrachter kann ganze Prüfungen ansehen, ohne sie in irgendeiner Weise ändern zu können. Sie können eine Vorschau der Prüfung anschauen oder die Prüfung testen, um zu sehen, wie sie sich dem Prüfling präsentiert. Diese Rolle wird oft dem Tutor zugeteilt, der die Prüflinge auf die Prüfung vorbereitet.

Funktionale Anforderungen des Prüfungsbetrachters:

Funktionale Anforderung 31: Das SSAOP muss dem Prüfungsbetrachter die Möglichkeit bieten eine Vorschau der Prüfung anzuschauen.

Funktionale Anforderung 32: Das SSAOP muss dem Prüfungsbetrachter die Möglichkeit bieten an einer Prüfung testweise teilzunehmen.

3.7.10 Prüfungsvalidierer

Die Rolle des Prüfungsvalidierers ist ähnlich zu der Rolle des Fragenvalidierers. Er kann bspw. bestätigen, ob das Bewertungsschema einer Prüfung angemessen ist und diese Feststellung im System dokumentieren. Des Weiteren kann er Kommentare zu den Prüfungen hinterlassen. Ein Prüfungsvalidierer ist auch ein Prüfungsbetrachter. Alle Prüfungen müssen vor dem Einsatz validiert werden.

Funktionale Anforderungen des Prüfungsvalidierers:

Funktionale Anforderung 33: Das SSAOP muss dem Prüfungsvalidierer die Möglichkeit bieten Prüfungen freizugeben bzw. abzulehnen.

Funktionale Anforderung 34: Das SSAOP muss dem Prüfungsvalidierer die Möglichkeit bieten Prüfungen zu kommentieren.

Funktionale Anforderung 35: Das SSAOP muss dem Prüfungsersteller die Kommentare des Prüfungsvalidierer automatisch mitteilen.

3.7.11 Prüfungsplaner

Der Prüfungsplaner wählt validierte Prüfungen aus und teilt sie Gruppen zu, die die Prüfung antreten müssen. Er bestimmt die Uhrzeit und das Datum der Prüfung sowie das Zeitfenster, innerhalb dessen die Prüfung von den Prüflingen angetreten werden muss. Außerdem bestimmt er die Prüfungsaufsicht, die die Prüfung überwacht.

Funktionale Anforderungen des Prüfungsplaners:

Funktionale Anforderung 36: Das SSAOP muss dem Prüfungsplaner die Möglichkeit bieten eine Prüfung einer Gruppe zu einer bestimmten Zeit und einem festgelegten Datum zugänglich zu machen.

Funktionale Anforderung 37: Das SSAOP muss dem Prüfungsplaner die Möglichkeit bieten ein Zeitfenster zu bestimmen, innerhalb dessen der Prüfling die Prüfung starten kann.

Funktionale Anforderung 38: Das SSAOP muss dem Prüfungsplaner die Möglichkeit bieten eine oder mehrere Prüfungsaufsichten für eine Prüfung zu bestimmen.

3.7.12 Prüfungsaufsicht

In den meisten Fällen werden Prüfungen beaufsichtigt. Die Aufsicht benötigt daher Zugriff auf die Überwachungsdaten der Prüflinge, um diese zu analysieren.

Funktionale Anforderungen der Prüfungsaufsicht:

Funktionale Anforderung 39: Das SSAOP muss der Prüfungsaufsicht die Möglichkeit bieten die Überwachungsdaten jedes Prüflings, den er beaufsichtigt, anzuschauen.

3.7.13 Prüfling

Nach der Anmeldung am SSAOP können Prüflinge die aktuell verfügbaren Prüfungen anzeigen lassen. Sie haben Zugriff auf die Ergebnisse der Prüfungen, die sie bereits abgelegt haben und können gegebenenfalls Kommentare zu der Prüfung sowie den Namen des Prüfungsbewerters einsehen. Sie können auch Zeit und Datum von anstehenden Prüfungen sehen. Dem Prüfling werden nach der Anmeldung auch Prüfungen angezeigt, die noch aktiv und nicht

abgeschlossen sind. Die Punkteanzahl zu jeder Frage ist klar ersichtlich, falls diese angezeigt werden sollen. Die Anordnung der Fragen ist, je nach Konfiguration durch den Prüfungsersteller, zufällig. Dies kann helfen, den Austausch der Fragen zwischen den Prüflingen für Täuschungszwecke zu erschweren.

Dem Prüfling ist es möglich Fragen, die er nicht beantworten kann zu überspringen. Er kann das Ergebnis der Prüfung gleich im Anschluss an die Prüfung oder aber erst ab einem bestimmten Zeitpunkt einsehen. Dieser wird vom Prüfungsplaner festgelegt.

Anleitungen zur Beantwortung der Fragen werden gut sichtbar angezeigt und stehen dem Prüfling jederzeit während der Prüfung zur Verfügung. Dem Prüfling ist es auch möglich die abgelaufene Zeit seit dem Beginn der Prüfung und die verbleibende Zeit bis zum Ende der Prüfung zu sehen. Den Prüflingen kann es erlaubt sein, bereits beantwortete Fragen abzuändern, bevor sie endgültig abgegeben werden. Im Falle eines Systemabsturz sollte die Arbeit und Mühe der Prüflinge nicht verloren gehen. Daher sollten ihre Antworten regelmäßig statt nur am Ende der Prüfung abgesichert werden.

Zu einem festgelegten Zeitpunkt vor der Prüfung (z.B. eine Woche davor) wird der Prüfling per Email an die Prüfung erinnert. Dies muss der Prüfungsplaner einstellen. Sobald die Prüfung abgegeben wurde, erhält der Prüfling eine Bestätigung per Email mit dem Datum und der Uhrzeit der Abgabe. Nach der Bewertung können Prüflinge Kommentare vom Prüfungsbewerter einsehen, sobald diese eingestellt und freigegeben sind.

Qualitätsanforderungen des Prüflings:

Qualitätsanforderung 8: Das SSAOP muss die erreichbaren Punkte pro Frage gut sichtbar darstellen.

Qualitätsanforderung 9: Das SSAOP muss die Fragen, Antworten und Anleitungen gut sichtbar darstellen.

Funktionale Anforderungen des Prüflings:

Funktionale Anforderung 40: Das SSAOP muss dem Prüfling die Möglichkeit bieten alle aktuell verfügbaren Prüfungen einzusehen.

Funktionale Anforderung 41: Das SSAOP muss dem Prüfling die Möglichkeit bieten die Ergebnisse, Kommentare und Antworten von bereits abgelegten Prüfungen anzuschauen.

Funktionale Anforderung 42: Das SSAOP muss dem Prüfling die Möglichkeit bieten Zeit und Datum von künftigen Prüfungen zu sehen.

Funktionale Anforderung 43: Das SSAOP muss dem Prüfling die Möglichkeit bieten frühzeitig verlassene Prüfungen weiterführen zu können, sofern die Prüfungsdauer nicht abgelaufen ist.

Funktionale Anforderung 44: Das SSAOP muss dem Prüfling die Möglichkeit bieten Prüfungsergebnisse im Anschluss bzw. ab einem bestimmten Zeitpunkt einsehen zu können.

Funktionale Anforderung 45: Das SSAOP muss dem Prüfling die Möglichkeit bieten die abgelaufene Zeit seit Prüfungsbeginn und die restliche Zeit bis zum Prüfungsende zu sehen.

Funktionale Anforderung 46: Das SSAOP muss dem Prüfling die Möglichkeit bieten bereits bearbeitete oder übersprungene Fragen erneut aufrufen zu können.

Funktionale Anforderung 47: Das SSAOP muss dem Prüfling die Möglichkeit bieten bereits ausgewählte Antworten ändern zu können.

Funktionale Anforderung 48: Das SSAOP muss Antworten regelmäßig absichern, nicht nur am Ende vom Test.

Funktionale Anforderung 49: Das SSAOP muss dem Prüfling eine Erinnerungsemail zu einer festgelegten Zeit schicken.

Funktionale Anforderung 50: Das SSAOP muss dem Prüfling eine Bestätigungsemail über den Erhalt der Prüfung schicken.

Funktionale Anforderung 51: Das SSAOP muss dem Prüfling eine Email mit dem Prüfungsergebnis zu einer festgelegten Zeit schicken.

3.7.14 Antwortüberwacher

Der Antwortüberwacher hat Zugriff auf alle Antworten, die von Prüflingen eingereicht wurden zusammen mit den Kommentaren der Prüfungsbewerter. Das Hauptziel dieser Rolle ist es, zu überprüfen, ob die Prüflinge die Fragen angemessen beantwortet haben und anhand der Antworten festzustellen, ob es möglicherweise Missverständnisse gab.

Funktionale Anforderungen des Antwortüberwachers:

Funktionale Anforderung 52: Das SSAOP muss dem Antwortüberwacher die Möglichkeit die Antworten von Prüflingen und die dazugehörigen Kommentare der Prüfungsbewerter einzusehen.

3.7.15 Prüfungsbewerter

Nicht automatisierte Fragentypen wie Freitextaufgaben können ebenfalls Bestandteil einer Prüfung sein. Dem Prüfungsbewerter wird vom SSAOP angezeigt, was er bewerten muss. Er kann die Antworten der Prüflinge einsehen und Kommentare sowie Bewertungen hinzufügen. Er kann Notizen zu einzelnen Prüflingen, Fragen, Antworten oder Prüfungen ablegen. Alle Kommentare werden persistiert und können zu einem späteren Zeitpunkt wieder abgerufen werden. Falls ein Prüfungsbewerter es versäumt eine Prüfung rechtzeitig (die Zeit wird vom Prüfungsplaner festgelegt) zu bewerten, wird er automatisch per Email daran erinnert.

Funktionale Anforderungen des Prüfungsbewerters:

Funktionale Anforderung 53: Das SSAOP muss dem Prüfungsbewerter anzeigen, was er bewerten muss.

Funktionale Anforderung 54: Das SSAOP muss dem Prüfungsbewerter die Möglichkeit bieten Kommentare zu Antworten anzuschauen und zu erstellen.

Funktionale Anforderung 55: Das SSAOP muss dem Prüfungsbewerter die Möglichkeit bieten Antworten zu bewerten.

Funktionale Anforderung 56: Das SSAOP muss dem Prüfungsbewerter die Möglichkeit bieten Notizen zu erstellen.

Funktionale Anforderung 57: Das SSAOP muss den Prüfungsbewerter automatisch benachrichtigten, wenn er eine Prüfung nicht rechtzeitig bewertet hat.

3.7.16 Bewertungsüberwacher

Der Bewertungsüberwacher ist in der Lage, die Antwort aller Prüflinge zu einer bestimmten Prüfungsfrage zu sehen. Er kann auch sehen, wie lange die Prüflinge im Durchschnitt mit einer Frage beschäftigt waren. Des Weiteren kann er erkennen, wie oft welche Antwortmöglichkeit gewählt wurde. Diese Informationen werden genutzt, um schlechte Fragen auszusortieren. Dies ist der Fall, wenn bspw. sehr viele Prüflinge eine Frage falsch beantworten bzw. sich sehr lange mit einer Frage beschäftigen.

Funktionale Anforderungen des Bewertungsüberwacher:

Funktionale Anforderung 58: Das SSAOP muss dem Prüfungsbewerter die Möglichkeit bieten die Antwort aller Prüflinge zu einer bestimmten Prüfungsfrage zu sehen.

Funktionale Anforderung 59: Das SSAOP muss dem Prüfungsbewerter die Möglichkeit bieten die durchschnittliche Verweildauer aller Prüflinge pro Frage zu sehen.

Funktionale Anforderung 60: Das SSAOP muss dem Prüfungsbewerter die Möglichkeit bieten zu sehen, wie oft eine Antwortmöglichkeit gewählt wurde.

3.7.17 Notenkorrektor

Es kann vorkommen, dass Bewertungen geändert werden müssen, wenn z.B. eine Frage falsch gestellt wurde oder ein Prüfling getäuscht hat. Notenkorrektoren können die Bewertung ändern, müssen jedoch einen Grund für die Änderung angeben. Alle derartigen Änderungen sowie die Originalbewertung werden protokolliert, um die Nachvollziehbarkeit zu gewährleisten.

Funktionale Anforderungen des Notenkorrektors:

Funktionale Anforderung 61: Das SSAOP muss dem Notenkorrektor die Möglichkeit bieten Bewertungen nur unter Angabe eines Grunds zu ändern.

Funktionale Anforderung 62: Das SSAOP muss die Originalbewertung und alle Änderungen protokollieren.

3.7.18 Forscher

Der Forscher untersucht die Statistiken des Systems, um z.B. das Verhalten der Prüflinge zu untersuchen. Er kann alle Daten sehen, die sich auf Prüfungen und Prüflinge beziehen, jedoch sind sie pseudonomisiert oder anonymisiert.

Funktionale Anforderungen des Forschers:

Funktionale Anforderung 63: Das SSAOP muss dem Forscher die Möglichkeit bieten Daten für Forschungszwecke einzusehen, ohne personenbezogene Daten sehen zu können.

3.8 Informationssicherheitsanforderungen

Das Prüfungsabnahmesystem ist ein System, das mit Informationen arbeitet. Daher sollten hierfür auch die Aspekte der Informationssicherheit analysiert werden, um mögliche nichtfunktionale Anforderungen davon abzuleiten. Im Folgenden werden die Aspekte im Kontext des SSAOP betrachtet.

3.8.1 Vertraulichkeit

Beim SSAOP haben die beteiligten Parteien, wie bswp. der Prüfling, der die Prüfung oder der Prüfer, der die Ergebnisse anschauen darf, unterschiedliche Vertraulichkeitsanforderungen. Um Vertraulichkeit zu gewährleisten, müssen die im System persistierten oder zwischen zwei Systemen übertragenen Daten vor unautorisiertem Zugriff geschützt werden. Eine sehr gängige Methode um Vertraulichkeit zu erhalten ist die Verschlüsselung der Informationen.

Die Verschlüsselung sorgt dafür, dass nur berechtigte Personen mit Hilfe eines Schlüssels an die Informationen kommen. Um die Vertraulichkeit der ausgetauschten Informationen zu schützen, muss also das System diese Informationen verschlüsseln ([Per08]).

Qualitätsanforderung aus der Informationssicherheit:

Qualitätsanforderung 10: Das SSAOP muss die Vertraulichkeit der übertragenen und abgespeicherten Informationen sicherstellen.

3.8.2 Integrität

Auch die Integrität der Daten bedarf einem Schutz vor unberechtigter Manipulation, Löschung, Veränderung und Erweiterung. Die Integrität muss auch hier in der Kommunikation und Speicherung der Informationen erhalten werden. Mit Hilfe einer digitalen Signatur oder einem Zugriffsschutz können unberechtigte Personen daran gehindert werden Informationen zu manipulieren.

Qualitätsanforderung aus der Informationssicherheit:

Qualitätsanforderung 11: Das SSAOP muss die Integrität der übertragenen und abgespeicherten Informationen sicherstellen.

3.8.3 Verfügbarkeit und Zuverlässigkeit

Die Verfügbarkeit der Informationen muss den Nutzern des SSAOP garantiert werden. Das kritischste Szenario wäre, wenn der Prüfling an der Prüfung teilnehmen will, diese jedoch nicht aufrufen kann. Daher muss durch Redundanz dafür gesorgt werden, dass bei einem Ausfall des Systems ein Ersatzsystem einspringt. Außerdem muss das SSAOP zuverlässig sein, da auch nur kurze Unterbrechung während der Prüfung, wenn sie regelmäßig auftreten, den Prüfling erheblich stören können.

Qualitätsanforderungen aus der Informationssicherheit:

Qualitätsanforderung 12: Das SSAOP muss die Verfügbarkeit der Informationen sicherstellen.

Qualitätsanforderung 13: Das SSAOP muss eine zuverlässige Nutzung sicherstellen.

3.8.4 Authentizität

Es muss sichergestellt sein, dass es sich bei dem Prüfling tatsächlich um die an der Prüfungsteilnahme berechtigte Person handelt. Der Authentizitätsnachweis umfasst zwei Prozesse, die Authentifizierung und Authentisierung. Die Authentifizierung bezeichnet den Prozess einer Person oder Objekt herauszufinden, ob eine andere Person oder Objekt tatsächlich das ist,

was sie oder es vorgibt zu sein. Bei der Authentisierung weist eine Person oder Objekt die eigene Authentizität nach. Dies bedeutet, dass das SSAOP den Prüfling authentifizieren muss. Es reicht jedoch nicht den Prüfling nur am Anfang zu überprüfen, da dieser danach ausgetauscht werden könnte. Daher muss der Prüfling kontinuierlich überwacht werden.

Es gibt bspw. folgende Möglichkeiten kontinuierliche Authentizität sicherzustellen:

- Abgleich des Gesichts
- Abgleich des Tippverhalten
- Abgleich des Mausverhaltens

Jeder dieser Möglichkeiten setzt voraus, dass dem SSAOP bereits überprüfte Referenzdaten vom berechtigten Nutzer bekannt sind. Bei der Gesichtserkennung bspw. werden die biometrischen Merkmale des Gesichts extrahiert und mit den Merkmalen auf bereits vorhandenen Bildern des tatsächlich zur Prüfung angemeldeten Teilnehmers abgeglichen. Beim Tipp- und Mausverhalten wird die Art und Weise, wie der Prüfling Eingaben tätigt bzw. den Mauszeiger bewegt mit einem vorher erstellten Verhaltensmodell verglichen.

Qualitätsanforderung aus der Informationssicherheit:

Qualitätsanforderung 14: Das SSAOP muss die kontinuierliche Authentizität des Prüflings sicherstellen.

3.8.5 Verbindlichkeit und Zurechenbarkeit

Ein Prüfling sollte nach Abgabe der Prüfung nicht abstreiten können, dass die abgegeben Prüfung von ihm stammt. Daher muss sichergestellt werden, dass die Aktivitäten des Prüfling eindeutig zurechenbar sind. Ein gängiges Verfahren hierfür ist die Protokollierung der Aktivitäten. Auch muss die Verbindlichkeit bspw. durch personalisierte Zertifikate gewährleistet werden, so dass bspw. der Prüfling nach der Prüfung seine Teilnahme nicht abstreiten kann.

Qualitätsanforderung aus der Informationssicherheit:

Qualitätsanforderung 15: Das SSAOP muss die Verbindlichkeit der Prüfungsteilnahme der Nutzeraktivitäten sicherstellen.

Qualitätsanforderung 16: Das SSAOP muss die Zurechenbarkeit der Nutzeraktivitäten sicherstellen.

3.9 Analyse von Prüfungsordnungen

Für die Analyse der Prüfungsordnungen werden die Prüfungsordnungen der fünf größten Universitäten Deutschlands (mit den meisten Studierenden, Stand: WS 16/17) [wik76] im Fach Bachelor Informatik (bzw. Wirtschaftsinformatik, falls Informatik nicht angeboten

wird) jeweils in der aktuellsten Fassung herangezogen. Dazu gehören die Fernuniversität Hagen, Ludwigs-Maximilians-Universität, Universität zu Köln, Johann Wolfgang Goethe-Universität und Westfälische Wilhelms-Universität. Das Ziel der Analyse ist es Anforderungen zu identifizieren, die Auswirkung auf das System haben. Hierbei wird insbesondere darauf geachtet, ob und welche Aussagen zu Online Prüfungen und Täuschungen gemacht werden.

Die Fernuniversität Hagen erlaubt mündliche Prüfungen auf elektronischem Weg über eine Ton- und Bildverbindung auf Antrag und im Einvernehmen mit dem Prüfenden. Dabei muss eine vom Prüfungsausschuss bestellte Person am Ort des Prüflings anwesend sein und die Ordnungsmäßigkeit der Prüfung sicherstellen. Schriftliche Prüfungen dürfen nur vor Ort durchgeführt werden (vgl. [fer17]).

An der Westfälische Wilhelms-Universität sind Online Prüfungen nicht explizit erlaubt. Grundsätzlich gilt nur, dass der Dozent einer Veranstaltung auch der Prüfer der seiner Veranstaltung zugeordneten Prüfungsleistungen sein muss und für die Überwachung verantwortlich ist. Wie der Prüfer die Prüfung überwachen muss, ist jedoch nicht beschrieben. Ob online-basierte Überwachungsmethoden zulässig sind, bleibt daher offen (vgl. [wes17]).

Die Universität zu Köln beschreibt in ihrer Prüfungsordnung die Ausprägungen von schriftlichen Prüfungsformen. Demnach ist eine Klausur eine unter Aufsicht anzufertigende Arbeit, in der vorgegebene Aufgaben allein und selbstständig nur mit den zugelassenen Hilfsmitteln zu bearbeiten sind. Außerdem sind Klausuren in elektronischer Form zugelassen. Nach der Prüfungsordnung ist die E-Klausur eine Prüfung, die am Computer mittels eines Prüfungsprogramms durchgeführt wird und deren Erstellung, Durchführung und Auswertung insgesamt durch Informations- und Kommunikationstechnologien unterstützt wird. Dem Prüfling muss vor der Prüfung ausreichend Zeit haben, sich mit dem elektronischen Prüfungssystem vertraut zu machen. Allerdings ist die E-Klausur in Anwesenheit einer Person durchzuführen, die über den Prüfungsverlauf eine Niederschrift anfertigt. In diese müssen bspw. die Namen des Protokollführers und der Prüflinge, Beginn und Ende der Prüfung sowie besondere Vorkommnisse aufgenommen werden. Des Weiteren muss sichergestellt sein, dass die elektronischen Daten eindeutig und dauerhaft dem Prüfling zugeordnet werden können. Dem Prüfling ist außerdem nach Bekanntgabe des Prüfungsergebnis die Möglichkeit der Einsichtnahme in die Prüfung zu gewähren. Diese Anforderungen wurden in der bisherigen Anforderungsanalyse bereits berücksichtigt (vgl. [uni17]).

E-Klausuren werden in der Prüfungsordnung der Johann Wolfgang Goethe-Universität nicht behandelt. Daher resultieren hieraus keine besonderen Anforderungen an das SSAOP (vgl. [wgu17]).

Die Ludwig-Maximilans-Universität fordert, dass bei E-Klausuren die datenschutzrechtlichen Bestimmung einzuhalten sind (vgl. [lmu17]).

Qualitätsanforderung aus den Prüfungsordnungen

Qualitätsanforderung 17: Das SSAOP muss den Datenschutz der Nutzer sicherstellen.

In allen Prüfungsordnungen wird benachteiligten Prüflingen ein Nachteilsausgleich eingeräumt. So muss für einen Prüfling, der glaubhaft machen kann, dass er wegen einer chronischen Krankheit oder einer Behinderung nicht in der Lage ist, die Prüfungsleistung ganz oder teilweise in der vorgesehenen Prüfungsdauer bzw. Frist abzulegen, die Bearbeitungszeit für die Prüfung bzw. die Fristen für das Ablegen der Prüfung verlängert werden.

Funktionale Anforderung aus den Prüfungsordnungen

Funktionale Anforderung 64: Das SSAOP muss dem Prüfungsplaner die Möglichkeit bieten für einzelne Prüflinge die Prüfungsdauer zu verlängern.

Funktionale Anforderung 65: Das SSAOP muss dem Prüfungsplaner die Möglichkeit bieten für einzelne Prüflinge die Prüfungsfrist zum Ablegen der Prüfung zu verlängern.

Für Täuschung sind in allen fünf Prüfungsordnungen Disziplinarmaßnahmen vorgesehen. Hat der Prüfling bei einer Prüfung getäuscht, kann der Prüfer nachträglich das Ergebnis für diejenigen Prüfungen, bei deren Erbringen der Prüfling getäuscht hat, entsprechend berichtigen oder diese Leistungen ganz oder teilweise für nicht bestanden erklären, auch falls diese Tatsache erst nach der Aushändigung des Zeugnisses bekannt wird. Im Extremfall kann dies sogar zur Aberkennung des Abschluss führen.

Keine der fünf Universitäten behandelt Online Prüfungen. Lediglich E-Klausuren, also Prüfungen die zwar elektronisch, jedoch an einen bestimmten Ort gebunden sind, werden teilweise erwähnt. Bei E-Klausuren muss am Ort des Prüflings eine vom Prüfungsausschuss bestellte Aufsicht anwesend sein. Aufgrund der fehlenden Berücksichtigung von Online Prüfungen bedarf es beim Einsatz des SSAOPs einer Überarbeitung der Prüfungsordnungen, da die geltenden Ordnungen diese Art von Prüfung bislang ausschließen.

3.10 Täuschungsszenarien

Studenten haben viele Möglichkeiten sich regelwidrige Unterstützung bei Online Prüfungen zu erschleichen. Rowe beschreibt drei typische Kategorien, die Studenten beim Täuschen einsetzen können. Studenten verzögern die Prüfungsabnahme, um an die Prüfungsfragen von anderen Studenten zu kommen, er wiederholt die Prüfung aufgrund von falschen Behauptungen oder er bedient sich unerlaubter Hilfe während der Prüfungsabnahme, welche mit unterschiedlichen Techniken erlangt werden kann (vgl. [Row04]). Die Täuschungsversuche der ersten und dritten Kategorie betreffen nicht nur Online Prüfungen, sondern können auch bei Präsenzklausuren erfolgen. Daneben sind noch weitere Szenarien denkbar. So kann die Prüfung durch einen dritte Person, einem sog. Double, abgelegt werden, der statt dem echten Prüfling den Prüfungstermin wahrnimmt. Außerdem kann der Prüfling ein unerlaubtes Hilfsmittel, wie z.B. einen Spicker, einsetzen, um an Informationen zu kommen. Im Folgenden werden die Szenarien erläutert und passende Gegenmaßnahmen, die im nächsten Kapitel erklärt werden, genannt.

3.10.1 Unberechtigter Besitz von Prüfungsfragen

Manche Universität bieten zwei oder mehr Termine für das Ablegen der Prüfung an. Meist wird der erste Termin für vor und der zweite für nach den Semesterferien festgesetzt. Dieses Angebot nutzen manche Studenten aus, indem sie warten bis ihre Kommilitonen die erste Prüfung mitschreiben, um sich dann von diesen die Prüfungsfragen zu besorgen. Um die Fragen in Besitz zu bringen prägen sich die Teilnehmer der ersten Prüfung so viele Fragen wie möglich ein oder fotografieren die Prüfung mit ihrem Smartphone ab. Eine andere Möglichkeit ist der Einsatz einer Foto - bzw. Videobrille. Diese Brille mit integrierter Kamera kann unbemerkt Aufnahmen von der Prüfung machen und sie auf einem internen Speicher ablegen. Die erlangten Fragen werden dann an die Teilnehmer der zweiten Prüfung weitergeleitet. Diese erhoffen sich durch die vorab besorgten Fragen eine bessere Vorbereitung auf die Prüfung oder die Optimierung des Spickzettels. Natürlich klappt dieser Trick nur, wenn die Prüfungen an den unterschiedlichen Terminen gleich oder zumindest ähnlich sind. Da Professoren, wie in der Einleitung geschildert, unter Zeitmangel leiden, kann es durchaus vorkommen, dass Klausuren nur unzureichend oder gar nicht abgeändert werden.

Gegenmaßnahmen: 3.11.1, 3.11.3, 3.11.5, 3.11.9, 3.11.11

3.10.2 Vermeintliche Störungen

Störungen können einen Prüfling bei der Prüfungsbearbeitung massiv behindern, falls sich diese nicht sofort beheben lassen, ständig wieder auftauchen oder gar die Verbindung zum System kappen. Beispiele für schwerwiegende Störungen sind fehlender Internetzugang oder ein Stromausfall. Aber auch einfachere Störungen, wie eine immer wieder aufgehende Fehlermeldung, aufgrund eines Softwarefehlers, führen dazu, dass sich der Student nicht mehr ganz auf die Bearbeitung der Prüfung konzentrieren kann. Diese Umstände führen aber auch dazu, dass der Prüfling bei der Erbringung der Prüfungsleistung drastisch benachteiligt wird. Aus diesem Grund haben die meisten Institutionen für diese Fälle Ausnahmeregelungen definiert, die unter Umständen auch eine Wiederholung der Prüfung vorsehen. Diese Ausnahmeregelung kann von unvorbereitete Studenten ausgenutzt werden, um entweder mehr Zeit für die Vorbereitung zu gewinnen, einen Blick in die Prüfung zu erhalten oder beides. Durch falsche Behauptungen versuchen sie eine Wiederholung der Prüfung zu provozieren. Ein Beispiel dafür könnte ein vorgetäuschter Stromausfall sein mit der Behauptung, dass während der Bearbeitung der Prüfung der Rechner sich ausgeschaltet hat. In Wirklichkeit hat der Student sich möglichst viele Fragen eingeprägt, bevor er den PC eigenhändig ausgeschaltet hat. Dadurch kommt der Prüfling unberechtigt in Besitz von Fragen und kann sich, da die Bearbeitung einer Störung eine gewisse Zeit beansprucht, in Ruhe die Lösungen besorgen.

Gegenmaßnahmen: 3.11.5, 3.11.7, 3.11.9, 3.11.11

3.10.3 Zusammenarbeit mit Dritten

Eine weiterer Methode der Täuschung ist die Zusammenarbeit mit Dritten, beispielsweise wenn Nachbarn sich bei einer Präsenzklausur die Lösungen gegenseitig zuflüstern. Mit „Zusammenarbeit“ ist jedoch nicht nur die Gemeinschaftsarbeit zwischen den Prüflingen gemeint, sondern auch die Hilfe von Dritten, die nicht gezwungenermaßen an der Veranstaltung beteiligt sein müssen. Online Prüfung haben die Besonderheit, dass sich die Teilnehmer der

Prüfung meistens an unterschiedlichen Orten befinden. Das bedeutet aber nicht, dass es keine Zusammenarbeit geben könnte. Trotz der Distanz gibt es für Studenten Möglichkeiten sich mit anderen Prüflingen zusammenzuschließen und die Prüfung so gemeinsam zu lösen. Einer dieser Möglichkeiten ist der Einsatz eines Smartphone Messengers. Aber auch die Nutzung des Instant Messenger auf dem PC wäre denkbar. Es gibt jedoch auch ausgefeilter Vorgehensweise, um möglichst unauffällig an fremde Hilfe zu kommen. Diese erfordern jedoch den Einsatz von spezieller Technik. Eine Brille mit einer verstecken integrierten Kamera (siehe Abbildung 3.3) kann benutzt werden, um das Blickfeld des Prüflings per Bluetooth an das Smartphone zu leiten, welches dieses wiederum an den PC eines Komplizen z.B. im Nebenraum schickt. Der Komplize, der sich entweder gut mit dem Prüfungsstoff auskennt oder aber lediglich im Besitz der Lösungen ist, kann die Fragen in Ruhe bearbeiten und die Antwort mit Hilfe von kabellosen Kopfhörer (siehe Abbildung 3.4) dem Prüfling einsagen. Der winzige Kopfhörer empfängt den Ton eines Mobiltelefons mit mit Hilfe einer Induktionsschleife.

Gegenmaßnahmen: 3.11.1, 3.11.2, 3.11.3, 3.11.4, 3.11.6, 3.11.7, 3.11.11

Abbildung 3.3: Brill mit integrierter HD Kamera. (vgl. [Spy16])

3.10.4 Double

Eine weiteres Szenario wäre der Einsatz eines Doubles, d.h. einer anderen Person, die die Prüfung statt des tatsächlichen Prüflings ablegt. Wer einen Zwilling hat oder zumindest eine Person, die einem ähnlich sieht, kann diese zur Prüfung schicken, anstatt selber hinzugehen. Das Double legt dann die Prüfung unerlaubterweise ab. Wichtig für den Erfolg der Täuschung ist, dass das „Double“ den Lichtbildabgleich besteht und idealerweise eine bessere Note erzielt als der echte Prüfling.

Gegenmaßnahmen: 3.11.8, 3.11.11

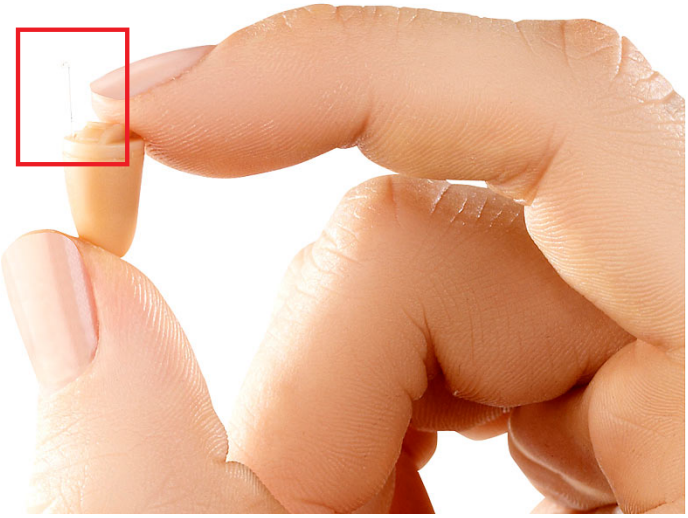


Abbildung 3.4: Kopfhörer mit Induktionsschleife (vgl. [Rup16])

3.10.5 Unerlaubte Informationsbeschaffung

Die unerlaubte Informationsbeschaffung, stellt einen Vorteil für den Prüfling gegenüber den anderen Teilnehmern dar. Dabei nutzt der Prüfling illegalerweise Hilfsmittel wie ein Buch, Heft oder einen Spickzettel für die Beantwortung der Fragen, um seine Wissenslücken auszugleichen. Er kann aber auch den Browser auf seinem Smartphone oder dem PC nutzten, um nach Lösungen bzw. Hilfe im Internet zu suchen. Neuere Technologien wie eine Datenbrillen, bswp. die Google Glass, die in das Bickfeld des Prüfling Informationen projiziert oder Smartwatches (siehe Abbildung 3.5), die Informationen in die Uhrzeit kodieren (vgl. [MDRH14]) können dem Prüfling das Spicken erleichtern.

Gegenmaßnahmen: 3.11.6, 3.11.7, 3.11.6, 3.11.10, 3.11.6, 3.11.11

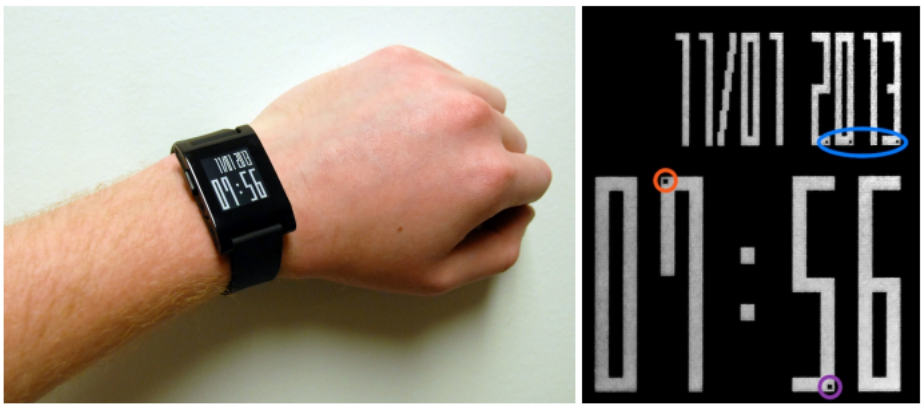


Abbildung 3.5: Smartwatch mit kodierten Pixel (vgl. [Sob16])

3.11 Anti-Täuschungsmaßnahmen

Im Folgenden werden Anti-Täuschungsmaßnahmen formuliert, um den Bedrohung aus den Täuschungsszenarien von Kapitel 3.10 entgegenzuwirken. Aus einigen Maßnahmen ergeben sich funktionale Anforderungen an das SSAOP, die in die Konzeption einfließen (vgl. [CJER11]).

3.11.1 Synchrone Prüfungsabnahme

Diese Maßnahme soll die Zusammenarbeit zwischen den Prüflingen und die Weitergabe von Prüfungsfragen erschweren, indem ein möglichst synchroner Prüfungsbeginn angestrebt wird. Das bedeutet, dass alle Prüflinge die Prüfung zu einer festgesetzten Zeit bzw. innerhalb eines definierten Zeitfensters (z.B. 15 Minuten) antreten müssen. So soll unterbunden werden, dass Prüfungsteilnehmer nacheinander die Prüfung ablegen und so Informationsfluss von Prüflingen, die die Prüfung bereits abgelegt haben, an künftige Prüflinge stattfindet. Ein Beispiel wäre ein Prüfling der eine Prüfung ein paar Stunden vor seinem Kommilitonen schreibt, um ihm nach der Prüfung mit den Prüfungsfragen oder zumindest mit dem Prüfungsstoff zu versorgen, so dass er sich besser auf die Prüfung vorbereiten kann. Der Nachteil dieser Maßnahme ist der Verlust der zeitlichen Flexibilität. Vor allem wenn sich die Prüflinge in unterschiedlichen Zeitzonen befinden, kann es zur Benachteiligung mancher Teilnehmer kommen, da ein Prüfung am Morgen in Deutschland zu einer Mitternachtsprüfung in den USA werden kann.

Funktionale Anforderungen aus den Anti-Täuschungsmaßnahmen:

Funktionale Anforderung 66: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten einen synchronen Prüfungsbeginn durchführen zu können.

Funktionale Anforderung 67: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten ein Zeitfenster für den Prüfungsbeginn einstellen zu können.

3.11.2 Veränderung der Fragen- und Antwortreihenfolge

Um die Weitergabe von Lösungen zu erschweren sollte die Reihenfolge der Prüfungsfragen und die Antworten (bei Multiple Choice Prüfungen) für jeden Prüfling zufällig generiert werden. Mit dieser Maßnahme reicht es zusammenarbeitende Prüflingen nicht mehr nur die Frage- und Antwortnummer auszutauschen. Sie müssen nun auch den Inhalt der Fragen und Antworten mitliefern, damit sie das Kreuz an die richtige Stelle setzen bzw. den Text zur richtigen Frage einfügen.

Funktionale Anforderungen aus den Anti-Täuschungsmaßnahmen:

Funktionale Anforderung 68: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten die Reihenfolge der Fragen zu verändern.

Funktionale Anforderung 69: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten die Reihenfolge der Antwortmöglichkeiten verändern zu können.

3.11.3 Kein Zurückspringen zu bereits beantworteten Fragen

Ein Prüfling sollte nur eine Frage gleichzeitig anzeigen und bearbeiten können. Sobald er ein Lösungsvorschlag abgibt, wird er zur nächsten Frage weitergeleitet. Ein Zurückgehen zu einer bereits beantworteten Frage sollte unterbunden werden. Daher müssen die Prüfungsfragen so entwickelt werden, dass man für die Bearbeitung der Prüfung nicht zu bereits bearbeiteten Fragen zurückspringen muss. Durch diese Maßnahme, muss dem täuschenden Prüfling genau zum richtigen Zeit die Antwort übermittelt werden, damit er sie eintragen kann. Kommt die Hilfe zu spät, kann er sie nicht in Anspruch nehmen.

Funktionale Anforderungen aus den Anti-Täuschungsmaßnahmen:

Funktionale Anforderung 70: Das SSAOP darf dem Prüfling nur eine Frage gleichzeitig anzeigen.

Funktionale Anforderung 71: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten das Zurückspringen zu bereits bearbeiteten Fragen zu deaktivieren.

3.11.4 Verknappung der Prüfungsdauer

Die Dauer für die Bearbeitung der Prüfung muss so gewählt werden, dass sie ausreichend ist, jedoch keine bzw. kaum Zeit für Täuschungsversuche zulässt. Durch die Verknappung der Zeit, soll der Prüfling gezwungen werden, sich auf die Beantwortung der Fragen zu konzentrieren und auf Täuschungsversuchen zu verzichten.

Funktionale Anforderung aus den Anti-Täuschungsmaßnahmen:

Funktionale Anforderung 72: Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten die Dauer für die Prüfung einstellen zu können.

3.11.5 Einmaliger Prüfungsantritt

Prüflinge können die Prüfung nur einmal öffnen und abgeben. Das bedeutet dass er die Prüfung nur einmal vom Server abrufen kann und nach der Abgabe keinen zweiten Versuch startet kann. Dies soll verhindern, dass bereits abgegebene Prüfungen mit neuem Wissen erneut bearbeitet werden. Eine Wiederholung der Prüfung bedarf einer Freigabe durch den Prüfungssteller.

Funktionale Anforderungen aus den Anti-Täuschungsmaßnahmen:

Funktionale Anforderung 73:
Das SSAOP darf dem Prüfling nur einen Prüfungsversuch gewähren, falls vom Prüfungssteller nicht anders konfiguriert.

Funktionale Anforderung 74:
Das SSAOP muss dem Prüfungsersteller die Möglichkeit bieten einzelnen Prüflingen ein erneuten Prüfungsversuch freizugeben.

3.11.6 Kontrollierte Prüfungsumgebung

Während der Prüfungsbearbeitung darf der Prüfling nicht auf andere Programme auf seinem Computer zugreifen, außer diese sind für die Bearbeitung erlaubt (z.B. Taschenrechner Applikation). Mit dieser Maßnahme soll unterbunden werden, dass Prüflinge neben der Prüfung ein anderes Programm öffnen können, wie z.B. einen Browser, um eine Täuschung zu begehen.

Funktionale Anforderung aus den Anti-Täuschungsmaßnahmen:

Funktionale Anforderung 75: Das SSAOP darf dem Prüfling nur Zugang zu explizit erlaubten Programmen außerhalb des SSAOP gewähren. Das Öffnen anderer Programme muss das SSAOP unterbinden.

3.11.7 Protokollierung der Prüflingsaktivitäten

Die Aktivität des Prüflings sollten protokolliert werden, um bei Täuschungsvorfällen das Protokoll als Beweismittel heranzuziehen.

Funktionale Anforderung aus den Anti-Täuschungsmaßnahmen:

Funktionale Anforderung 76: Das SSAOP muss alle Aktionen des Prüflings, soweit möglich, mitprotokollieren.

3.11.8 Überwachung der Authentizität des Prüflings

Die Überwachung der Authentizität ist bei der Prüfung einer der wichtigsten Aspekte. Um auszuschließen, dass der Prüfling die Prüfung durch einen Dritten ablegen lässt, muss sichergestellt werden, dass der Prüfling sich fortwährend vor dem Bildschirm befindet. Daher ist eine kontinuierliche Authentifizierung des Prüflings zwingend notwendig.

Funktionale Anforderung aus den Anti-Täuschungsmaßnahmen:

Funktionale Anforderung 77: Das SSAOP muss die Authentizität des Prüflings kontinuierlich überwachen.

3.11.9 Variation der Prüfungsfragen

Die Fragen einer Prüfung sollten regelmäßig veränderten werden. Wenn beispielsweise ein Drittel aller Prüfungsfragen nach der Prüfungsabnahme durch neue ersetzt werden, so hat man nach drei Prüfungsterminen eine komplett neue Prüfung. Eine Weitergabe von alten Prüfungsfragen hilft künftigen Prüflingen nur bedingt.

Funktionale Anforderung aus den Anti-Täuschungsmaßnahmen:

Funktionale Anforderung 78: Das SSAOP muss die Variation von Fragen ermöglichen.

3.11.10 Aufgeräumter Prüfungsort

Der Ort, an dem der Prüfling die Prüfung ablegt, sollte frei von unerlaubten Hilfsmitteln, aber auch Sachen, die nicht für die Bearbeitung der Prüfung notwendig sind, sein. Das bedeutet, dass nur das nötigste, wie Computermaus, Tastatur und Monitor auf dem Schreibtisch liegen sollten. Auch Uhren und andere technischen Geräte sollten für die Dauer der Prüfungsabnahme nicht an den Prüfungsort mitgenommen werden.

Der Prüfling sollte auch dafür sorgen, dass am Prüfungsort ausreichend Licht vorhanden ist, so dass, falls eine Webcam zur Überwachung eingesetzt wird, die Qualität des Bilds nicht unter der schlechten Beleuchtung leidet. Auch sollte darauf geachtet werden, dass hinter dem Prüfling eine helle Wand vorhanden ist. Dadurch sollen Missverständnisse aufgrund von auffälligen Gegenständen in der Nähe des Prüflings vermieden werden.

3.11.11 Disziplinarmaßnahmen beim Täuschungsversuch

Wird ein Prüfling bei einem Täuschungsversuch erwischt so sollten disziplinarische Maßnahmen folgen. Diese sollten so gewählt werden, dass sie vor Täuschungsversuchen abschrecken, wie beispielsweise die Aberkennung der Leistungen, der Ausschluss aus der Veranstaltung oder die Exmatrikulation bei mehreren Täuschungsversuchen. Den Prüflingen sollte aufgrund der Disziplinarmaßnahmen klar sein, dass es sich nicht lohnt zu täuschen, da die Auswirkung einer solchen Tat dramatisch wären. Dazu bedarf es einer guten Kommunikation der Regelung zur Handhabung von Täuschungsversuchen. Da die meisten Prüflinge selten die Prüfungsordnung lesen, sollten die wesentlichen Punkte der Regelung dem Prüfling vor Beginn der Prüfung angezeigt werden und das Einverständnis seitens des Prüflings eingefordert werden. So werden die Prüflinge vor der Online Prüfung erneut sensibilisiert.

4 Evaluation der Anforderungen

Für die Evaluation der Anforderungen wurden Universitätsdozenten, Studenten, Schulungstrainer und IT Sicherheitsexperten befragt. Insgesamt haben 17 Personen an der Umfrage teilgenommen und 17 Fragen beantwortet.

4.1 Expertenumfrage

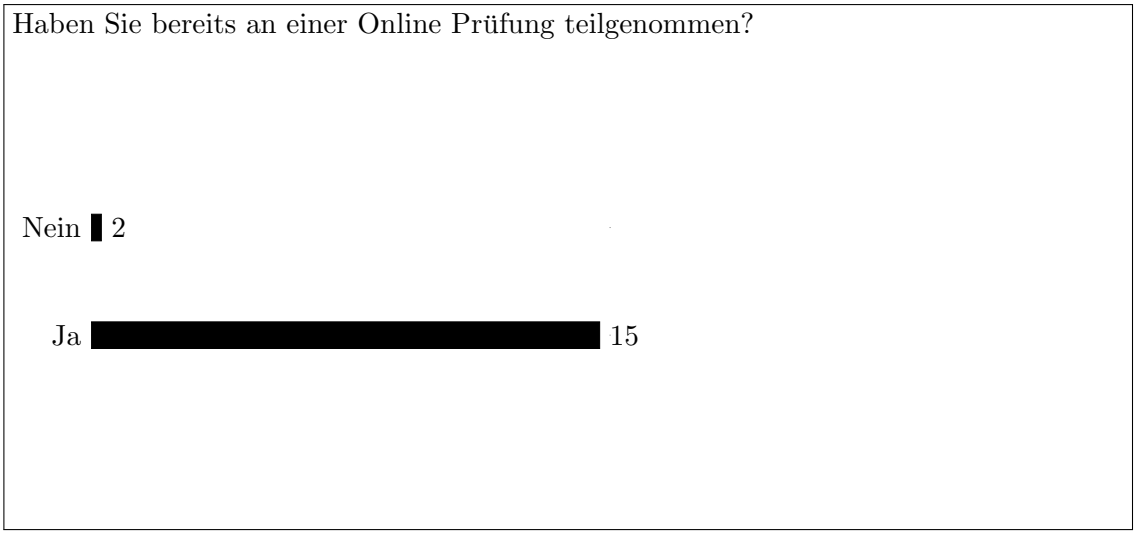
4.1.1 Resümee

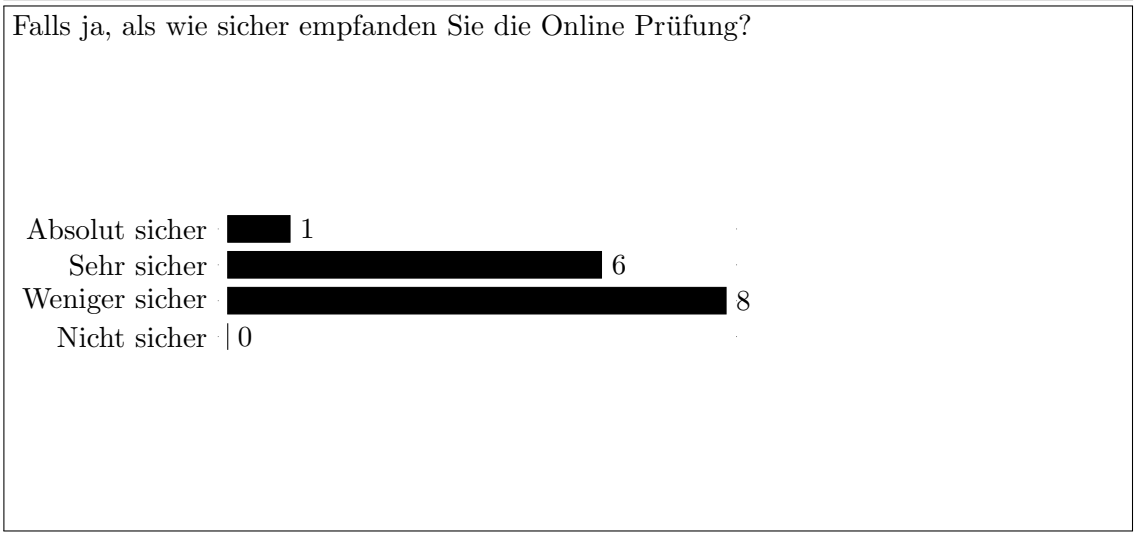
Die große Mehrheit der Befragten haben bereits an einer Online Prüfung teilgenommen. Knapp die Hälfte dieser Personen empfand die Prüfung als „Absolut sicher“ oder „Sehr sicher“. Jedoch denken zehn der 17 Teilnehmer, dass eine Präsenzprüfung sicherer ist als eine Online Prüfung und 15 Personen finden, dass eine Online Prüfung gegen Täuschungsversuche geschützt werden muss.

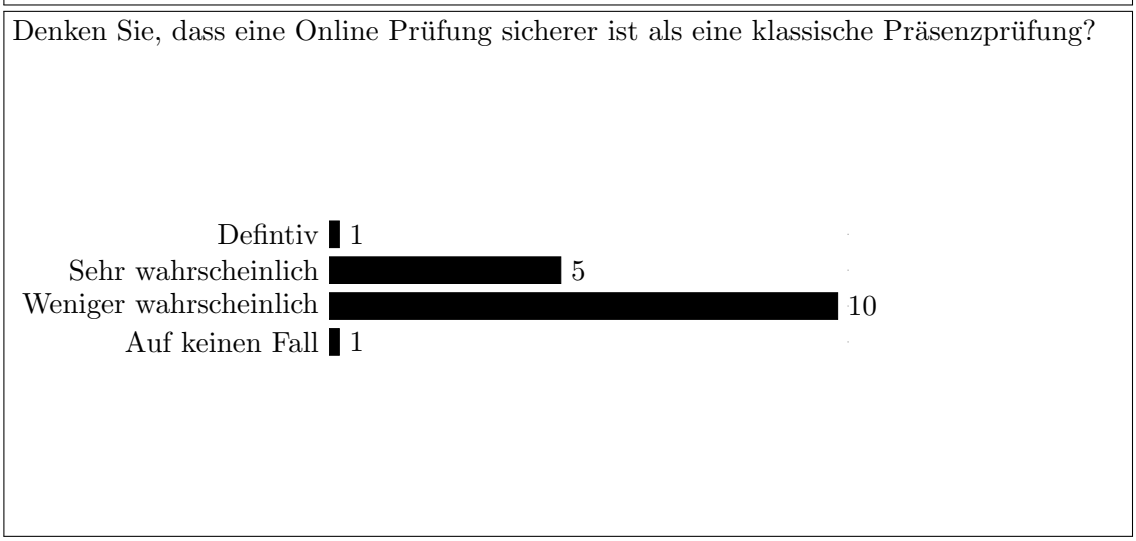
Über die Hälfte der Teilnehmer denkt, dass eine knapp bemessene Bearbeitungszeit und der damit entstehende Zeitdruck „definitiv“ bzw. „sehr wahrscheinlich“ zur Sicherheit einer Online Prüfung beitragen kann. Die gleiche Anzahl der Leute denkt jedoch, dass eine Randomisierung der Fragen- oder Antwortenreihenfolge „weniger wahrscheinlich“ bzw. „auf keinen Fall“ zur Sicherheit einer Online Prüfung beiträgt. 13 der Befragten finden eine Webcam zur Überwachung des Prüfling und dem dadurch entstehenden Gefühls der dauerhaften Beobachtung als „definitiv“ bzw. „sehr wahrscheinlich“ sicher. Auch die Gesichtserkennung trägt für elf der Teilnehmer zu Sicherheit der Online Prüfung bei. Das Tippverhalten sehen wiederum elf Personen als „weniger wahrscheinlich“ bzw. auf keinen Fall sicherheitsfördernd. Die meisten Experten würden trotz der Überwachung an einer Online Prüfung teilnehmen.

Das Fazit aus der Umfrage ist, dass es unter den Befragten zwei nahezu gleichgroße Parteien für und wider Online Prüfungen gibt. Die eine Partei denkt, dass der Schutz einer Online Prüfung mit organisatorischen Sicherheitsmaßnahmen erhöht werden kann. Die andere Gruppe ist davon nicht überzeugt. Lediglich beim Einsatz von einer Webcam zur kontinuierlichen Überwachung des Prüflings ist sich die große Mehrheit einig, dass die Maßnahme die Sicherheit einer Online Prüfung erhöht. Das Tippverhalten sehen die meisten Teilnehmer als weniger sicher. Im Folgenden werden die Ergebnisse der Umfrage dargestellt.

4.1.2 Ergebnisse der Umfrage







Denken Sie, dass eine Online Prüfung vor Täuschungsversuchen geschützt werden muss? Bitte begründen Sie Ihre Antwort, falls Sie mit Neinäntworten.

Begründungen:

„es muss verhindert werden , dass eine andere Person die Prüfung für einen anderen ablegt.“

„Da sie ohne Supervisor erfolgt“

Denken Sie, dass eine knapp bemessene Bearbeitungszeit und der damit entstehende Zeitdruck zur Sicherheit einer Online Prüfung beitragen?

Denken Sie, dass eine Randomisierung der Fragenreihenfolge zur Sicherheit einer Online Prüfung beiträgt?

Denken Sie, dass eine Randomisierung der Anwortenreihenfolge zur Sicherheit einer Online Prüfung beiträgt?

Denken Sie, dass die Androhung von harten Disziplinarmaßnahmen bei Täuschung die Anzahl von Täuschungsversuchen reduziert?

Welche weiteren organisatorische Maßnahmen können zur Sicherheit einer Online Prüfung beitragen?

Antworten:

„mir fallen keine weiteren ein“

„Prüfungsaufsicht bei den Teilnehmern, die beobachtet was die Teilnehmer machen.“

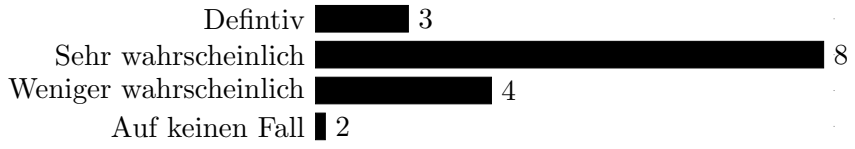
„keine Idee“

„häufige Neuentwicklung der Fragen“

„Online Prüfungen, die nur Wissen in Multiple-Choice abfragen, sind mit remote Prüfungen sind nicht sicher zu bekommen - es gibt immer die Möglichkeit, dass jemand anders die Prüfung macht oder den Prüfling unterstützt (auch bei Überwachung durch Webcam).“

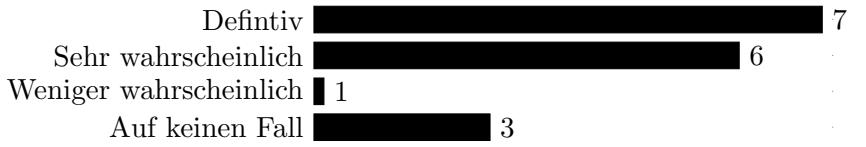
Denken Sie, dass eine kontinuierliche Überwachung des Prüflings z.B. per Webcam (aufgrund des Gefühls der dauerhaften Beobachtung) zur Sicherheit einer Online Prüfung beiträgt?

Denken Sie, dass eine kontinuierliche Authentifizierung des Prüflings mit Hilfe von Gesichtserkennung zur Sicherheit einer Online Prüfung beiträgt?



Denken Sie, dass eine kontinuierliche Authentifizierung des Prüflings mit Hilfe des Tippverhaltens zur Sicherheit einer Online Prüfung beiträgt?

Denken Sie, dass Sie an einer Online Prüfung teilnehmen würden, die per Webcam überwacht wird?



Denken Sie, dass Sie an einer Online Prüfung teilnehmen würden, die das Tippverhalten überwacht?

Welche technische Maßnahmen können zur Sicherheit einer Online Prüfung beitragen?

Antworten:

„mehrere Kameras, z.B. eine die die ganze Zeit den Prüfling sieht und eine die den gesamten Raum überwacht“

„Secure Browser die unterbinden das Teilnehmer die Seite wechseln oder andere Programme aufrufen kann.“

„keine Idee“

„einbau von challenges (Herausforderungen) die im nachinein überprüft werden können und nur von der richtigenPerson richtig beantwortet werden können - gegen Täuschungsversuch ander Person schreibt Prüfung“

„ich bin skeptisch, ob das überhaupt über technische Maßnahmen gelöst werden kann.“

Welche Vorteile sehen Sie bei einer Online Prüfung gegenüber einer Präsenzprüfung?

Antworten:

„spontan von jedem Ort durchführbar, skalierbar“

„Einfacher organisatorischer Aufwand. Kostenersparnis für Teilnehmer und auch für den Prüfer. Auch Teilnehmer die vom Prüfer weit entfernt sind, können die Prüfung schreiben.“

„- Keine „Überwachungspersonal“ notwendig

- Zeitliche Unabhängigkeit

- Man kann sich „lockerer“ fühlen, da keine „Schüler-Lehrer“ - Konstellation während der Prüfung“

„kann überall und jederzeit geschrieben werden

Kosten pro TN geringer als bei Präsenzeinzelprüfungen

leichtere Möglichkeit der Permutation von Fragen und Antworten (individualisierung der Prüfung)

meist sofortiges Ergebnis (bei Multiple Choide Tests)“

„keine Vorteile“

Welche Nachteile sehen Sie bei einer Online Prüfung gegenüber einer Präsenzprüfung?

Antworten:

„gesteigerte Kreativität für Täuschungsversuche, Schwierigkeit qualifiziertes Personal für die Überwachung zu finden“

„Prüfungen mit viel Text (bsp. Freitext Fragen) sind für viele Teilnehmer Online unangenehmer zu bewältigen als auf Papier. Daher liegt bei den meisten Online Prüfung der Schwerpunkt auf MC.“

„- Moralische Unterstützung durch Prüfungsleiter fehlt.

- Abhängigkeit zur Technik, bei einer unter Umständen für die Person sehr wichtigen (z.B. berufswegweisend) Prüfungen –¿ unbeeinflussbare Einflussgröße“ „mehr Überwachung

die vertraulichkeit der Fragen ist schwerer Sciherzustellen“

„Täuschungsmöglichkeiten“

5 Konzeption und beispielhafte Implementierung

Dieses Kapitel widmet sich der Erstellung eines Konzepts für das SSAOP. Es beschreibt die grundlegende Systemarchitektur, die einzelnen Systemkomponenten und deren Abhängigkeiten. Die Umsetzung des SSAOPs wird im nächsten Kapitel beschrieben.

5.1 Architektur

Das SSAOP unterliegt einer klassischen Client-Server-Architektur (s. Abb. 5.1). Dies entspricht einer Netzwerkarchitektur, in der der Server die meisten Ressourcen und Dienste hostet, bereitstellt und verwaltet, die vom Client konsumiert werden. Bei dieser Art von Architektur sind ein oder mehrere Client-Computer über ein Netzwerk oder eine Internetverbindung mit einem zentralen Server verbunden. Auf dem Client-Computer befindet sich die Nutzerschnittstelle zum Prüfungsverwaltungssystem (im Folgenden Exam Management System genannt), worüber bspw. Prüflinge die Teilnahme an der Prüfung realisieren oder Fragenersteller Prüfungsfragen einstellen können sowie Überwachungsmodule, die das Verhalten oder das Gesicht des Prüflings aufnehmen und an den Server schicken. Die Module schicken Informationen, wie z.B. Bilder vom Gesicht des Prüflings, an den Proctor Server, wo die Daten ausgewertet und zum Report zusammengefasst werden. Auf der Serverseite befindet sich die Schnittstelle und die Logik zur Verarbeitung der gesendeten Daten der Überwachungsmodule und die Logik des Exam Management Systems.

5.2 Exam Management System

Das Exam Management System (EMS) ist ein online-basiertes System, das den unterschiedlichen Rollen bestimmte Funktionen zu Verfügung stellt. So bietet es dem Prüfungsersteller die Möglichkeit eine Prüfung zu verwalten. Der Prüfungsplaner kann über das EMS Prüfungstermine planen, indem er Datum, Teilnehmer und Prüfungsbewerter bestimmt. Außerdem kann er Nutzern Identitäten bzw. Zugänge zuteilen und sie mit Rechten wie Teilnahmeberechtigungen ausstatten. Dem Prüfling ist es möglich über das EMS an einer Prüfung teilzunehmen und Ergebnisberichte einzusehen. Im EMS werden die meisten der in dieser Arbeit identifizierten Anforderungen umgesetzt. Im Folgenden werden ein paar Kernelemente des EMS knapp erläutert.

5.2.1 Identity- und Access-Management

Die Identitäts- und Zugangsverwaltung ermöglicht es, Nutzern eine eindeutige Identität, einen Schlüssel und andere Informationen zuzuweisen und ihnen so einen gesicherten Zugang zum System zu Verfügung zu stellen. Der Nutzer kann sich dann mit der zugewiesenen Identität und seinem Schlüssel am System anmelden. Jeder Identität können Rollen und/oder

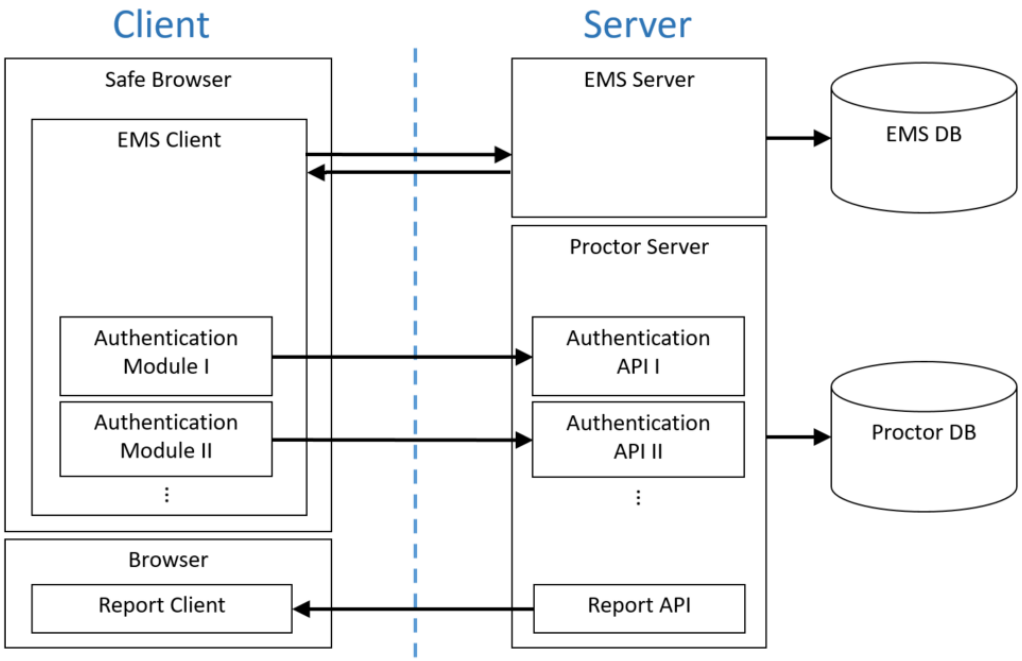


Abbildung 5.1: Server-Client-Architektur des SSAOP

Gruppen zugewiesen werden. In Abhängigkeit von der zugewiesenen Rolle bzw. Rollen erhält der Nutzer Rechte, um auf Funktionen, Dienste und Objekte des EMS zuzugreifen. Für den Fall, dass Identitäten aus einem bestehenden Identity- und Access management verwendet werden sollen, wird eine spezielle Schnittstelle für die Intergration angeboten.

5.2.2 Prüfungsverwaltung

In der Prüfungsverwaltung kann der Prüfungsersteller Prüfungsfragen inkl. Musterlösung erstellen und diese einer Prüfung zuteilen. Dabei kann er die Fragestellung nach seinen Anforderungen konfigurieren. So kann er bspw. einstellen, ob die Antwort der Frage als Freitext oder Auswahl erwartet wird. Des Weiteren kann er Prüfungsfragen bzw. Prüfungen bearbeiten oder stilllegen.

5.2.3 Terminierung

Das EMS erlaubt es einen Prüfungstermin zu erstellen. D.h. der Prüfungsplaner kann mit Hilfe des EMS für eine Prüfung Datum, Zeit, Teilnehmer und Prüfungsbewerter sowie ggf. einen Ort bestimmen. Der Prüfling kann sich dann für diesen Termin anmelden.

5.2.4 Prüfungsteilnahme

Ein Ziel des EMS ist es Prüflingen eine Interaktionsschnittstelle anzubieten, über der sie an einer Prüfung teilnehmen können. Ein Prüfling kann sich für die Teilnahme an einer Prüfung anmelden oder auch abmelden, vorausgesetzt er besitzt eine Berechtigung zur Teilnahme. Während der Prüfungsteilnahme kann der Prüfling über die Nutzeroberfläche die Fragen einer Prüfung bearbeiten. Ist er fertig oder ist die angesetzte Zeit abgelaufen, endet die

Prüfungsteilnahme und es ist dem Prüfling nicht mehr möglich weitere Änderungen an den Antworten vorzunehmen.

5.2.5 Prüfungsbewertung

Prüfungen können durch das System automatisiert bewertet werden. Jedoch bietet das EMS dem Prüfer auch die Möglichkeit eine manuelle Bewertung vorzunehmen.

5.2.6 Ergebnisbericht

Ein Ergebnisbericht teilt dem Prüfling mit, welches Ergebnis er bei der Prüfung erzielt hat. Hier sind zwei Szenarien denkbar. Erstens, dem Prüfling wird direkt nach der Prüfung das Ergebnis angezeigt. Dies erfordert jedoch, dass die Prüfung automatisiert ausgewertet werden kann. Oder der Prüfling bekommt das Ergebnis erst nach einer manuellen Korrektur. Dabei wird der Prüfling per benachrichtigt, sobald der Ergebnisbericht abholbereit ist.

5.3 Authentication Framework

Das Authentication Framework ist eine Struktur, die als Leitfaden oder Unterstützung für die Implementierung von Überwachungsmechanismen dient. Hiermit können beliebige Authentifizierungsfunktionalitäten integriert werden, um die Authentizität des Nutzers zu überwachen. Voraussetzung dafür ist eine verteilte Architektur. Eine Authentifizierungsfunktionalität besteht aus einem Clientmodul (Authentication Module), der in das EMS integriert wird und einem Servermodul (Authentication API) auf dem Proctor Server. Sie sammelt Informationen beim Prüfling und verschickt sie an den Server. Der Proctor Server wertet die Informationen aus und stellt sie in Form eines Berichts der Prüfungsaufsicht bereit. Der Bericht kann über den Browser abgerufen werden. In der Abbildung 5.2 sind die Komponenten des Authentication Frameworks dargestellt.

Die von den Authentication Modulen gesammelten Daten können unterschiedliche Formen haben. So sind das im Fall der Gesichtserkennung Bilder und beim Tippverhalten Zeiten und Tasteninformationen. Die Algorithmen in den entsprechenden Application Programming Interfaces (kurz: APIs) im Proctor Server berechnen aus den Daten einen Closeness Score, der aussagt, wie hoch der Algorithmus die Authentizität des Nutzers einschätzt. Der Closeness Score entspricht dem Grad der Übereinstimmung der aufgenommenen Daten mit den Referenzdaten.

Sowohl die Authentication Module als auch der Proctor Server mit den Authentication APIs sind Bestandteile des hier entwickelten Authentication Frameworks und können bei Bedarf um zusätzliche Funktionalitäten erweitert werden. Das bedeutet, dass neue Ideen zur Überwachung der Authentizität analog zu den in dieser Arbeit vorgestellten Modulen und APIs konzipiert und implementiert werden können. Im Folgenden werden die Funktionalitäten Gesichtserkennung und Tippverhalten beschrieben.

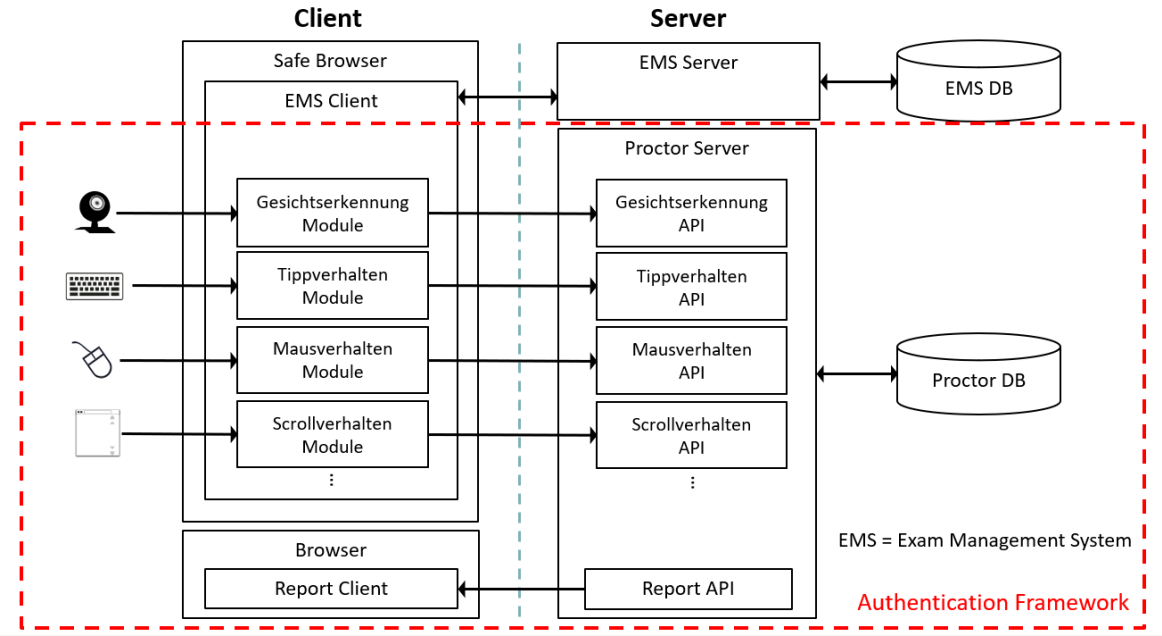


Abbildung 5.2: Die einzelnen Komponenten des Proctoring Systems und ihre Abhängigkeiten

5.3.1 Algorithmus für die Gesichtserkennung

Eine Möglichkeit um die kontinuierliche Authentizität zu gewährleisten ist das Gesicht des Prüflings während der ganzen Prüfung zu verfolgen und zu authentifizieren. Dafür muss das Gesicht des Prüflings für die Dauer der Prüfung aufgenommen werden. Um das zu realisieren benötigt man eine Kamera, die das Gesicht des Prüflings aufnimmt. In bestimmten Zeitabständen wird dann ein Bild vom Prüfling von dem im EMS integrierten Modul aufgenommen und an die API zur Verarbeitung weitergeschickt. // // Der Algorithmus für die Gesichtserkennung soll einerseits Gesichter auf einem Bild auslesen und andererseits beurteilen, wie sehr sich das Gesicht der Personen vor dem Rechner dem des angemeldeten Prüflings ähnelt. Dies bedeutet, dass zwei Schritte für die Gesichtserkennung nötig sind. Für den ersten Schritte, dem Auslesen von Gesichtern (englisch: Face Detection), wird ein ressourcenschonend und performanter Algorithmus benötigt, da sehr viele Bilder nacheinander verarbeitet werden müssen. Ein Algorithmus, der diese Kriterien erfüllt, ist der Viola-Jones Algorithmus *vgl.*[Jon01], der auf die Erkennung von Mustern setzt. Jedoch hat dieses Verfahren den Nachteil, dass das Gesicht frontal erfasst werden muss. Für das SSAOP stellt dies aber kein Problem dar, da das Gesicht des Prüflings während der Prüfung ohnehin frontal auf den Bildschirm gerichtet sein muss. Daher wird eine Abweichung bzw. ein Nichterkennen, wenn z.B. der Nutzer zur Seite oder auf den Boden schaut, als Hinweis auf einen Täuschungsversuch gewertet. Für das tatsächliche Wiedererkennen des Gesichts (englisch: Face Recongnition) wird das Local Binary Patterns (LBP) Verfahren angewandt. Auch dieser Algorithmus ist ressourcenschonend, so dass eine schnelle Verarbeitung gewährleistet werden kann.

1. Schritt: Face Detection

Das Verfahren der Face Detection basiert auf die Klassifikation von Bilder nach den Werten

der enthaltenen Features (Merkmalen). Die Nutzung von Features anstatt von Pixeln hat den Vorteil, dass es die Erkennung wesentlich performanter macht. Es werden die Werte von drei Features verwendet. Der Wert eines Zwei-Rechteck-Features ist die Differenz zwischen der Summe der Pixel innerhalb von zwei rechteckigen Bereichen. Die Bereiche haben die gleiche Größe und Form und sind entweder horizontal oder vertikal aneinandergereiht. Ein Drei-Rechteck-Feature berechnet die Summe innerhalb der zwei außenliegenden Rechtecke und subtrahiert davon die Summe des mittigen Rechtecks. Das dritte Merkmal ist das Vier-Rechteck-Feature und dessen Wert berechnet sich aus dem Unterschied zwischen den diagonalen Paaren von Rechtecken (s. Abb. 5.3).

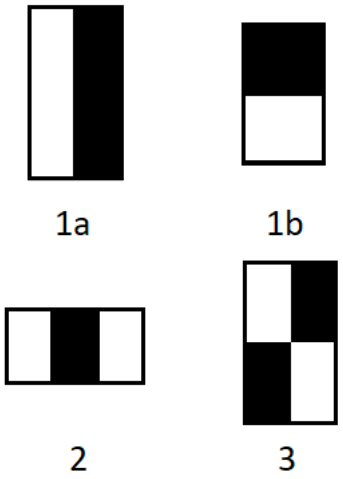


Abbildung 5.3: 1a und b sind Zwei-Rechteck-Features, 2 ist ein Drei-Rechteck-Feature und 3 ist ein Vier-Rechteck-Feature

Viereck-Features können sehr schnell mit Hilfe einer Hilfsdarstellung, einem sogenannten integralen Bild, berechnet werden. Das integrale Bild an der Stelle (x, y) umfasst die Pixel über und links von (x, y), wobei x auf der horizontalen und y auf der vertikalen Achse liegen.

$$ii(x, y) = \sum_{x' \leq x, y' \leq y} i(x', y'), \tag{5.1}$$

wobei *ii(x, y)* das integrale Bild und *i(x, y)* das originale Bild sind. Nutzt man folgende Rekursion:

$$s(x, y) = s(x, y - 1) + i(x, y) \tag{5.2}$$

$$ii(x, y) = ii(x - 1, y) = s(x, y) \tag{5.3}$$

wobei *s(x, y)* die kumulative Summe pro Zeile, *s(x, -1) = 0* und *ii(-1, y) = 0* sind, kann das integrale Bild in einem Zug berechnet werden.

Um eine höhere Sicherheit zu erlangen, ob sich auf dem Bild ein Gesicht befindet werden bei der Analyse mehrere Detektoren hintereinander ausgeführt (s. Abb. 5.4). Jeder Detektor

sucht nach einem bestimmten Merkmal wie z.B. der Augenbrauen-Partie oder Augen-Nasen-Partie. Bei einem menschlichen Gesicht sind bei der Augenbrauen-Partie oben die dunklen Augenbrauen und unten die helleren Augen. Bei der Augen-Nase-Partie entspricht es einem dunkel-hell-dunkel Feature, was dem ersten Auge, der Nase und dann dem zweiten Auge entspricht (s. Abb. 5.4).

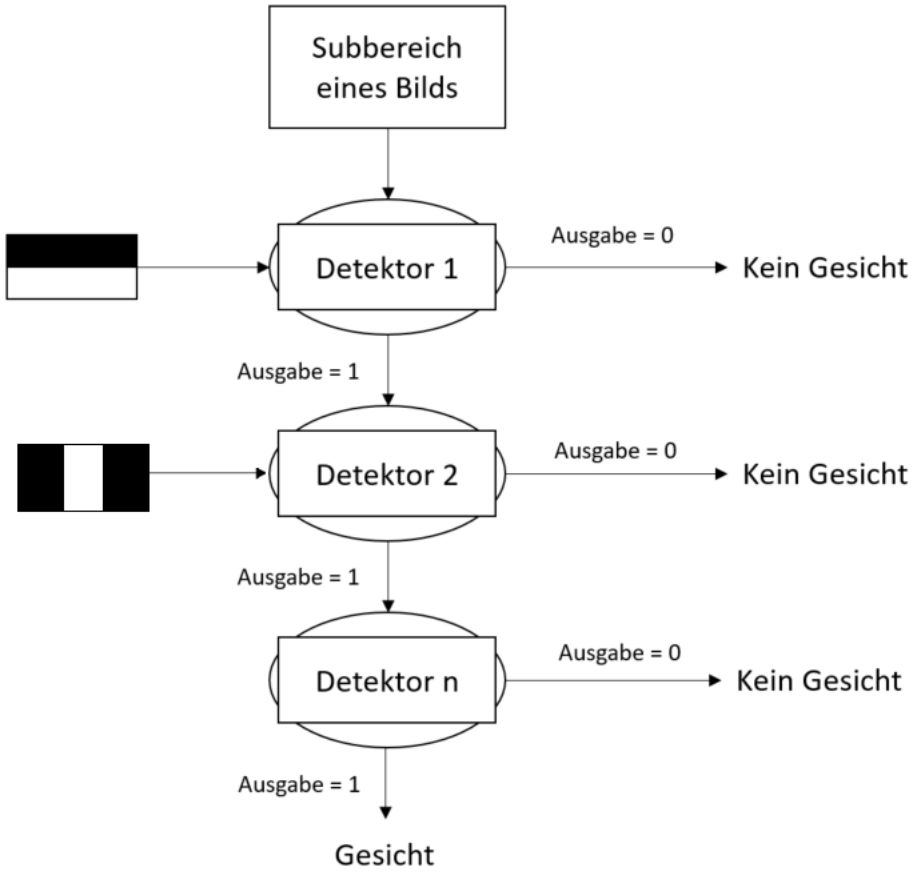


Abbildung 5.4: Auf dem Subbereich des Bildes werden nacheinander n unterschiedliche Detektoren angewendet. Erst falls alle Detektoren ein Feature finden, wurde ein Gesicht erfolgreich erkannt.

2. Schritt: Face Recognition

Um die Ähnlichkeit zwischen zwei Gesichtern zu berechnen wird der LBP Algorithmus genutzt. Es berechnet für ein Gesicht einen beschreibenden Wert und vergleicht diesen dann mit einem Referenzwert. Bevor das Bild verarbeitet werden kann muss es als erstes vorbereitet werden. Dazu wird das Gesicht aus dem ursprünglichen Bild ausgeschnitten und in eine Graustufendarstellung überführt. Dieser Schritt ist nötig, um den LBP Algorithmus anwenden zu können. Die Grundidee von LBP besteht darin, die lokale Struktur in einem Bild zusammenzufassen, indem jedes Pixel mit seiner Umgebung verglichen wird. Dabei wird ein Pixel als Mittelpunkt fixiert und von seinen Nachbarn abgegrenzt. Falls die Intensität

Abbildung 5.5: Vereinfachte Darstellung für die Erkennung der Augenpartie (links) und Nasenpartie (rechts) mit Hilfe eines Zwei-Rechteck-Features und Drei-Rechteck-Features

des zentralen Pixels kleiner ist als die seines Nachbarn, wird der Nachbar als 1, falls nicht als 0 markiert. Dazu werden die Nachbarn des zentralen Pixel im Uhrzeigersinn abgegangen (s. Abb. 5.6). Dadurch ergibt sich eine Binärzahl für jedes Pixel. Mit 8 umgebenden Pixeln gibt es also 2 hoch 8 mögliche Kombinationen für das lokale Binärmuster. Das Binärmuster für den Pixel in der Abb. 5.6 lautet 10010100. Alle lokalen Binärmuster für alle Pixel des Bildausschnitts zusammen ergeben den beschreibenden Wert für das Gesicht. Dieser Wert kann dann mit dem des Referenzgesichts verglichen werden. Das Ergebnis aus dem Vergleich ist die euklidische Distanz zwischen den beiden Werten.

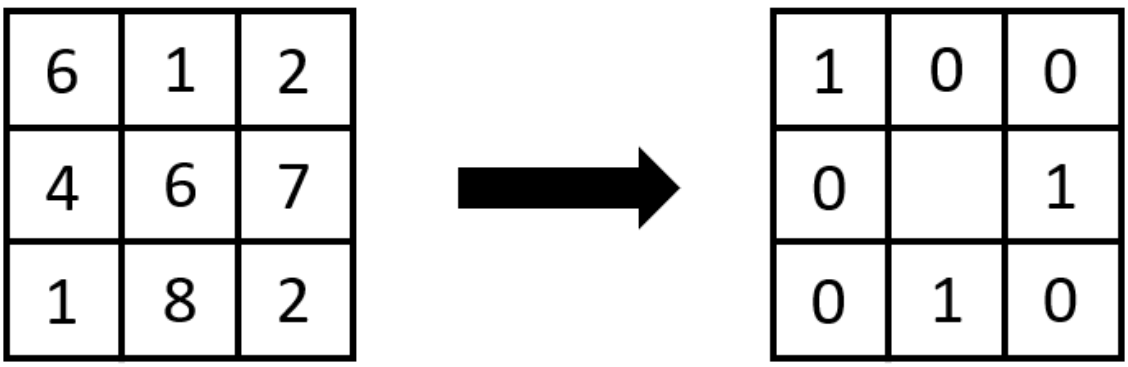


Abbildung 5.6: Die Abgrenzung des zentralen Pixel zu seinen Nachbarn. Das Binärmuster lautet 10010100.

Formell dargestell schaut der LBP Algorithmus wie folgt aus:

$$LBP(x_c, y_c) = \sum_{p=0}^{P-1} 2^P s(i_p - i_c), \tag{5.4}$$

mit x_c, y_c als zentralen Pixel und der Intensität i_c; und i_p als Intensität des Nachbarpixels. s ist eine Signumfunktion und wie folgt definiert:

$$s = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{else} \end{cases}$$

5.3.2 Algorithmus für das Tippverhalten

Auch das Tippverhalten des Nutzers auf der Tastatur kann verwendet werden, um ihn kontinuierlich zu authentifizieren *vgl.*[She95]. Die erste wissenschaftliche Arbeit zu diesem Thema wurde von *vgl.*[SGLPS80] 1980 veröffentlicht. Sie haben sich die Frage gestellt, ob Nutzer über die Art und Weise wie sie tippen identifiziert werden können. Dabei wurde sieben Versuchspersonen ein Text zum Abtippen gegeben, um das Tippmuster aufzuzeichnen. Nach vier Monaten wurde der Versuch wiederholt und man kam zu dem Ergebnis, dass die Personen eine „Tippsignatur“ besitzen und es somit möglich ist einzelne Menschen voneinander zu unterscheiden. *vgl.*[KAK10] haben im Jahr 2010 37 wissenschaftliche Arbeiten analysiert und daraus fünf Kategorie (Statistische Methoden, Neuronale Netze, Mustererkennung, Hybride Techniken und weitere Vorgehensweisen) zusammengefasst und sind zu dem Entschluss gekommen, dass die meisten Tippverhalten Konzepte auf Timing-Informationen der Tastenanschläge basieren.

Der Algorithmus der Tippverhalten API arbeitet mit dem Tipprhythmus der Prüflinge, um sie kontinuierlich bei jeder Tastatureingabe zu authentifizieren. Dabei werden die Verweilzeit auf einer Taste und die Latenzzeit zwischen zwei Tasten als Grundlage für die Generierung des Rhythmus genutzt (s. Abb. 5.7). Beim erstmaligen Eingeben eines Wortes wird der Tipprhythmus jedes einzelnen Nutzers aufgezeichnet und als Tippmuster persistiert. Bei späteren gleichen Tastatureingaben kann mit Hilfe des ursprünglich aufgezeichneten Musters verglichen werden, inwieweit sich die Tippmuster ähneln und somit, ob immer noch derselbe Nutzer an der Tastatur sitzt. Der dabei resultierende Wert wird Closeness-Score genannt und beschreibt den Grad der Übereinstimmung zwischen den beiden Tippmustern.

5.3.3 Reporting Client und API

Für die Visualisierung der mit Hilfe der Algorithmen gesammelten Ergebnisse ist das Reporting zuständig. Der Nutzer kann über den Report Client für jeden Nutzer jeweils die Beurteilungen der Authentizitätsprüfung für die Gesichtserkennung und das Tippverhalten einsehen. Die Werte der Gesichtserkennung werden in einem Plot Chart dargestellt. Die Y-Achse entspricht der euklidischen Distanz und die X-Achse der Zeit. Grüne Punkte markieren erfolgreich erkannte Gesichter, wobei rote Punkte eine nicht ausreichende Ähnlichkeit widerspiegeln. Werden gelbe Punkte angezeigt, so bedeutet das, dass sich mehr als ein Gesicht auf dem aufgenommenen Bild befand. Zusätzlich zum Chart kann jedes aufgenommene Bild des Prüfling zu einer bestimmten Zeit angeschaut werden. Auf dem Bild werden erkannte Gesichter eingerahmt und der Rahmen mit nach dem oben beschriebenen Prinzip

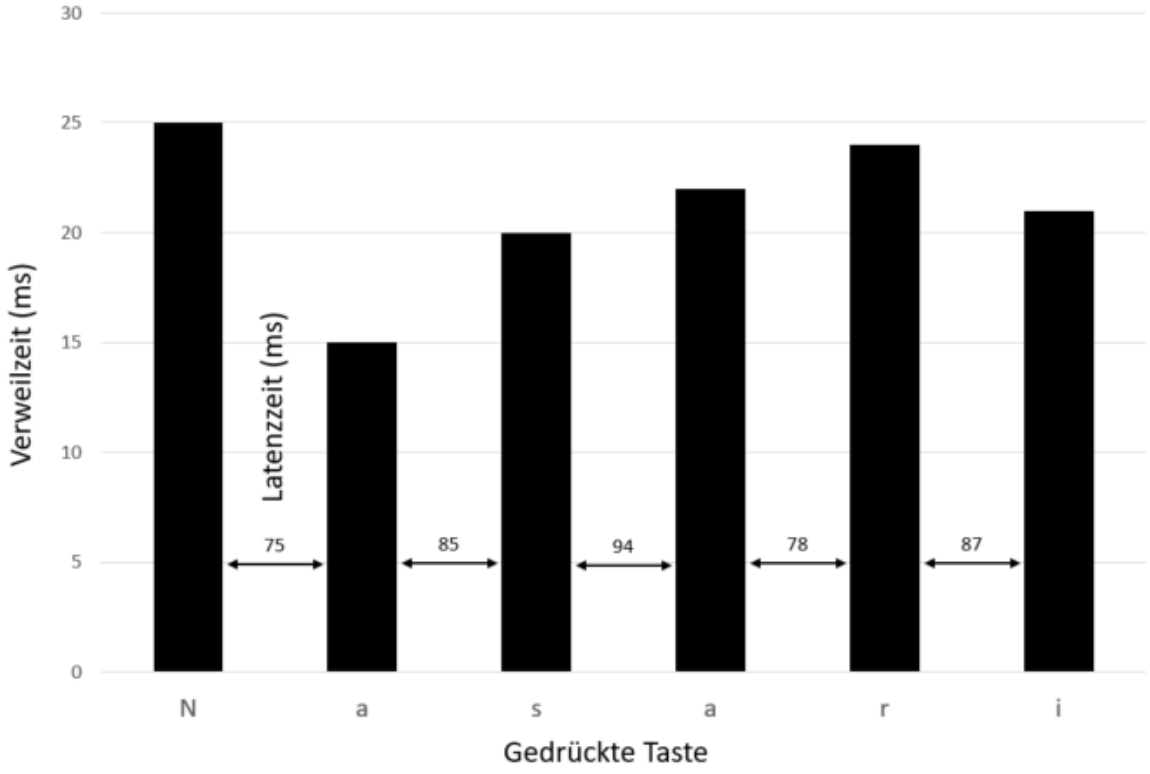


Abbildung 5.7: Tippmuster für das Wort „Nasari“

eingefärbt. Für das Tippverhalten wird jedes Wort, das der Prüfling eingibt und zu dem ein Refereneztippmuster in der Datennbank vorhanden ist, der Closeness-Score in Prozent angezeigt.

5.3.4 Serverseitige Datenbanken

Zum Ablegen der gesammelten Daten wird eine dokumentenorientierte NoSQL Datenbank eingesetzt. Dies bedeutet, dass die Daten im Gegensatz zu einer traditionellen Datenbank z.B. als JSON Objekte, hierarchisch in einer Collection abgelegt werden. Eine Collection entspricht einer Tabelle in einer relationalen Datenbank und verwaltet statt Zeilen Dokumente. Ein wesentliches Wesensmerkmal der NoSQL Datenbank besteht darin, dass die Dokumente einer Collection gänzlich unterschiedlich strukturiert sein können. Dies hat den Vorteil, dass die geladenen Objekte direkt und ohne vorheriger Transformation bzw. Object Mapping bspw. mit dem JavaScript Server verarbeitet werden können. Umgekehrt können Datenobjekte unbehandelt in die Datenbank geschrieben werden, ohne dass sie in ein vorgegebenes Schema umgeändert werden müssen. Dadurch können die vom Authentication Module gesammelte Daten ungeachtet des Formats eins zu eins persistiert und bei Bedarf auch wieder im selben Format ausgelesen werden. Die Logik für die Transaformation wird obsolet, wodurch die Performanz gesteigert werden kann (vgl. [GRGA15]).

5.3.4.1 Collections und Dokumente

Für das SSAOP wird eine Datenbank („ssaop“) und zwei Collections, jeweils eine für die Gesichtserkennung („facerecogntion“) und eine für das Tippverhalten („keystroke“), angelegt. In den Collections werden die von den Servermodulen verarbeitete Daten abgelegt, um sie bspw. für die Erstellung des Ergebnisberichts zu nutzen.

Für die Servermodule generierten Daten werden JSON Objekte mit folgenden Mindesteigenschaften als Datenträger genutzt:

- Zeitstempel
- Nutzer-ID
- Prüfungs-ID
- Ergebns

Das Ergebnis ist der Wert, der als Resultat der Einschätzung vom jeweiligen Algorithmus berechnet wird. Im Falle der Gesichtserkennung ist das die euklidische Distanz zum trainierten Modell und beim Tippverhalten ist es die Übereinstimmung mit dem zuvor trainierten Wort, dem Closeness-Score.

5.4 Safe Browser

Für die Durchführung einer Online Prüfung stellt der Einsatz eines klassischen Browsers, wie Internet Explorer, Google Chrome oder Firefox, ein Sicherheitsrisiko dar, da dem Prüfling Funktionen zu Verfügung gestellt werden, die ihm Täuschungen ermöglichen könnten. Aus diesem Grund muss für die Prüfungsteilnahme ein sicherer Browser verwendet werden. Der sichere Browser ist ein Programm, das dem Prüfling die als HTML übermittelte Prüfung darstellt, jedoch weitere Funktionen, die nicht zur Bearbeitung der Prüfung erforderlich sind, deaktiviert. So unterbindet er bspw. das Aufrufen von externen Programmen oder das Speichern, Betrachten und Editieren von Quelltexten. Dadurch wird der Zugriff auf die Prüfung abgesichert und das Risiko für Täuschung reduziert.

Der Safe Browser kann den Aufruf des Taskmanagers (Tastenkürzel: Strg+Alt+Ent), das Ausloggen vom Betriebssystem, das Wechseln des Betriebssystemnutzers, das Herunterfahren, das Aufrufen des Start Menüs, das Wechseln zu anderen Programmen, Copy & Paste sowie Drucken deaktivieren. Der Prüfungsersteller muss entscheiden, welche Funktionen nicht erlaubt sein sollen und dementsprechend den Safe Browser konfigurieren. Wenn der Safe Browser beendet wird, kann die Prüfung nicht erneut angetreten werden, und gilt somit als abgegeben. Der Browser beendet sich, sobald die Prüfung abgegeben wurde, ohne dass der Prüfling dies machen muss.

Im Browser funktioniert der Aufruf des Kontextmenüs mit der rechten Maustaste bzw. einem Tastenkürzel nicht. Somit kann auch der Quelltext nicht betrachtet werden. Außerdem bemerkt der Safe Browser, wenn er in einer virtuellen Maschine statt der nativen Umgebung gestartet wird und blockiert daraufhin die Nutzung.

5.5 Sichere Anbindung

Die Kommunikation zwischen Client und Server erfolgt über das Internet und ist durch TLS geschützt. Transport Layer Security (TLS) ist ein Protokoll, das die Vertraulichkeit und Datenintegrität zwischen zwei kommunizierenden Anwendungen gewährleistet. Es ist das am weitesten verbreitete Sicherheitsprotokoll für den Datenaustausch über ein Netzwerk.

6 Beispielhafte Implementierung

In diesem Kapitel geht es um die beispielhafte Implementierung des SSAOP. Die Umsetzung beinhaltet die Auswahl des Betriebssystems, die Konfiguration des EMS und Safe Browsers sowie die Implementierung der Algorithmen zur kontinuierlichen Authentifizierung und des Reporting (s. Abb. 6.1). Dabei wird auch die Implementierung des Authentification Frameworks dargestellt.

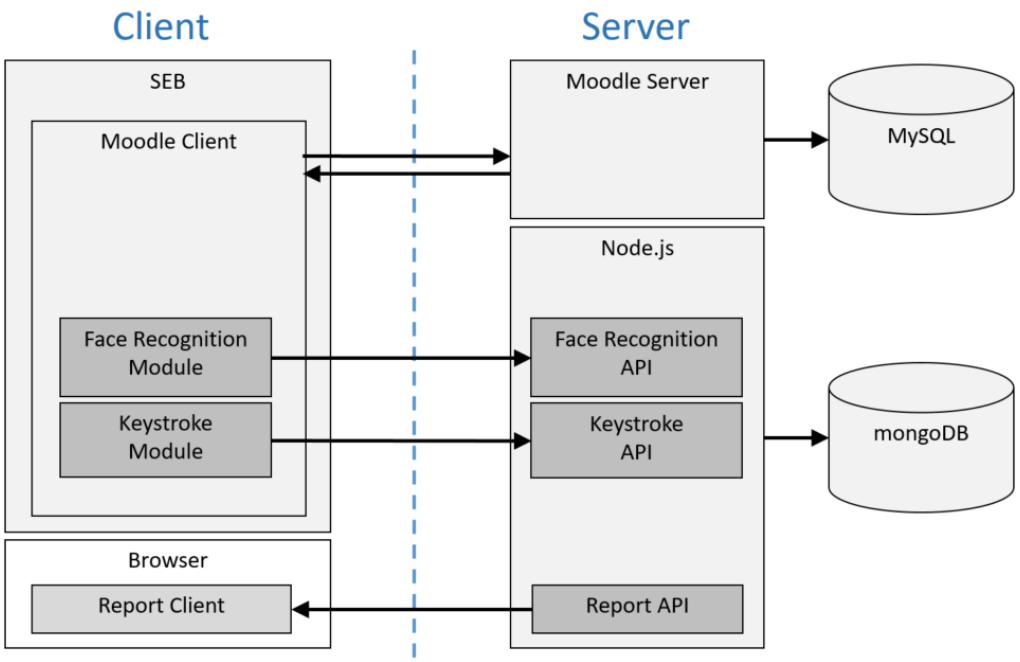


Abbildung 6.1: Implementierung des SSAOP. Hellgraue Kästchen: Konfiguration; Dunkelgraue Kästchen: Implementierung

6.1 Server Betriebssystem

Auf dem Server ist als Betriebssystem die Linux Distribution Debian 8.7 Jessie installiert. Für die Implementierung kann jedoch auch ein Windows oder MacOS Betriebssystem verwendet werden. Die Installation der Komponenten muss für diese Systeme entsprechend angepasst werden.

6.2 Implementierung des EMS

Auf dem Markt gibt es sogenannte Learning Management Systeme (LMS), die die Funktionalitäten eines EMS anbieten. Im Folgenden wurden Learning Management Systeme betrachtet, die entweder eine freie Demoversion für Testzwecke anbieten oder Open-Source sind, um herauszufinden, welches System, die meisten zuvor genannten Anforderungen an das EMS erfüllt. Verglichen wurden die Produkte Moodle, Ilias, ATutor und Claroline.

Anforderung	**Moodle**	**Ilias**	**ATutor**	**Claroline**
Prüfungsverwaltung	✓	✓	✓	✓
Identitätsverwaltung	✓	✓	✓	✓
Zugangsverwaltung	✓	✓	✓	✓
Provisionierung	✓	✓	✓	✓
Prüfungsteilnahme	✓	✓	✓	✓
Ergebnisbericht	✓	✓	✓	✓
Terminierung	✓	✓	✓	✓
Synchrone Prüfungsabnahme (REQ-1, REQ-2)	✓	✓	✓	✓
Veränderung der Fragen- und Antwortreihenfolge (REQ-3, REQ-4)	✓	✓	✓	
Kein Zurückspringen zu bereits beantworteten Fragen (REQ-5, REQ-6)	✓	✓	✓	✓
Konfiguration der Prüfungsdauer (REQ-7)	✓	✓	✓	✓
Einmaliger Prüfungsantritt (REQ-8, REQ-9)	✓	✓	✓	✓
Kontrollierte Prüfungsumgebung (REQ-10)				
Protokollierung der Prüflingsaktivitäten (REQ-11)	✓	✓		
Überwachung der Authentizität Prüflings (REQ-12)				

Der Vergleich der LMS zeigt, dass Moodle das System mit den meisten übereinstimmenden Funktionalitäten ist. Daher wird für das SSAOP Moodle als EMS eingesetzt.

6.2.1 Installation von Moodle

Moodle wird auf einem Apache HTTP Server installiert. Der Apache HTTP Server ist die Software, auf der Moodle in der Skriptsprache PHP läuft. Auch andere Webserver wie z.B. Internet Information Services (IIS) unter Windows können hierfür eingesetzt werden, jedoch ist der Apache HTTP Server aufgrund seiner Interoperabilität auf allen Plattformen sehr beliebt (https://news.netcraft.com/archives/2017/02/27/february-2017-web-server-survey.html). Für den Prototypen wird die Linux Distribution Debian 8.7 als Betriebssystem verwendet.

Apache HTTP Server

Um den Apache HTTP Server zu installieren, wird der folgende Befehl ausgeführt:

```
1 sudo apt-get install apache2
```

Listing 6.1: Installation von Apache HTTP Server

Nachdem die Pakete heruntergeladen und installiert wurden, kann der Server unter „/var/www/“ gefunden werden.
TLS

Moodle bietet die Möglichkeit das Protokoll HTTPS für die gesamte Website anzuwenden. Daher muss der Server entsprechend konfiguriert werden. Hierfür muss der Parameter „wwwroot“ von „http://“ auf „https://“ geändert werden. Des Weiteren ist ein SSL Zertifikat nötig. Dafür gibt es zwei Optione - ein selbst signiertes Zertifikat oder ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle. Der Einsatz eines selbstsignierten Zertifikats ist nur für die Testphase geeignet, da der User ansonsten vor einem „nicht vertrauenswürdigen“ Zertifikat gewarnt würde. Der Erwerb eines Zertifikats von einer vertrauenswürdigen Zertifizierungsstelle ist sinnvoll, falls auf Moodle über das Internet zugegriffen werden soll. Um das Zertifikat dem Server bekannt zu machen, muss der folgende Eintrage in die Datei „default“ aufgenommen werden:

```
1 Listen 443
2 NameVirtualHost *:443
3 <VirtualHost *:443>
4     SSLEngine On
5     SSLCertificateFile /tls/certificate.crt
6     SSLCertificateKeyFile /tls/certificate.key
7 </VirtualHost>
```

Listing 6.2: TLS Konfiguration des Apache HTTP Servers

MySQL

Als nächstes muss ein Datenbankserver installiert werden, auf dem die Daten von Moodle persisitiert werden. Moodle empfiehlt die Datenbank MySQL. Mit folgendem Befehl wird MySQL auf dem Betriebssystem installiert:

```
1 sudo apt-get install mysql-server
```

Listing 6.3: Installation von MySQL

Nach der Installtion muss eine leere Datenbank mit dem namen „ssaop“ erstellt werden. Diese Datenbank wird später von Moodle genutzt.

Moodle

Um Moodle zu installieren, muss das Softwarepaket von der offiziellen Hersteller Seite (http://moodle.org/downloads) heruntergeladen und in einem Ordner „moodle“ entpackt werden. Die Dateien werden nun in das Webverzeichnis „/var/www/html/“ des Apache HTTP Servers verschoben. Moodle ist nun bereit für die Installation.

Moodle bietet eine Installation über eine grafische Oberfläche im Browser an. Der Installationsvorgang erstellt automatisiert alle benötigten Datenbanktabellen und fordert die Eingabe der Administratorkontodaten sowie Informationen über die Webseite. Am Ende des Installationsvorgangs ist Moodle einsatzbereit.

6.2.2 Anlegen der Nutzer

Zum Anlegen eines Nutzers wird das Administratorkonto genutzt. Als erstes wird ein Prüfungsersteller angelegt. Im Menü wird der Punkt „Einstellungen / Website-Administration / Nutzerkonten / Nutzerkonten / Nutzer/in neu anlegen“ ausgewählt. Nun werden Informationen zum Nutzer wie Name und Email eingegeben sowie dem Nutzer die Rolle „Trainer/in“ zugewiesen.

Der zweite Nutzer ist der Prüfling. Hier muss ebenfalls über den Menüpunkt „Einstellungen / Website-Administration / Nutzerkonten / Nutzerkonten / Nutzer/in neu anlegen“ ein Account angelegt und dem Nutzer die Rolle „Teilnehmer/in“ zugeteilt.

Die angelegten zwei Nutzer sind für den Test des Prototyps nötig. Weitere Nutzer können nach Bedarf angelegt werden.

6.2.3 Erstellen einer Onlineprüfung

Moodle bietet ein Modul namens „Quiz“ an, um eine Prüfung (in Moodle Quiz genannt) zu erstellen. Dies geschieht mit Hilfe eines zweistufigen Prozesses. Im ersten Schritt wird eine Quiz-Activity angelegt und konfiguiert. Die Konfiguration bildet die Regeln für das Quiz ab. Im zweiten Schritt werden dem Quiz Fragen hinzugefügt. Im Folgenden werden als erstes die Konfigurationsparameter und dann das Hinzufügen von Fragen erläutert.

Konfiguration des Quiz

Bevor die Regeln für das Quiz konfiguriert werden, muss zuerst ein Name für die Prüfung bestimmt werden. Für den Tests des Prototypen wird eine „IT Management“ Prüfung angelegt. Als Nächstes wird die Anzahl der Teilnahmeversuche auf 1 gesetzt. Das bedeutet, dass der Prüfling die Prüfung nur ein Mal ablegen darf. Außerdem wird das Anfangsdatum und die Uhrzeit für die Prüfung festgelegt. Analog dazu wird das Enddatum und die Uhrzeit eingestellt. Die Prüflinge können die Prüfung nur in der angegebene Zeitspanne ablegen.

Die Prüfungsdauer, also die Zeit, die die Prüflinge für das Beantworten der Prüfungsfragen haben, ist vom Quiz Modul standardmäßig nicht beschränkt. Daher muss an dieser Stelle

eine Prüfungsdauer bestimmt werden. Während der Bearbeitung der Prüfungsfragen wird dem Prüfling die verbleibenden Zeit angezeigt. Sollte die Zeit ablaufen, wird die Prüfung automatisch abgegeben. Im Falle, dass ein Prüfling betrügt, indem er nach Ablauf der Zeit weitere Fragen beantwortet, so werden diese serverseitig nicht bewertet.

Die Bewertung der Fragen kann automatisiert durch das Quiz Modul erfolgen. Hierfür muss eine entsprechende Regel definiert werden. Für die Beispielprüfung werden aus Vereinfachungsgründen nur Multiple Choice Fragen mit genau einer richtiger Antwort eingesetzt. Jede richtig beantwortete Frage entspricht einem ganzen Punkt. Das Ergebnis der Prüfung ist die Summe der richtig beantworteten Fragen.

Um Täuschungsmöglichkeiten zu reduzieren, wird jede Frage auf einer einzelnen Seite angezeigt. Dies kann mit der Option „New Page“ aktiviert werden. Um den Prüfling daran zu hindern zu bereits betrachteten Fragen zurückzuspringen, muss beim Frageverhalten die Option „Sequentiel“ eingeschaltet werden.

Das Quiz Modul gibt dem Prüfling per Default nach jeder Beantwortung einer Frage ein Feedback darüber, ob die Frage richtig beantwortet wurde. Dieses Verhalten ist u.U. bei einer Übungsprüfung sinnvoll, jedoch bei einer Leitsungsbewertung nicht wünschenswert. Daher wird bei den Review Optionen die Option „Whether correct“ deaktiviert. Der Prüfling sieht nun keine Hinweise zur Bewertung der einzelnen Fragen. Jedoch soll der Prüfling nach Bekanntgabe des Ergebnisses die richtigen Anworten sehen können, weswegen die Option „Right answer“ aktiviert wird. Dem Prüfling wird das Ergebnis direkt nach Abgabe der gesamten Prüfung angezeigt. Die Option, die hierfür aktiviert werden muss heißt „Immediately after attempt“.

Um das Risiko für weitere Täuschungsversuche zu minimieren, muss Moodle in einem besonders abgesicherten Browser laufen. Moodle empfiehlt hierfür den Einsatz des Safe Exam Browsers. Der Safe Exam Browser ist ein konfigurierbarer Webbrowser, der vom Prüfling heruntergeladen und auf dem Computer installiert werden muss. Er ist Voraussetzung für die Teilnahme an der Prüfung und beschränkt den Zugriff auf Browser-Funktionalitäten wie die Web-Navigation, Tastenkombinationen einschließlich Kopieren und Einfügen und das Aufrufen von anderen Seiten im Internet während der Prüfung. Damit der Safe Exam Browser genutzt werden kann, wird die entsprechende Option auf der Seite „Site administration / Development / Experimental / Experimental settings“ ausgewählt.

Hinzufügen von Prüfungsfragen

Sobald ein Quiz erstellt wurde und die Quiz-Konfiguration eingerichtet wurden, kann der Prüfungsersteller beginnen Prüfungsfragen zu erstellen. Hierfür kann der Typ der Frage, wie bspw. Multiple Choice, Rechenaufgabe oder Textaufgabe, bestimmt werden. Nun kann die Frage und ggf. ein Hinweis formuliert werden. Danach werden alle Antwortmöglichkeiten erstellt. Den Antwortmöglichkeiten müssen Punkte zugeteilt werden. Da bei der Testprüfung nur eine Antwort richtig sein kann, bekommt nur eine Antwortmöglichkeit die Punktezahl 1 und alle anderen 0. Alle erstellten Prüfungsfragen landen automatisch auch im Fragekatalog. So können andere Prüfungsersteller die Fragen wiederverwenden.

6.3 Safe Exam Browser

Der Safe Exam Browser (kurz: SEB) wurde 2008 im Rahmen eines Projektes an der Universität Giessen und der ETH Zürich entwickelt. Seit 2010 wird die Entwicklung des Open-Source-Browsers durch das SWITCH3-Förderprogramm unterstützt. Die SEB ist eine Softwareanwendung, die analog zu einem Webbrowser plattformunabhängige Visualisierung und interaktive Nutzung von Webinhalten ermöglicht. Der Fokus der SEB liegt jedoch auf dem sicheren Zugriff auf onlinebasierte Prüfungen. Der SEB unterstützt die Learning Management Systeme Moodle sowie ILIAS. Unabhängig von der verwendeten Plattform kann er sowohl auf Windows- als auch auf Mac-Betriebssystemen installiert werden. Dadurch macht der SEB jeden Rechner zu einer abgesicherten Prüfungsumgebung, in der diverse Betriebssystemfunktionen wie bspw. das Umschalten auf andere Applikationen, unerwünschte Tastenkombinationen zur Systemsteuerung oder die Nutzung des Internet temporär eingeschränkt bzw. ausgeschaltet werden können. Nach Beendigung der Online Prüfung stellt der SEB seinen ursprünglichen Zustand wieder her.

Die Browser-Komponente des SEB kann alle üblichen Elemente von Webseiten darstellen, inklusive Video-, Audio-, Java- und Plugin-Inhalten. Sie verfügt aber nicht über die üblichen Navigationselemente wie Adresszeile oder Suchmaschinenfeld. Die Startadresse der Prüfung beziehungsweise einer Prüfungsportalseite mit Links auf die jeweils aktuellen Prüfungen wird vorkonfiguriert, sodass sich der SEB nach dem Starten automatisch damit verbindet. Die eigentlichen Prüfungen laufen in der Regel im Quiz-Modul innerhalb des LMS ab. Für den SEB wurden Erweiterungen zu diesen Modulen in Moodle realisiert, sodass SEB hier ohne weiteren Programmieraufwand funktioniert. Die Erweiterungen gewährleisten eine sichere Durchführung der Prüfungen und sind inzwischen im Core-Code der Lernplattform integriert. Durch spezielle Themes werden die Navigationselemente des LMS während der Prüfung ausgeblendet. Die Prüfungskandidaten können also nicht per Link aus dem Prüfungsmodul heraus in den allgemeinen Bereich des LMS gelangen. Außerdem wird so der Zugang zu den häufig im LMS vorhandenen Kommunikationsmöglichkeiten, wie Chat oder Nachrichten, unterbunden. Die „Secure Browser“-Option in Moodle bietet außerdem die Möglichkeit, die Ausführung der Prüfung im SEB zu erzwingen. Diese Einstellungen lassen sich bei der Erstellung der Tests durch den Prüfungsersteller in den der Lernplattform konfigurieren. Der SEB ist als abgesicherter Webbrowser grundsätzlich in der Lage, mit jedem webbasierten Exam Management System zusammenzuarbeiten. Deswegen ist der Einsatz keinesfalls auf die ausdrücklich unterstützten LMS-Prüfungsmodule beschränkt. Neben der Anbindung über das Internet bzw. Intranet an ein Exam Management System kann SEB zusätzliche, auf dem Prüfungsrechner installierte Applikationen, wie z.B. einen Taschenrechner, zur Benutzung während einer Prüfung zulassen.

6.3.1 Konfiguration des SEB

SEB für Windows verfügt über ein komfortables Konfigurationstool, das zur Konfiguration von SEB verwendet werden kann. Es befindet sich im SEB-Programmordner „C:\Programme\SafeExamBrowser“ und heißt „SEBConfigTool.exe“. Im SEB-Konfigurationstool sind die Einstellungen in mehreren Reiter gruppiert. Dort kann man die unten beschriebenen Parameter einstellen:

- Im Reiter „General“ befinden sich die grundlegenden Einstellungen wie die URL, die

SEB als Erstes öffnen soll, und die Passwörter zum Öffnen der Konfigurationsdatei und zum Beenden bzw. Neustarten von SEB.

- Unter „Config File“ sind Details zur Verschlüsselung der SEB-Konfigurationsdateien sowie alle Funktionen zum Öffnen, Speichern, Wiederherstellen, Duplizieren und Anwenden von Einstellungen enthalten.
- „User Interface“ enthält allgemeine SEB-Benutzeroberflächeneinstellungen
- Unter „Browser“ befinden sich alle Detaileinstellungen für den integrierten Webbrowser
- „Down/Uploads“ befasst sich mit dem Herunter- und Hochladen von Dateien
- „Exam“ behandelt die Verbindung zum LMS und prüfungsspezifischen Einstellungen
- Im Reiter „Application“ kann man erlaubte und verbotene Prozesse verwalten
- Unter „Network“ kann man URL Filter, Zertifikate und Proxies konfigurieren
- „Security“ enthält Details zum Deaktivieren von sicherheitsrelevanten Systemfunktionen
- „Registry“ ermöglicht die Verwaltung von Optionen im Task Manager sowie eine Option zum Einsatz von Virtualisierung
- Unter „Hooked Keys“ kann man Tastatur- und Mausbefehle blockieren

Für den Prototpyen wird eine sehr strenge Konfigurationen gemäß den Anforderungen aus der Anforderungsanalyse gewählt.

6.3.1.1 General

Als Start-URL wird der Pfad (https://10.54.32.12/moodle) zur Portalseite des LMS konfiguriert. Ein Administrationskennwort ist erforderlich, um die Konfigurationsdatei vor unberechtigten Änderungen zu schützen, auch wenn diese nicht an den Prüfling übertragen wird. Die Option „Allow user to quit SEB“ wird deaktiviert und die Option „Ignore exit keys“ wird aktiviert. So kann der Prüfling während der Prüfung den Browser nicht über die Systemfunktionen beenden. Dem Prüfling wird jedoch die Möglichkeit geboten, über einen Link im Browserfenster SEB zu schließen. Diese Aktion gilt dann als Abgabe der Prüfung.

6.3.1.2 Config File

Unter „Use SEB settings file for“ wird die Option „start an exam“ ausgewählt, da dies die initiale Konfiguration für eine Prüfung ist. Prüflinge dürfen nicht das Fenster für die Einstellungen öffnen. Daher wird die Option „Allow to open preferences window on client“ abgewählt.

6.3.1.3 User Interface

Unter Browser View Mode wird die Option „Use full screen mode“ ausgewählt. Dies bewirkt, dass der Prüfling nur den Inhalt des SEB angezeigt bekommt und keine weiteren Programme bzw. den Desktop. Wenn eine andere Webseite in einem neuen Fenster geöffnet wird, wird diese hinter dem Hauptfenster des Vollbildschirms versteckt. Das Einblenden alle Menüs bis auf das des SEB wird deaktiviert.

6.3.1.4 Browser

Link, die ein neues Browserfenster öffnen, werden nicht ausgeführt. Daher wird für „Links requesting to be opened in a new browser window“ die Option „get generally blocked“ aktiviert. Dies wird auch für Weiterleitungen, die per JavaScript ausgelöst werden, eingestellt. „Block when directing to a different server“ sorgt dafür, dass keine anderen Server, außerhalb der Domäne des Prüfungssystems angesteuert werden können.
Unter „Browser Security Settings“ wird die Nutzung von Browser Plugins und Java Applets deaktiviert, da diese vom LMS nicht eingesetzt werden. Lediglich JavaScript muss aktiviert werden, damit die Authentication Module, die in JavaScript geschrieben sind, funktionieren. Um die Aufnahme von Webcambildern für die Face Recognition zuzulassen, muss die Option „Allow video capture (webcam)“ aktiviert werden. Das Vor- und Zurücknavigieren wird mit der Option „Allow browsing back/forward“ deaktiviert. Außerdem wird „Remove profile“ ausgewählt, um die Daten, die der Browser seit dem Start des Programms generiert, nach Beendigung von SEB vom Rechner zu entfernen.

6.3.1.5 Down- und Uploads

Das Herunter- und Hochladen von Dateien ist für die Bearbeitung der Prüfung nicht notwendig. Deshalb wird dies unterbunden. Lediglich das Herunterladen von neuen SEB Konfigurationen wird erlaubt. So können geänderte Konfigurationen während der Prüfung nachgeladen werden.

6.3.1.6 Exam

Um sicherzustellen, dass nur die veröffentlichte Instanz von SEB und die dazugehörige Konfiguration auf die Prüfung zugreifen kann, wird eine sogenannter Browser Exam Key verwendet. Dieser Key wird im SEB Konfigurationstool erstellt und in der Moodle Konfiguration eingetragen. Der Browser Exam Key wird dann während der Prüfung an das LMS im HTTP Header an das LMS geschickt und der Prüfling somit authentifiziert.

Nachdem der Prüfling die Prüfung bearbeitet und abgegeben hat, schließt sich SEB automatisch. Hierfür muss in der SEB Konfiguration der Link zu der Seite in Moodle, die erscheint, wenn die Prüfung abgegeben wurde, hinterlegt werden. Moodle zeigt jedem Prüfling nach Abgabe der Prüfung eine Zusammenfassung an. Der Pfad zu dieser Seite wird für die automatische Beendigung von SEB genutzt.

6.3.1.7 Application

Anwendungen von Drittanbietern dürfen nicht verwendet werden, während SEB ausgeführt wird. Auch wird der Zugriff auf das lokale Dateisystem und das Internet über eine andere

Anwendung deaktiviert. Dies stellt einen redundanten Schutz dar, falls der Prüfungsersteller vergisst andere Anwendungen zu blockieren. Hierzu werden die Optionen „Accessing the file system“, „Accessing the internet“ und „Allow switching to third party applications“ abgewählt.

6.3.1.8 Network

Im „Network“ Reiter wird der URL Filter so eingestellt, dass ein Navigieren außerhalb der Prüfungsumgebung unterbunden wird. SEB erstellt hierfür automatisch eine Filterregel für die Adresse, die als Start-URL definiert wurde. Dies bedeutet, dass wenn die Start-URL 10.54.32.12/moodle ist, alle Seiten und Ressourcen in der Domäne 10.54.32.12/moodle zulässig sind. Zertifikate und Proxies werden nicht konfiguriert.

6.3.1.9 Security

Der SEB-Dienst ist ein Hintergrundprozess mit Administratorrechten. Dieser ist notwendig, um unerwünschte Systemfunktionen, wie z.B. den Taskmanager, den Windows-Update-Dienst und den Screenshot-Dienst zu blockieren. Der SEB-Windows-Dienst wird automatisch zusammen mit der SEB-Anwendung installiert und anschließend gestartet. SEB funktioniert auch ohne diesen Dienst, jedoch mit einer niedrigeren Sicherheitsstufe. Um ein Starten von SEB ohne den SEB-Dienst zu unterbinden, wird unter „SEB Service policy“ die Option „allow to use SEB only with service“ ausgewählt.

Auch das Ausführen des SEB in einer virtuellen Maschine birgt Risiken. Deshalb wird die Option „Allow SEB to run inside virtual machine“ ebenfalls deaktiviert.

Der SEB wird als Kiosk Applikation ausgeführt. Dies bedeutet, dass der Nutzer nicht über Tastenkürzel auf andere Programme umschalten kann. Hierfür wird SEB auf einem neuen Desktop gestartet. Die Umstellung auf den Standard-Desktop ist dadurch nicht mehr möglich. Andere Anwendungen sind unsichtbar und können während der Prüfung nicht erreicht werden. Der Kiosk-Mode verhindert außerdem, dass Bildschirmaufzeichnungssoftware die Nutzeroberfläche aufnimmt.

6.3.1.10 Registry

Der Prüfling darf während der Prüfung unter keinen Umständen den Desktop des Betriebssystems bzw. seinen Account verlassen, da er sonst Möglichkeiten zur Täuschung hätte. Daher sind die Optionen „Enable Switch User“, „Enable Lock this computer“, „Enable Change a password“ und „Enable Start Task Manager“, „Enable Log off“, „Enable Shut down“ und „Enable Ease of Access“ deaktiviert.

6.3.1.11 Hooked Keys

in diesem Reiter wird das Aufnehmen von Screenshots und die Nutzung von Funktionstasten der Tastatur deaktiviert. So kann der Nutzer keine Screenshots von den Prüfungsfragen erstellen.

6.4 Framework

Für die Authentifizierung des Prüflings werden Module eingesetzt, die das Gesicht und das Tippverhalten des Nutzers überwachen. Die Programme sind in Client- und Servermodule aufgeteilt. Für die Implementierung wurde ein Framework erstellt mit dessen Hilfe die Implementierung der Authentifzierungsmodule vereinfacht wird. Dazu werden als Datenbank MongoDB, als Server Node.js verwendet und clientseitig JavaScript Module eingesetzt.

6.4.1 Node.js

Node.js ist ein sehr leistungsfähiges JavaScript-basiertes Framework, das auf der JavaScript V8 Engine von Google Chrome basiert. Es wird verwendet, um I/O-intensive Webanwendungen wie Video-Streaming-Seiten und andere Webanwendungen zu entwickeln. Node.js ist Open Source und kostenlos. Aus den genannten Gründen eignet sich node.js besonders für die serverseitige Verarbeitung der Gesichtserkennung und Tippverhalten API. Mit folgenden Befehlen wird node.js auf dem Server installiert.

```
1 sudo apt-get install -y nodejs
2 sudo apt-get install -y build-essential
```

Listing 6.4: Installation von Node.js

Um den Datenverkehr, der über HTTP bzw. HTTPS am Node.js Framework ankommt, routen zu können, wird das das Modul Express.js benötigt. Express.js ist ein Routing Framework für Node.js. Es bietet verschiedene Funktionen, die die Entwicklung von Webanwendungen schnell und einfach machen. Die eigenständige Implementierung würde ansonsten mehr Zeit in Anspruch nimmt. Express.js basiert auf dem Middleware-Modul von Node.js mit dem Namen connect, das wiederum das Modul http verwendet. Im Folgenden wird die Installation und Einrichtung des Routing mit express.js erläutert.

```
1 npm install -g express
2 npm install express --save
```

Listing 6.5: Installation von Express.js

Nun wird das Express Framework mit dem HTTP Port 8080 initialisiert. Dies bedeutet, dass der API Server über diesen Port alle Anfragen empfängt.

```
1 var app = express();
2 app.set('port', configServer.httpPort);
3 app.use(express.static('public'));
4 app.use(express.static(configServer.staticFolder));
```

Listing 6.6: Express.js wird initialisiert

Die Konfiguration des Express Frameworks befindet sich in der Datei server.js und schaut wie folgt aus:

```
1 module.exports = {
2   httpPort: 8080,
3   staticFolder: path.join('./client')
4 };
```

Listing 6.7: Die Konfiguration des Servers

6.4.2 MongoDB

MongoDB ist eine Open-Source-Dokumentendatenbank, die hohe Leistung, hohe Verfügbarkeit und automatische Skalierung bietet [mon17]. In dieser Datenbank werden Daten persistiert, die die APIs generieren.

```
1 sudo apt-get install -y mongodb-org
```

Listing 6.8: Installation von MongoDB

Die Datenbank wird durch das Node.js Modul „mongodb“ in den API Server integriert. Es ist eine Art Treiber für die Kommunikation zwischen dem API Server und der Datenbank.

6.4.3 Socket.io

Socket.io ist eine JavaScript-Bibliothek für Echtzeit-Webanwendungen. Es ermöglicht eine bidirektionale Echtzeitkommunikation zwischen Webclients und Servern. Es besteht aus zwei Teilen: einer clientseitigen Bibliothek, die im Browser ausgeführt wird, und einer serverseitigen Bibliothek für Node.js. Beide Komponenten haben eine nahezu identische API. Mit folgendem Befehl wird Socket.io der Node.js Instanz hinzugefügt:

```
1 npm install socket.io --save
```

Listing 6.9: Installation von Socket.io

Danach wird die Bibliothek in den API Server eingebunden und so konfiguriert, dass eingehende Verbindungen an das Skript „socket.js“ weitergeleitet werden. In „socket.js“ werden die Socketschnittstellen für die beiden APIs definiert. Die konkrete Kommunikation zwischen den Modulen und APIs wird später erläutert.

```
1 var io = require('socket.io')(server);
2 io.on('connection', require('./lib/routes/socket'));
```

Listing 6.10: Konfiguration des Sockets

Clientseitig wird ebenfalls die Socket.io Bibiliothek eingebunden und an die Variable „socket“ übergeben. Danach kann eine Verbindung zum Server aufgebaut werden.

```
1 var socket = io.connect('http://192.168.10.58:8080');
```

Listing 6.11: Aufbau einer Socket Verbindung im Module

Nun ist das Authentication Framework einsatzbereit und die einzelnen Authentication Modules und APIs können implementiert werden.

6.5 Gesichtserkennung

Die Implementierung der Gesichtserkennung gliedert sich in zwei Teile. Das Gesichtserkennung Module nimmt Bilder vom Prüfling per Webcam auf und schickt sie dann an die Gesichtserkennung API. Diese wendet auf das Bild die Algorithmen Viola Jones und LPB an, um den Nutzer kontinuierlich zu authentifizieren.

6.5.1 Gesichtserkennung Module

Der Client bei der Gesichtserkennung übernimmt die Aufgabe der Bildaufnahme und -weiterleitung. Des Weiteren werden die Metadaten der Prüfung, also u.a. die ID des Prüflings und der Prüfung an den Server geschickt, um die Bilder später dem Prüfling und der Sitzung zuordnen zu können. Für die Aufnahme des Bilds werden die Boardmittel von HTML5 genutzt. Mit dem Tag „video“ wird das Bild der Webcam angefordert. Die Auflösung wird auf 640x480 gesetzt, welche ausreichend ist, um das Gesicht des Prüflings bis drei Meter vor dem Bildschirm zu erkennen.

```
1 <video id="video" width="640" height="480" autoplay></video>
```

Listing 6.12: Erstellung eines Video Elements für die Aufnahme der Bilder

Sobald festgestellt wurde, dass eine Webcam vorhanden ist, setzt eine einfache Methode die Quelle des Videoelements auf die Webcam des Benutzers. Das Aufrufen der Abspielmethode des Videos startet dann die Live-Streaming-Video-Verbindung des Elements.

Um das Bild per Websocket an den Server schicken zu können, muss es jedoch zuerst in ein übertragbares Format konvertiert werden. Hier bietet sich die Base64 Kodierung an, die es ermöglicht Bilder in Zeichen umzuwandeln.

```
1 setInterval(function() {
2   socket.emit('pic', canvas.toDataURL().replace("", "")
        );
3 }, 1000);
```

Listing 6.13: Senden der Daten an die Gesichtserkennung API

Nach der Umwandlung wird die Base64 Zeichenkette via Websocket an den Server geschickt. Dies geschieht jede Sekunde.

6.5.2 Gesichtserkennung API

Für die Gesichtserkennung wird der Viola-Jones Algorithmus genutzt. Implementiert ist der Algorithmus in der Bibliothek OpenCV *vgl.*[Ope17], die neben der Gesichtserkennung auch Algorithmen für die Alters- und Geschlechtsbestimmung bereitstellt. OpenCV ist in C++ geschrieben und eignet sich nicht für den nativen Einsatz auf einem Webserver. Daher wird das node.js Binding „opencv“ *vgl.*[Bra17] eingesetzt, um via JavaScript auf die Bibliothek zuzugreifen.

Zuerst müssen per Kommandozeile und dem Paketmanager apt-get die relevanten Pakete, die OpenCV voraussetzt, heruntergeladen und installiert werden.

```
1 sudo apt-get install build-essential
2 sudo apt-get install cmake git libgtk2.0-dev pkg-config libavcodec-dev
      libavformat-dev libswscale-dev
3 apt-get install imagemagick
```

Listing 6.14: Installation der unterstützenden Bibliotheken für OpenCV

Anschließend wird OpenCV als Quellcode heruntergeladen und mit dem Programm make kompiliert. Anschließend ist das System bereit, um auf die Bibilotheken von OpenCV zuzugreifen.

```
cd ~/opencv
mkdir release
cd release
cmake -D CMAKE_BUILD_TYPE=RELEASE -D CMAKE_INSTALL_PREFIX=/usr/local ..
make
sudo make install
```

Listing 6.15: Installation von OpenCV

Die mit Base64 kodierte Zeichenkette wird in einen Puffer geladen. Diese Datenstruktur ist nötig, da OpenCV keine Base64 kodierten Bilder verarbeiten kann.

```
cv.readImage(Buffer.from(data.image, 'base64'), function(err, im)
```

Listing 6.16: Einlesen des empfangenen Bilds

Mit der Funktion „detectObject“ wird auf dem Bild nach Gesichtern gesucht. Die gefundenen Gesichter werden im Array „faces“ gesammelt.

```
im.detectObject('./node_modules/opencv/data/haarcascade_frontalface_alt_tree.
    xml', {}, function(err, faces)
```

Listing 6.17: Erkennung von Gesichtern auf dem Bild

Jedes gefundene Gesicht wird aus dem Bild ausgeschnitten und in eine Graustufendarstellung konvertiert, um es für den Vergleich mit dem trainiert Modell mit Hilfe des LBP Algorithmus vorzubereiten.

```
var im2 = im.roi(face.x, face.y, face.width, face.height);
```

Listing 6.18: Ausschneiden des Gesichts aus dem empfangenen Bild

```
im2.cvtColor('CV_BGR2GRAY');
```

Listing 6.19: Konvertierung in eine Graustufendarstellung

Das optimierte Bild kann mit Hilfe der Funktion „predictSync“ mit dem Referenzmodell verglichen werden. Für die Bestimmung der Ähnlichkeit wird der LBP Algorithmus verwendet. Dieser wir mit dem Wert acht initialisiert. Die bedeutet, dass die acht nächsten Nachbarn jedes Pixeln für die Erstellung des lokalen Binärmusters betrachtet werden. Die Rückgabe der Funktion „predictSync“ ist die euklidische Distanz zwischen den beiden Bildern.

```
var facerec = cv.FaceRecognizer.createLBPHFaceRecognizer(1, 8, 8, 6, 80.0);
```

Listing 6.20: Initialisierung des LBP Algorithmus

```
facerec.predictSync(im2);
```

Listing 6.21: Vergleich des optimierten Bilds mit dem Referenzmodell

Die Ergebnisse des Gesichtsvergleichs werden zusammen mit den Metadaten der Prüfungssitzung in der Datenbank persistiert.

Das Referenzmodell ist das Gesicht des echten Prüflings. Dieses Modell muss vor der Prüfung von einem berechtigten Mitarbeiter der Universität erstellt werden. Denkbar wäre die Aufnahme der Bilder zum Trainieren des Modells bei der Immatrikulation des Studenten oder in einer Übungsstunde vor der Prüfung. Die aufgenommenen Bilder werden in einen Array geladen und der Funktion „trainSync“ übergeben, die das Modell trainiert.

```
var trainingData = [];

for (var j = 0; j < 38; j++) {
    trainingData.push([1, __dirname + "/pics/" + j + "_pic_user.jpg"]);
}
facerec.trainSync(trainingData);
```

Listing 6.22: Training des Referenzmodell mit 39 Bilder des Studenten

Das trainierte Modell des Studenten wird anschließend in der Datenbank abgelegt.

6.6 Tippverhalten

Auch die Überwachung des Tippverhaltens teilt sich auf zwei Systeme auf. Die Clientseite nimmt die Daten zum Tippverhalten auf und schickt sie dann an die API, die sie mit dem trainierten Modell des überprüften Studenten vergleicht. Hierfür wird die JavaScript Bibliothek tappy.js verwendet, die Tippmuster aufzeichnen und mit anderen vergleichen kann.

6.6.1 Tippverhalten Module

Immer wenn der Nutzer bei der Prüfung eine Taste drückt, wird eine Funktion aufgerufen, die Daten zum Tastendruck wie Verweildauer und Zeichen aufzeichnet. Ist das Zeichen ein Leerzeichen oder Zeilenumbruch, werden die bisher eingegeben Daten zu einem Rhythmus geformt und zusammen mit den Metadaten der Prüfung an die API geschickt.

```
trainer.addEventListener('keypress', function(e) {

  if ((e.which === 32 || e.which === 13)) {
    emitRhythm(e);
  } else {
    testRhythm.tap();
  }
}, false);
```

Listing 6.23: Aufruf der Funktion bei jedem Tastendruck

```
socket.emit('keystroke', keystrokePackage);
```

Listing 6.24: Senden der aufgenommenen Daten per Socket an die Tippverhalten API

6.6.2 Tippverhalten API

Das empfangene Tippmuster wird auf der Serverseite nun mit dem Referenzmodell verglichen. Dazu wird die Funktion „compare“ genutzt, die die Ähnlichkeit zwischen beiden Mustern berechnet. Das Ergebnis ist der Grad der Übereinstimmung, hier Closeness genannt, zwischen den Rhythmen. Alle Ergebnisse werden zusammen mit den Metadaten in der Datenbank abgelegt.

```
closeness = (tappy.compare(keystrokePackage.testRhythm, userKeystrokePackage.
    keystroke, true) * 100);
```

Listing 6.25: Vergleich des empfangenen Tippmusters mit dem Referenzmodell

Das Referenzmodell des Studenten kann beispielsweise in einer überwachten Übungsklausur erstellt werden. Dazu wird jede Eingabe des Studenten für das Training des Modells genutzt.

6.7 Reportgenerierung

Die Ergebnisse der Authentizitätsprüfung einer Prüfungssitzung werden im Reporting dargestellt. Der Report Client zeigt die sekündlich aufgenommen Bilder während der Prüfung an. Zusätzlich kann man sich zu jedem Bild die Einschätzung der Gesichtserkennung in einem Plot Chart anschauen. Außerdem werden in einer Tabelle die Closeness-Werte zum Tippverhalten angezeigt.

Der Plot Chart wird mit der Chart Library D3.js [d3117] generiert. Die Werte des Chart werden aus der Datenbank gelesen und dann mit Hilfe der Bibliothek visualisiert. Die Punkte der Datenwerte können unterschiedliche Farben haben. Ein grüner Punkt bedeutet, dass das Gesicht als ausreichend authentisch eingestuft wurde. Ein roter Punkt zeigt an, dass die euklidische Distanz einen Schwellenwert überschritten hat und somit nicht ausreichend authentisch ist. Sind mehr als ein Gesicht auf dem Bild erkannt worden, so wird dies als gelber Punkt dargestellt.

Mit einem Regler können einzelne Bilder angesteuert werden. Es ist auch möglich mit einem Startknopf den Ablauf in einem Zeitraffer anzuschauen. Die Geschwindigkeit des Ablaufs kann mit einem zweiter Regler erhöht bzw. verringert werden.

Zu jedem erkannten Tipprythmus wird die Closness angezeigt. Ist der Wert über 50% so wird dies als ausreichend authentisch bewertet. Daher erscheint neben dem Wert ein grüner Punkt. Andernfalls ist der Punkt rot.

7 Evaluation des Prototypen

In diesem Kapitel geht es um die Evaluation des Prototyps. Mit Hilfe eines Probandentests soll herausgefunden werden, wie das SSAOP in realitätsnahen Szenarien reagiert. Dabei führt eine Probandengruppe Anweisungen eines Skripts an dem Testobjekt aus.

7.1 Probandentest des Systems

Ein Probandentest bietet die Möglichkeit das SSAOP mit repräsentativen Nutzern der Zielgruppe zu testen. Es wird die Methode des szenariobasierten Nutzungstests angewendet. Die Versuchsteilnehmer werden mit Hilfe eines Skripts angeleitet Aufgaben am SSAOP zu lösen. Die Szenarien entsprechen dabei möglichst realen Nutzungsfällen. Während der Proband die Aufgaben löst, wird sein Verhalten mit den Methoden des SSAOP überwacht und später analysiert.

7.1.1 Fragestellungen

Durch den Probandentest soll herausgefunden werden, inwieweit Täuschungsversuche offengelegt werden können. Hierbei soll einerseits untersucht werden, ob eine fremde Person bzw. ein zweites Gesicht anhand der Analysedaten der Gesichtserkennung API erkannt werden kann. Andererseits soll evaluiert werden, ob die Daten der Tippverhalten API Rückschlüsse auf die Authentizität des Prüflings zulassen.

7.1.2 Testobjekt

Das Testobjekt ist das SSAOP, dass sich vollständig auf dem Testrechner befindet, der von den Probanden für das Lösen der Prüfungsfragen genutzt wird. D.h. Server und Client befinden sich hierbei beide auf demselben Rechner. Im Realfall würden diese Systeme voneinander getrennt betrieben werden. Diese Konfiguration hat jedoch keine Auswirkungen auf die Testergebnisse.

7.1.3 Probandengruppe

Bei der Auswahl der Versuchsteilnehmer steht im Vordergrund, dass die ausgewählten Personen aus der angestrebten Zielgruppe stammen. Daher werden für das Experiment zwei Studenten ausgewählt, die die Szenarien durchführen. Sie werden dazu angehalten, sich strikt an die Vorgaben zu halten. Proband A ist hierbei der „echte“ Prüfling, dessen Gesicht und Tippverhalten als Referenzmodelle im System hinterlegt sind. Proband B ist dem System nicht bekannt.

7.1.4 Szenarien

Die Szenarien geben dem Probanden vor, wie er die Prüfung bearbeiten soll. Hier wird der Versuchsteilnehmer einmal dazu angewiesen Täuschungsversuche anzuwenden und das andere Mal auf diese zu verzichten. Im ersten Szenario kommt die zweite Personen zum Einsatz, um der ersten zu helfen. Die zwei Testpersonen müssen die unten beschriebenen Szenarien ausführen.

Szenario 1: Mit Täuschungsversuche

Proband A ist die Person, die für die Prüfungsteilnahme berechtigt ist. Er bekommt die Anweisung im Verlauf der Prüfung zu täuschen. Zu Beginn bearbeitet er die erste Frage alleine. Danach kommt der zweite Proband B dazu, dessen Gesicht nicht für die Teilnahme autorisiert ist. Nachdem beide zusammen die zweite Aufgabe gelöst haben, verlässt A die Prüfungsumgebung. B bearbeitet die Prüfung nun alleine weiter. Die Antwort zu Frage vier soll er mit Hilfe seines Smartphones suchen. Nach der fünften Aufgabe kommt A wieder hinzu. Er bleibt solange, bis die Frage beantwortet ist. Die letzte Frage absolviert B erneut alleine.

Szenario 2 Ohne Täuschungsversuche

Der Proband bekommt die Anweisung, die Aufgaben ohne Täuschungsversuche zu bearbeiten. Es sind keine Hilfsmittel erlaubt. Auch dürfen Dritte dem Versuchsteilnehmer nicht bei der Bearbeitung unterstützen. Ein Aufstehen vom Prüfungsort ist nicht gestattet. Der Blick muss stets auf dem Bildschirm gerichtet sein. Der simulierte Prüfling ist die Person, die für die Prüfung autorisiert ist.

7.1.5 Prüfung

Die Prüfung besteht aus fünf Multiple-Choice und zwei Freitext Fragen. Alle Fragen müssen von den Probanden beantwortet werden. Die letzte Aufgabe fordert den Probanden zum Abtippen eines Textes ab. Hier soll die Tippverhalten API getestet werden.

1. Welcher Buchstabe kam in der Entstehungsgeschichte des heute gebräuchlichen Alphabets erst im Mittelalter hinzu?

- V
- W (richtig)
- C
- A

2. Welches Instrument spielte der Inder Ravi Shankar?

- Klavier
- Tabla
- Flöte
- Sitar (richtig)

3. Das Kfz-Kennzeichenkürzel welcher Landeshauptstadt findet man nicht als Symbol eines chemischen Elements?

- Stuttgart
- Potsdam
- Düsseldorf (richtig)
- Hannover

4. Wo kann man die sogenannte Guillotine-Technik sehr häufig beobachten?

- Beim Frühstücken (richtig)
- Beim Rasieren
- Beim Bügeln
- Beim Boxen

5. Wobei unterscheidet man zwischen einer Grün- und einer Blaureihe?

- Wellensittiche (richtig)
- Beeren
- Karate Gürtel
- Medikamente

6. Wofür steht die Abkürzung „B.Sc.“?

Antwort: „Bachelor of Science“

7. Schreiben Sie folgenden text ab:

In der Mitte vom Spiel-Feld gibt es einen Kreis. Dieser Kreis heißt Anstoß-Kreis. In dem Kreis ist ein Punkt. Dort beginnt das Spiel. 2 Spieler aus einer Mannschaft stehen in dem Kreis. Der Ball liegt auf dem Punkt. Der Schieds-Richter pfeift. Dann kann ein Spieler den Ball spielen und das Spiel beginnt. Das nennt man auch: Anstoß.

7.1.6 Ergebnis

Die Ergebnisse der kontinuierlichen Authentifizierung werden über die Reportingschnittstelle abgerufen. Hier kann man die Bildaufnahmen und Tastatureingaben einsehen. Für den Probandentests wurden die Grenzwerte für die Algorithmen bei 60 für die Gesichtserkennung und bei 50 für das Tippverhalten festgelegt. Dies bedeutet, dass ein Wert über dieser Grenze als „erfolgreich authentifiziert“ interpretiert wird. Im Folgenden werden die Daten für die zwei Szenarien erläutert.

7.1.6.1 Szenario 1

Im ersten Szenario sollten zwei Probanden, A und B, bei der Prüfung betrügen. Der Plot Chart dokumentiert das Verhalten der Probanden (s. Abb. 7.1). So kann man in den ersten Sekunden des Tests erkennen, dass das Gesicht des Nutzers erfolgreich authentifiziert wurde. Kurz danach werden zwei Gesichter erkannt. Zu dieser Zeit befanden sich tatsächlich beide Teilnehmer vor der Kamera. Anschließend entfernte sich Proband A, der den echten Prüfling simulierte, vom Bildschirm. Auch dies kann man im Chart anhand der roten Punkte erkennen. Nach einer kurzen Phase, in der Proband B die Aufgaben löste, erkennt man schwarze Punkte. Diese Farbe zeigt an, dass gar kein Gesicht erkannt wurde. Auch diese Informationen spiegelt den tatsächlichen Ablauf wieder, da zu der Zeit Proband B sein Kopf nach unten geneigt hatte, um auf sein Smartphone zu schauen. Die Kamera nahm nur das Haar des Teilnehmers auf. Anschließend blickt Proband B zurück auf den Bildschirm. Das erkennt man an den roten Punkten. Auf diese folgen gelbe Punkte, da Proband A zum Prüfungsort zurückgekehrt ist. Jedoch verlässt er diesen nach kurzer Zeit wieder, weswegen die euklidische Distanz von dort an bis zum Ende über den Wert 60 klettert.
Auf die letzten zwei Aufgaben sollten die Probanden mit Hife von Texteingaben über die Tastatur antworten. In Szenario eins sollte Proband B die Aufgaben lösen. Dies bedeutet, dass die Closeness Werte unter 50 liegen sollte. Ein Blick auf die Reportingschnittstelle verrät, dass die meisten der 32 Eingaben als nicht authentisch erkannt wurden (s. Abb. 7.2). Lediglich der Wert von neun Eingaben lag über dem Grenzwert von 50.

7.1.6.2 Szenario 2

Der Proband hat für das zweite Szenario die Anweisung bekommen keine Täuschungsversuche zu übernehmen. Der Plot Chart zur Visualisierung der euklidischen Distanz zeigt bis auf zwei Ausnahmen keine Auffälligkeit. Die zwei gelben Punkte zeigen eine Erkennung von mehr als einem Gesicht. Da im Versuch kein zweites Gesicht vor der Kamera war, liegt diese Einschätzung daran, dass fälschlicherweise andere Objekte oder Schatten als Gesicht erkannt

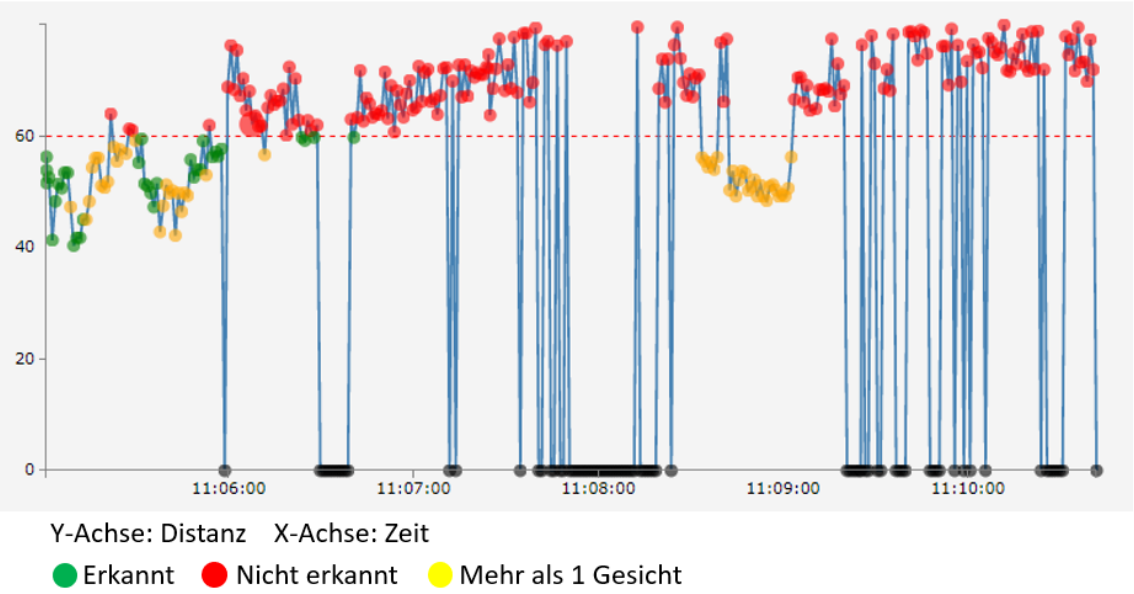


Abbildung 7.1: Der Ablauf kann anhand des Charts nachvollzogen werden

wurden. Die Einschätzung für das Tippverhalten liegt im Durchschnitt über 85 Prozent. Auch hier gibt es einen Ausreißer bei dem Begriff „es“ (s. Abb. 7.3).
Zusammengefasst haben die Ergebnisse der kontinuierlichen Authentifizierung in einem zuverlässigen Maß die Geschehnisse vor der Kamera und an der Tastatur dokumentiert. Jedoch ist die Anzahl der Tests nicht repräsentativ, weswegen weitere Versuche durchgeführt werden sollten.

word	closeness	
In	80.2	
der	52.1	
Mitte	48.1	●
vom	28.6	●
Spiel-Feld	46.4	●
gibt	42.0	●
es	93.1	
einen	35.3	●
Kreis	28.4	●
Kreis	38.1	●
heißt	60.1	
Kreis.	31.3	●
dem	26.9	●
Kreis	43.4	●
ist	43.3	●
ein	30.5	●
Punkt.	39.0	●
Dort	38.9	●
das	28.7	●
Spiel	38.5	●
Spieler	51.6	
aus	55.1	
einer	36.5	●
Mannschaft	45.0	●
stehen	33.7	●
dem	38.4	●
Der	25.1	●
Ball	58.0	
liegt	62.7	
auf	26.7	●
dem	42.9	●
.Der	64.7	

Closeness: Prozent

Abbildung 7.2: Die meisten Texteingaben liegen unter 50

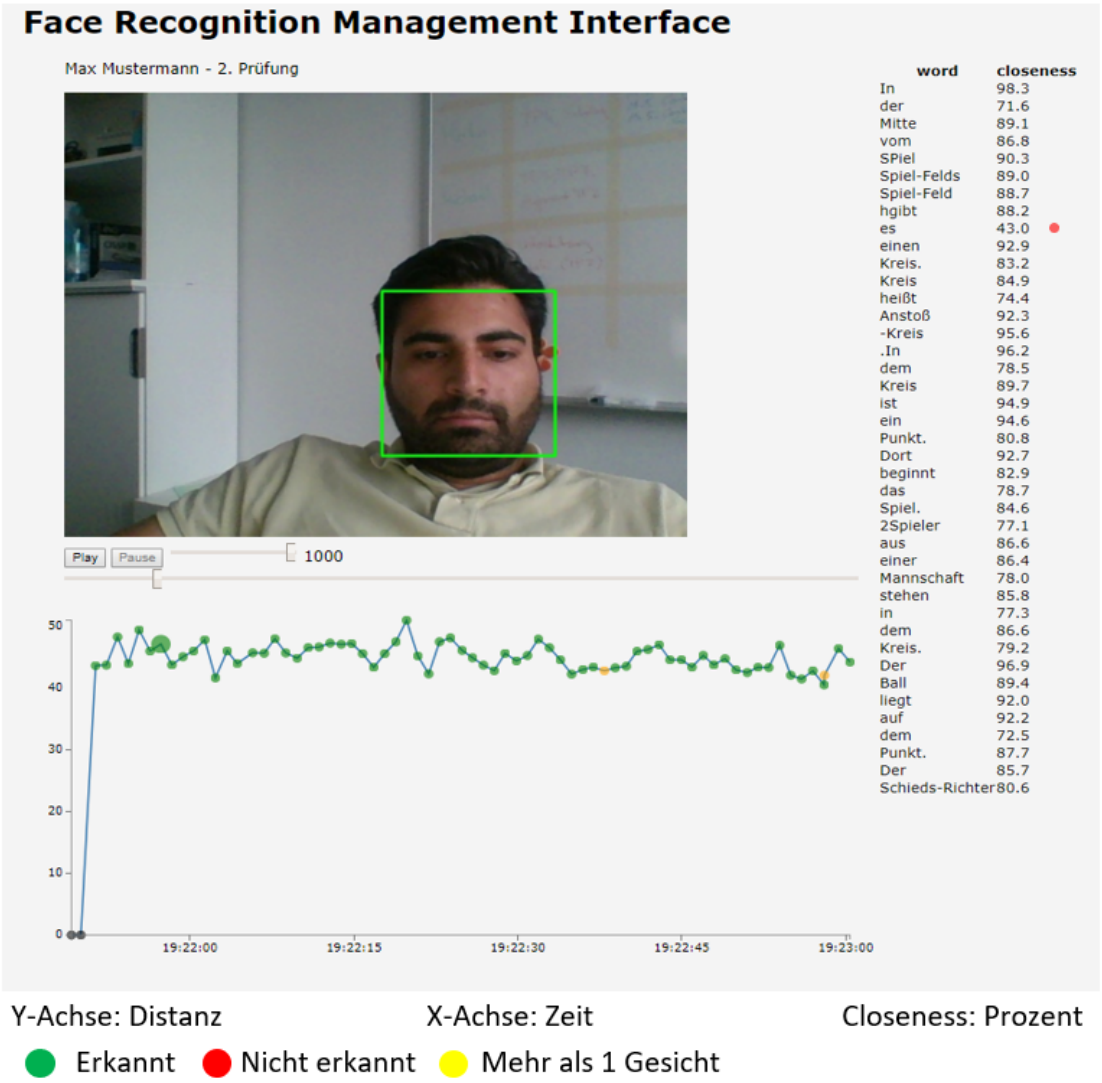


Abbildung 7.3: Unauffällige Werte bei Szenario 2

8 Zusammenfassung und Ausblick

8.1 Zusammenfassung

Das Ziel dieser Arbeit, ein Konzept für ein generisches und modulares Systems für die Abnahme von Online Prüfungen zu erarbeiten, wurde erreicht. Mit Hilfe einer fundierten Anforderungsanalyse konnten aus Anwendungsfällen, Prüfungsordnungen, Täuschungsszenarien und Informationssicherheitsaspekten 17 Rollen und fünf Gruppen sowie 100 Anforderungen identifiziert werden. Die Anforderungen wurden durch eine Expertenumfrage evaluiert und anschließend für die Konzipierung eines Systems zur sicheren computergestützten Abnahme von Online Prüfungen genutzt. Das Konzept wurde dann mit Hilfe von Moodle, OpenCV und Tappy.js in eine beispielhafte Implementierung überführt. Der Prototyp kann das Gesicht und Tippverhalten eines Nutzers kontinuierlich authentifizieren. Die Ergebnisse der Authentifizierung können durch die Reportingschnittstelle betrachtet werden. Ein Probandentest hat die Funktionsfähigkeit des Systems untersucht. Täuschungsversuche konnten zuverlässig enttarnt werden.

8.2 Ausblick

Im Zuge der Konzeption ist auch ein Framework entstanden, mit welchem weitere Methoden für die kontinuierliche Authentifizierung implementiert werden können. So können in einer zukünftigen Arbeit weitere Module und APIs wie die Erkennung des Scrollingverhaltens oder der Stimme umgesetzt werden. Aber auch die bereits implementierte Gesichtserkennung kann mit Hilfe von neueren Technologien wie der Tiefenerkennung einer 3D-Kamera bezüglich der Zuverlässigkeit verbessert werden. Außerdem kann ein Test unter realen Umständen , z.B. im Rahmen einer Übungsklausur, Aufschluss darüber geben, ob ein Einsatz des Systems im alltäglich Lehrbetrieb praktikabel wäre. Vergleichsstudien zwischen der Sicherheit von Online Prüfungen und Präsenzprüfungen können zeigen, welche Form der Prüfung einen besseren Schutz gegen Täuschungen bietet. Des Weiteren sollten die datenschutzrechtlichen Aspekte der Online Prüfungen untersucht werden, da über das System personenbezogene Daten erhoben und verarbeitet werden.

Abbildungsverzeichnis

Literaturverzeichnis

[ARC09] Agulla, Elisardo Gonzalez, Enrique Argones Rua und Jose Luis Alba Castro: *Multimodal Biometrics-based Student Attendance Measurement in Learning Management Systems*. 2009.

[Bra17] Braden, Peter: *opencv*, Februar 2017. `https://www.npmjs.com/package/opencvr`.

[Bun16] Bundesamt, Statistisches: *Personal an Hochschulen*, Dezember 2016. `https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/BildungForschungKultur/Hochschulen/Tabellen/PersonalGruppen.html;jsessionid=B31F0C190F2E2DB2DA33435EA2C44C82.cae4`.

[Bun17] Bundesamt, Statistisches: *Zahl der Studierenden steigt im Wintersemester 2016/2017 weiter an*, Februar 2017. `https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2016/11/PD16_417_213.html;jsessionid=B31F0C190F2E2DB2DA33435EA2C44C82.cae4`.

[CJER11] Cluskey Jr., G. R., Craig R. Ehlen und Mitchell H. Raiborn: *Thwarting online exam cheating without proctor supervision*. Journal of Academic and Business Ethics, 4:4–6, 2011.

[d3117] *Data-Driven Documents*, September 2017. `https://d3js.org/`.

[Eck12] Eckert, Claudia: *IT-Sicherheit*. Oldenburg Verlag, München, 7. Auflage, 2012.

[fer17] *Fernuniversität Hagen*, September 2017. `http://www.fernuni-hagen.de/mathinf/studium/studiengaenge/diplom/informatik/anmeldeformulare_diplinf.shtml`.

[GRGA15] Gy?rödi, Cornelia, Gy?rödi Robert, Pecherle George und Olah Andrada: *A comparative study: MongoDB vs. MySQL*, 2015.

[ire17] *IREB*, November 2017. `https://www.ireb.org/de`.

[IUB16] IUBH: *Fernstudium mit Online-Klausur: neue Technik macht Prüfungen zeitlich und räumlich völlig flexibel*, November 2016. `http://www.iubh.de/2016/11/30/fernstudium-mit-online-klausur/`.

[Jon01] Jones, Viola: *Rapid Object Detection using a Boosted Cascade of Simple Features*, 2001.

[KAK10] Karnan, M., M. Akila und N. Krishnaraj: *Biometric personal authentication using keystroke dynamics: A review*, 2010.

[KS15] Karim, Nader Abdel und Zarina Shukur: *Review of User Authentifaction Methods in Online Examination*, 2015.

[lmu17] *LMU*, September 2017. https://www.uni-muenchen.de/studium/studienangebot/studiengaenge/studienfaecher/informatik/bachelor/pruefstudord/index.html.

[MDRH14] Migicovsky, Alex, Zakir Durumeric, Jeff Ringenberg und Alex J. Halderman: *Outsmarting Proctors with Smartwatches: A Case Study on Wearable Computing Security.* Proc. 18th Intl. Conference on Financial Cryptography and Data Security, 2014.

[MfI16] Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfalen Ministerium für: *Landesinterne Umsetzung des Hochschulpakts 2020 durch die Hochschulen des Landes Nordrhein-Westfalen im Jahr 2015*, November 2016. http://www.wissenschaft.nrw.de/fileadmin/Medien/Dokumente/Hochschule/Bericht_Monitoring_2016.pdf.

[mIT16] mITSM: *ISO/IEC 27000(R) Foundation V. 2.4*, 2016.

[mon17] *MongoDB*, September 2017. https://www.mongodb.com/.

[OG16] Oevel, Gudrun und Lange Gerald: *Umfrage des ZKI-AK E-Learning, welche Lernmanagementsysteme eingesetzt werden.*, Dezember 2016. http://doodle.com/poll/uyvcg2wz6s4bwv6v.

[Ope17] Opencv.org: *OpenCV Homepage*, Februar 2017. http://www.opencv.org.

[Pea17] PearsonVue: *Homepage PearsonVue*, Februar 2017. https://home.pearsonvue.com/.

[Per08] Perrin, Chad: *The CIA Triad.* http://www.techrepublic.com/blog/it-security/the-cia-triad/, 2008. Aufgerufen am: 2016-03-10.

[Pro17] ProctorU: *Homepage ProctorU*, Februar 2017. https://www.proctoru.com/.

[Que17] Questionmark: *Homepage Questionmark*, Februar 2017. https://www.questionmark.com/.

[Row04] Rowe, Neil C.: *Cheating in Online Student Assessment: Beyond Plagiarism.* Online Journal of Distance Learning Administration, 7, 2004.

[Rup16] Rupp, Michael: *Unsichtbares Mini-Headset fürs Handy*, November 2016. http://www.com-magazin.de/news/mobile-geraete/unsichtbares-mini-headset-fuers-handy-192896.html.

[Sec17] Secure, Software: *Homepage Software Secure*, Februar 2017. http://www.softwaresecure.com/.

[SGLPS80] Stockton Gaines, R., William Lisowsko, S. James Press und Norman Shapiro: *Authentication by keystroke timing: Some preliminiary results*, 1980.

[She95] Shepherd, S. J.: *Continuous authentication by analysis of keyboard typing characteristics*, 1995.

[SI13] Sarrayrih, Mohammad und Mohammed Ilyas: *Challenges of Online Exam, Performances and problems for Online University Exam*, 2013.

[Sob16] Sobiraj, Lars: *Digitale Spickzettel Schummeln mit Smartwatches*, November 2016. https://www.golem.de/news/digitale-spickzettel-schummeln-mit-smartwatches-1312-103183.html.

[Spy16] Spyshop: *CM-SG20 Spionage Brille für Hobbydetektive mit langer Betriebszeit*, November 2016. http://www.spyshop.berlin/kleine-spionagekamera-in-einer-brille-cm-sg20-fuer-einen-detektiv-625.html.

[Tag15] Tagesschau: *Online-Kurse von Unis in der Kritik - Massig Daten von Studenten*, Dezember 2015. https://www.tagesschau.de/inland/moocs-113.html.

[uni17] *Universität Köln*, September 2017. http://www.mi.uni-koeln.de/home-institut/alle/Lehre-Studium/Informationen_zum_Studium/Studien_und_Pruefungsordnungen.de.html.

[Wan16] Wannemacher, Klaus: *Organisation digitaler Lehre in den deutschen Hochschulen*, Juni 2016. http://www.iubh.de/wp-content/uploads/sites/10/2016/11/HFD_AP_Nr21_Organisation_digitaler_Lehre_web.pdf.

[wes17] *Westfälische Universität*, September 2017. https://www.uni-muenster.de/imperia/md/content/wwu/ab_uni/ab2014/ausgabe26/beitrag01.pdf.

[wgu17] *Goethe-Universität*, September 2017. https://www.informatik.uni-frankfurt.de/index.php/de/.

[Wie16] Wiesbaden, Statistisches Bundesamt: *Bildung und Kultur - Studierende an Hochschulen*, März 2016. https://www.destatis.de/DE/Publikationen/Thematisch/BildungForschungKultur/Hochschulen/StudierendeHochschulenVorb2110410168004.pdf?__blob=publicationFile.

[wik76] *Liste der Hochschulen in Deutschland*, Juni 20176. https://de.wikipedia.org/wiki/Liste_der_Hochschulen_in_Deutschland.