Hochschule Worms

Fachbereich Informatik

Studiengang Angewandte Informatik B.Sc.

Gewährleistung von sicherem digitalen Bezahlen bei einem Click-and Buy-Automat

Exposé für Wissenschaftliches Arbeiten

Bruno Macedo da Silva und Dominic Meyer

Betreuer	Michael Derek Werle-Rutter
Bearbeitungszeitraum:	Wintersemester 2021/2022
Abgabedatum:	8.Februar 2022

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung

Seit einigen Jahren entscheiden sich immer mehr Menschen Urlaub auf einem Campingplatz zu machen [Graefe, 2021a]. Der Gedanke an Menschenmassen und Fallen für Touristen schreckt die Leute von den typischen Touristenzielen ab. Zudem ist der Kontakt zu der Natur für viele ein wichtiger Teil in einem Urlaub. In den letzten anderthalb Jahren stieg die Anzahl von Campinplatzbesuchern rasant [Graefe, 2021c]. Die Corona-Pandemie drängte die Leute dazu, Urlaubsmöglichkeiten zu suchen, bei denen das Risiko von einer Infektion niedrig sei und wo genug Abstand gehalten werden könne [Graefe, 2021b]. Da viele Hotels und andere Ferieneinrichtungen geschlossen waren, blieb vielen Leuten, besonders Familien, nichts anderes übrig, als die Ferien etwas anders zu organisieren und gestalten

(hier können wir vielleicht schreiben, dass durch Corona immer weniger Leute wegfliegen wollten und deshalb lieber mit dem Auto weggefahren sind). (Die Statistik von dem vorherigen Punkt, können wir hier vielleicht auch vewenden).

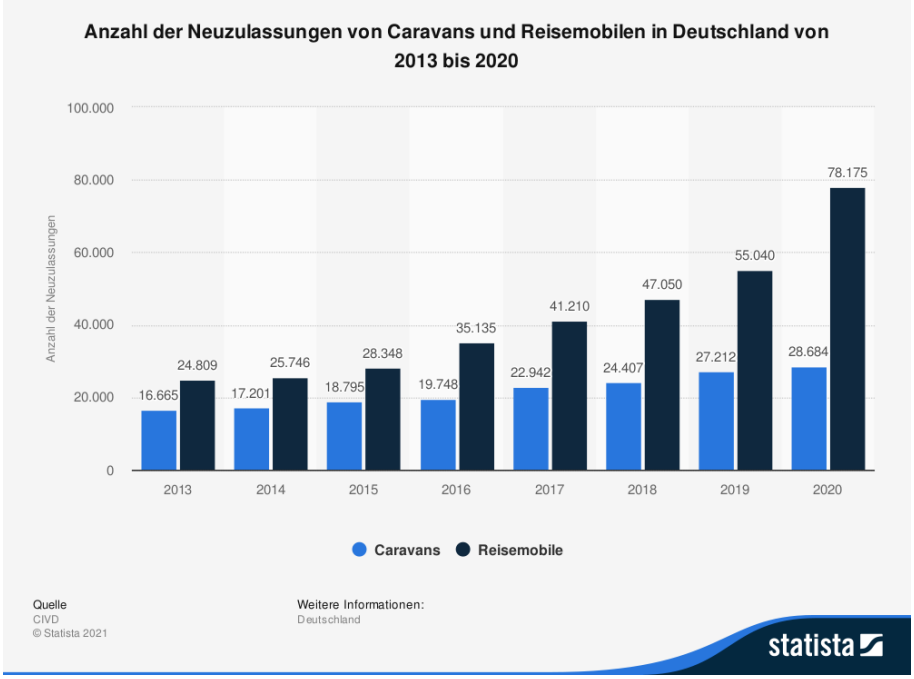

Abbildung 1: Neuzulassungen von Caravans und Reisemobilen (2013-2020) [Graefe, 2021c]

Die traditionelle Idee von Campingplätzen, bei der Jugendliche oder Familien weit entfernt von der Gesellschaft sind, ist heute eine andere. Heute wollen Urlauber auf den Kontakt mit der Natur möglichst nicht verzichten, wodurch Campingplätze immer voller werden. Aus diesem Grund wäre es sinnvoll, die Möglichkeiten zur Grundversorgung zu erweitern, ohne direkt einen neuen Supermarkt bauen zu müssen. In dieser Hinsicht kann die Einrichtung eines elektronischen Click-and-Buy-Automaten [1], der mit einem Automaten zu vergleichen ist, eine wesentliche Rolle spielen, um einen Campingplatz und die Gegend drum herum zu modernisieren, die Möglichkleiten zur Grundversorgung zu erweitern und ihn attraktiver für Reisende und die Leute auf dem Land zu machen.

[1] Die Waren werden online bezahlt und zu einem gewünschten Zeitpunkt können sie angeholt werden [Ghosh and C., 2014].

Die Sicherheit der digitalen Zahlungsmethoden stellt eines des wichtigsten Punkte für die Entwicklung eines solchen Systems dar. Vernachlässigungen in diesem Bereich führen zu unberechenbaren Vertrauensverlust seitens der potenziellen Nutzenden und zu finanziellen und moralischen Schäden der direkten Stakeholder. Die geplante Wissenschaftliche Arbeit soll folgende Frage behandeln: Wie kann sicheres bargeldloses Bezahlen in einem Click-and-Buy-Automat gewährleistet werden?

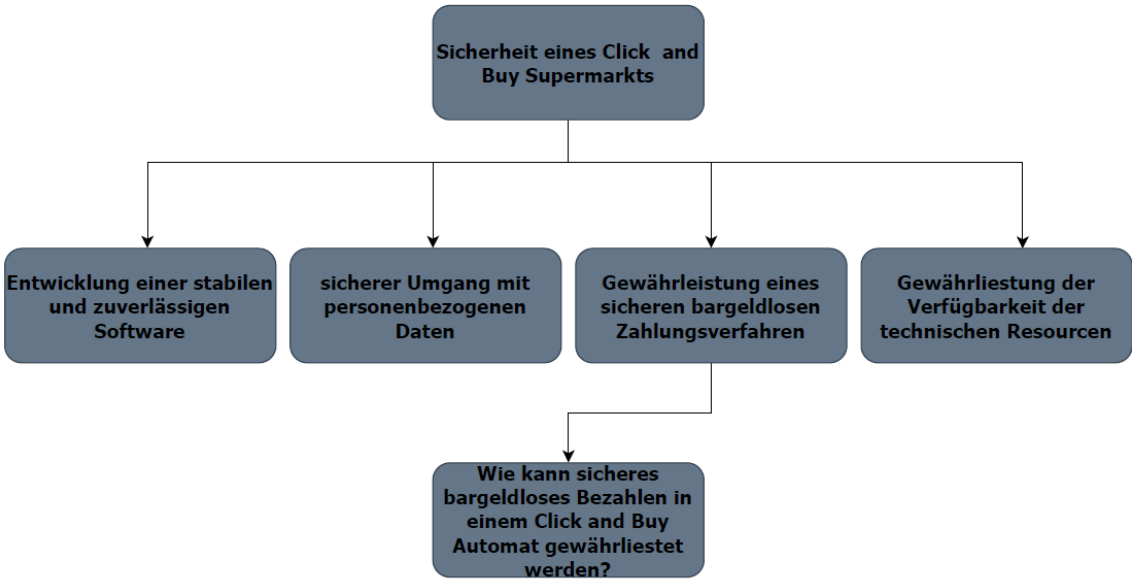

Abbildung 2: Forschungsfrage (eigenes Bild)

2 Forschungsziele

In der geplanten Wissenschaftlichen Arbeit, soll ein Konzept für ein Click-and-Buy-Automat direkt neben dem Campingplatz entwickelt werden. Solch ein Konzept kann dazu beitragen, dass Campingplätze und die Gegend modernisiert werden und noch mehr Touristen angelockt werden. Bevor das Projekt jedoch umgesetzt werden kann, müssen noch wichtige Dinge beleuchtet werden.

Ziel der geplanten Untersuchung ist es, einen elektronischen Supermarkt zu entwickeln, jedoch müssen vorher einige Voraussetzungen erfüllt werden. Der Zugang zum Netzwerk über das Glasfaser sollte immer gewährleistet werden, eine stabile Software, die den Qualitätsstandards entspricht, ein sicherer Umgang mit Kundendaten, der sich an spezifischen und internationalen Richtlinien[2] orientiert, ein benutzerfreundliches System, das sich an verschiedenen Kundentypen, wie Alters- und Bildungsgruppe anpasst und letztlich ein kryptographisches Verfahren[3] für das bargeldlose Bezahlen, das die Vertraulichkeit sicherstellt.

Um die Verfügbarkeit des Netzwerkzugangs für den Click-and-Buy-Automat zu gewährleisten, muss zum einen geprüft werden, ob die bereits vorhandenen Leitungen ausreichen, um solch ein Projekt umsetzen zu können. Die Vernetzung soll so aufgebaut sein, dass es auch in remoten Regionen einwandfrei funktioniert. Die Software muss zudem so entwickelt werden, sodass diese eine geringe Ausfallquote aufweist, denn der Automat soll rund um die Uhr betriebsbereit sein, um das Ziel der Verfügbarkeit des Systems nicht zu verletzen [Wendzel, 2018].

[2] Es gibt Regeln, die aussagen, was mit personenbezogenen Daten passieren darf und was nicht [Datenschutz, 2021].

[3] Mit Hilfe kryptographischer Verfahren wie Verschlüsselung sollen Daten vor unbefugtem Zugriff geschützt und sicher ausgetauscht werden [Luber and Schmitz, 2017].

Zudem soll das System so entwickelt werden, sodass auch Digital Non-Natives[4], die Möglicheit [Wang et al., 2013] haben das System einfach bedienen zu können. Die Kunden sollten also nicht von Informationen überladen werden, sondern es sollte einfache Ein- und Ausgaben geben. Da sich besonderes ältere Menschen für solch eine Urlaubsmöglichkeit entscheiden, spielt es für den Erfolg des Konzeptes eine entscheidene Rolle, dass auch sie mit dem Automaten umgehen können. Deshalb sollten die Bedürfnisse und Einschränkungen dieser Altergruppe besonders berücksichtigt werden, um ihr Vertrauen zu gewinnen [Lübbecke, 2018] und hauptsächlich gegen Social-Engineering[5] Angriffe zu schützen. Die Auswahl der Tests trägt dazu bei, dass die Zufriedenheit und die Akzeptanz gewährleistet wird, sodass jeder potenziellen Endnutzer das System bedienen kann [Sommerville, 2010].

Außerdem spielt die Sicherheit bei den bargeldlosen Zahlungsvorgängen eine große Rolle und sollte deshalb höchste Priorität haben. Verschiedene aktuelle Beispiele von Cyberangriffe zeigen, dass der Umgang mit solchen Daten, kritisch zu sehen ist [Bundeskriminalamt, 2020].

Es wird oft von Situationen in den Medien berichtet, bei denen Kunden ihr Geld verloren haben oder dessen personenbezogenen Daten missbraucht wurden. In seltenen Fällen sogar von der eigenen Regierung, weil das System nicht ausreichend gegen Angriffe geschützt wurde. In dieser Hinsicht sollten bei der Entwicklung spezifische und klare Richtlinien berücksichtig werden, sodass der sichere Umgang mit personenbezogenen Daten gewährleistet ist [Riebe et al., 2020]. Um diese Vertraulichkeitsverletzung zu vermeiden, spielt die Konziperiung von sicheren bargeldlosen Zahlungsmethoden eine wesentliche Rolle in diesem Artikel.

[4]Bezeichnet eine Person, die in der Kindheit ohne Informationstechnologien und ohne dem Internet aufgewachsen ist und eine welt mit digitalen Medien nicht kennt [Siepermann, 2018].

[5]Beim Social-Engineering nutzt der Täter den “Faktor Mensch” als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen.[Bundesamt für Sicherheit in der Informationstechnik, 2020]

Da das gesamte Thema sehr umfangreich ist, soll hier hauptsächlich die folgende Frage behanldet werden: Wie kann sicheres bargeldloses Bezahlen in einem Click-and-Buy-Automat gewährleistet werden?

3 Stand der Forschung

Im folgenden Abschnitt behandeln wir Wissenschaftliche Literatur zum Thema sichere bargeldlose Zahlungsverfahren. Zusätzlich beleuchten wir die Entwicklung vom bargeldlosen Bezahlen in Deutschland und die daraus resultierenden Schwachstellen und Schutzmechanismen.

3.1 Chanchen und Risiken vom bargeldlosen Bezahlen

Die zunehmende Tendenz in Deutschland von bargeldloser Bezahlung erfordert neuen Umgang mit den eigegebenen Daten. Eine Studie von 2009 der Deutschen Bundesbank zeigte den rasanten Anstieg von bargeldloser Bezahlung in der Bundesrepublik seit der Einführung von solchen Zahlungsmethoden [Bundesbank, 2009].

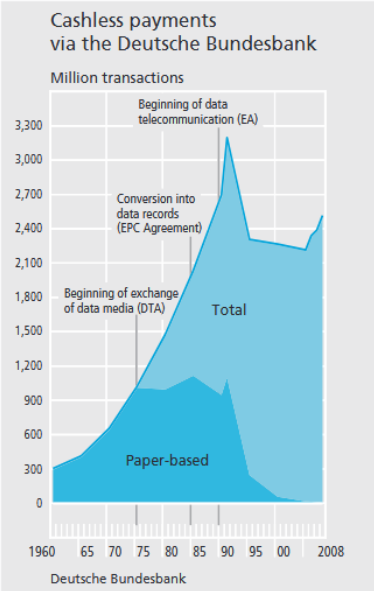

Abbildung 3: Cashless payments via the Deutsche Bundesbank (Bundesbank, 2009, S.52)

Laut einer Statistik des Handelsforschungsinstituts EHI von 2019 [Seibel, 2019] bezahlen 48,6% der deutschen ihre Waren mit Karte, wohingegen nur noch

46,9% der deutschen den klassischen Weg über Bargeld gehen. Auch das kontaklose Bezahlen, bei dem kleine Beträge nicht einmal mit einer PIN bestätigt werden müssen, nimmt immer weiter zu. Doch gerade bei dieser Variante ist es sehr einfach im Namen eines anderen zu bezahlen, was eine Sicherheitsrisiko darstellt. Diese Tendenz wurde auch von [Dahlberg et al., 2008] in seiner Studie beobachtet, bei der er die meist verbreiteten Zahlungsarten in verschidenen Regionen dieser Welt vergleicht.

Immer wenn mit Karte bezahlt wird, gehen die Kunden davon aus, dass die Zahlungsabwicklung sicher ist. Wie sicher ist das bargeldlose Zahlen heutzutage wirklich?

3.2 IT-Schutzziele vom bargeldlosen Zahlungsverfahren

Vertraulichkeit ist die erste und wichtigste Voraussetzung, das ein solches Zahlungssystem erfüllen muss, um neue potenzielle Kunden zu gewinnen. Unter diesem Begriff Vertraulichkeit verstehen wir, dass es keine unautorisierte Informtionsgewinnung gibt [Wendzel, 2018] .Unter diesem Begriff soll ein System nur auf autorisierte Informationen zugreifen. In dieser Hinsicht ist die Entwicklung einer Click-and-Buy-Automat so zu konzipieren, dass sie einen sicheren Umgang mit den Kundendaten anbietet. Die Interaktion zwischen einem Kunden und systemkritischen Mechanismen wurde von [Hassan et al., 2020] so dargestellt:

Um das IT-Sicherheitsziel der Vertraulichkeit zu gewährleisten, sollten einige Schritte berücksichtigt werden. Im ersten Schritt, sendet der Client, also der Nutzer seinen Namen, generiert einen Session Key und sendet eine Anfrage für eine Transaktion. Diese Anfrage wird daraufhin an den Händler geschickt,der diese wiederrum bearbeitet [Isaac and Zeadally, 2012]. Nachdem das abgeschlossen wurde, sendet der Händler seine Antworz an das Bezahlgerät, das wiederrum die Antwort an den Client weiterleitet. Im zweiten Schritt

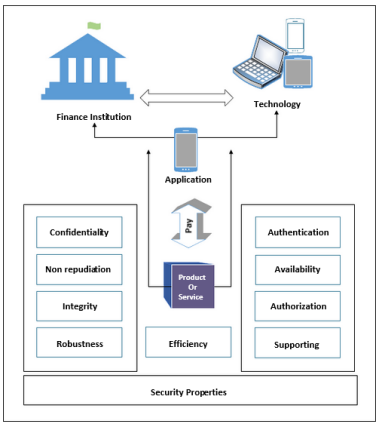

Abbildung 4: Sicherheitseigenschaften von digitalen Zahlungsmethode (Hassan et al. 2020, S8)

wird die eigentliche Bezahl Anfrage an das Bezahlgerät gesendet, die unter anderem den Preis und die Uhrzeit enthält. Das Bezahlgerät leitet die empfangene Nachricht an den Händler weiter. Dieser empfängt die Daten und prüft auf Aktualität der Daten. Wenn dieser Test erfolgreich war, wird wieder eine Nachricht an das Bezahlgerät geschickt. Dieses schickt die Daten dann wiederrum an die Bank, welche überprüft, ob das Geld von dem Konto abgebucht werden kann oder nicht. Wenn das geprüft wurde, wird eine Nachricht an das Bezahlgerät gesendet, in der steht, dass das Geld abgebucht wurde. Hinzuzufügen ist, dass bei jeder Kommunikation die Daten verschlüsselt werden, sodass es einem potenziellen Angreifer nicht möglich ist, Daten zu ändern oder zu entschlüsseln. In der Folgenden Abbildung wird da oben genannten Verfahren dargestellt:

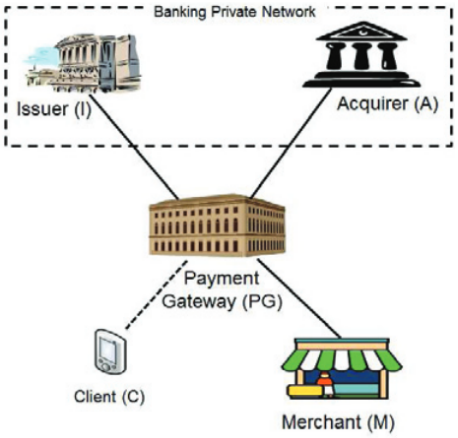

Abbildung 5: Muster für den Payment Gateway Centric Scenario[Isaac and Zeadally, 2012]

Das folgende Sequenzdiagramm[6] stellt den Nachrichtenaustausch zwischen den Elemeten dieser Zahlungsmethode dar:

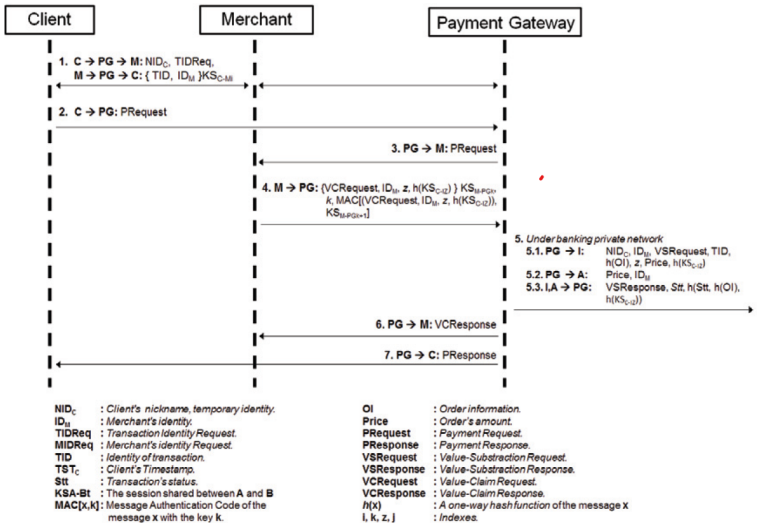

Abbildung 6: Nachrichtenflussaustausch [Isaac and Zeadally, 2012]

[6]Ein Sequenzdiagramm ist ein Verhaltensdiagramm, welches eine Interaktion im Sinne der Unified Modeling Language (UML) grafisch darstellt [Sommerville, 2010]

Zudem sollten die weiteren Schutzziele der IT-Sicherheit: Integrität, Verfügbarkeit und Authentizität berücksichtigt werden, sodass die Systeme einwandfrei und sicher funktionieren [Me, 2003]. Eine Zahlungsmethode, bei der alle Vorraussetzungen erfüllt werden, kann in der Lage sein, das Vertrauen und die Akzeptanz von den Nutzenden zu bekommen [Hassan et al., 2020]. Besonders im deutschen Markt, spielen die oben genannten Schutzziele eine wesentliche Rolle [Khodawandi et al., 2003], da sie ein Entscheidungsfaktor dafür sind, ob ein System genutzt wird oder nicht.

Da es um einen dynamischen und breiten Bereich geht, bei dem es sehr schnell zu Änderungen kommen kann, besonders bei den Angriffstechniken, müssen die dazu gehörige [Yildirim and Varol, 2019] Technologie stets weiterentwickelt und angepasst werden, um Vertraulichkeitsverlust seitens der Kunden zu vermeiden. Da die Vertraulichkeit noch nicht zu 100 Prozent gewähleistet werden kann, verweigern viele Kunden das bargeldlose Bezahlen.

Viele Studien befassen sich mit den verschiedenen Aspekten der Sicherheit bei bargeldlosen Zahlungsmethoden. Die Literatur dieses Forschungsfeldes ist sehr umfangreich und kümmert sich um die Vielfältigkeit dieser heterogen [Me, 2003] Umgebung. Im nachfolgenden Artikel sollen zwei dieser Technologien in Bezug auf Angriffstechniken und Gegenmaßnahmen genauer betrachtet werden.

4 Stand der Technik

Für die Bezahlungsmethoden werden hier zweiverschiedene Arten von Zahlungsverfahren analysiert und deren Vorteile in Bezug auf Sicherheit und Härtungsmaßnahmen dargestellt: drahtlose Zahlung und Kartenzahlung.

4.1 Drahtlose Verbindungen und Sicherheit bei Bezahlungen

Viele digitale Zahlungen finden über WLAN statt, was ein großes Risiko darstellen kann [Yildirim and Varol, 2019], da WLAN-Verbindungen nicht so sicher sind wie Kabelverbindungen. Maßnahmen zu entwickeln, die sich an verschiedenen Systeme anpassen, kosten Zeit und Investitionen von Banken und Sicherheitsfirmen. Für jeden möglichen Angriffe sollte präventiv etwas getan werden, sodass die Integrität des Kunden geschützt bleibt. Die folgenden Schwachstellen bei digitaler Zahlung wurden von [Yildirim and Varol, 2019] zusammengefasst:

- Erstellung von Dateien in dem Opfersystem mit umfangreichen Privilegien
- unzureichende Sicherheit bei der Validierung von Zertifikaten
- Quellcode ist öffentlich zugänglich, sodass das Opfersystem von Reverse Engineering betroffen sein könnte
- Unsicherer Umgang mit Cookies-Einstellungen.

[Yildirim and Varol, 2019] schlägt einige Sicherheitsmechanismen vor, die die oben gennanten Schwachstellen bei kabelosen Verbindungen reduzieren können. Unter denen werden folgende hervorgehoben:

- Nutzung von modernen kryptographischen Standards für die Validierung von Zertifikaten

- Erstellung von Loggdatei, sodass jeder Anormalität schnell überprüft werden kann
- Zwei-Faktor-Authentifizierung
- digitale und zufällig geordnete Tastatur
- Schwierigkeitsgrad bei der Erstellung von Passwörtern
- besserer Umgang mit der Verwaltung von Cookies
- Registrierung von Geräten
- künstliche Intelligenz (KI) für die Detektion von abweichenden Verhalten
- ständige Kontrolle gegen Social Engineering **Fußnote**. Ich denke wir haben weiter oben schon eine Fußnote zum Social Engineering, sollen wir hier die selbe verwenden?

Testen, interviewn, testen. diese ist gut, weil, weil weil

Kredit- und EC-Karten sollen auch als Zahlungsmittel bei unserem Click-and-Buy-Automat akzeptiert werden. In Bezug auf diese Zahlungsmittel, wird die Sicherheit im folgenden untersucht.

4.2 Anwendung von Smartcards und sicheres Bezahlen

Der Begriff Smartcards bezeichnet eine Plastikkarte mit einem eingebauten Chip, der ein eigenes Betriebssystem, einen Mikroprozessor und minimale Funktionalitäten besitzt. Im folgenden ist ein Beispiel von einer Smartcard zu sehen:

Abbildung 7: Eine Smartcard und deren eingebetete Mikrochip
(eigene Quelle)

Sie wurde vor mehr als 40 Jahren erfunden und ihr Ziel ist die Sicherheit von Kartenzahlung und allgemeine Authentifizierungsverfahren zu erhöhen [Farrell, 1996]. Sie unterscheiden sich von traditionelen Magnetstreifenkarten, weil sie verschiedene Authentifizierungsmethoden ermöglichen auch ohne direkte Verbindung zur Bank [Tanembaum, 2009]. Im folgenden wird der Authentifizierungsprozess einer Smartcard 8 dargestellt.

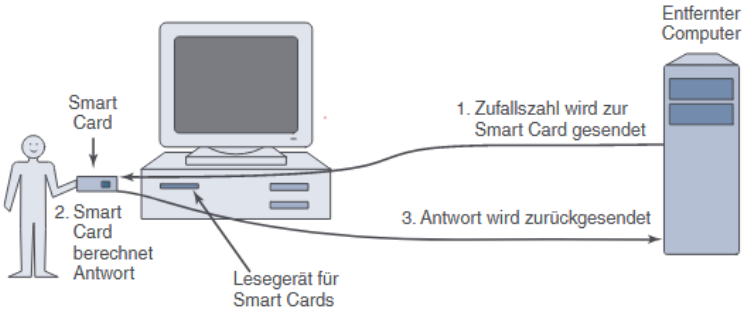

Abbildung 8: Authentifizierungsprozess von Smartcards
(Tanenbaum, 2009, S.755)

Die meisten Angriffe bei Smartcards geschehen laut [Steffen, 2012] auf Hardwareebene. Er beschreibt folgende Techniken für Angriffe:

- Protokollanalyse: schwache Konzipierung oder mangelnde Verschlüsselung ermöglichen den Zugang zu dem Klartext;
- Relay: Konzentriert auf kontaktlose Smartcards, um den Inhalt umzuleiten;
- Seitenkanal-Attacken: zielt nicht direkt den Inhalt des Kommunikation, sondern versucht sie irgendwie zu stören;
- Hardware Reverse Engineering: Verständnis über die Algorithmen oder Extrahieren des Schlüssels.

Die Schutzmaßnahmen können laut [Steffen, 2012] in drei Gruppen aufgeteilt werden: physikalisch, logisch und organisatorisch. Auf der physikalischen Ebene soll die Hardware rrobustäufgebaut werden, um Angriffe schwieriger zu gestalten. Diese Konstruktion soll komplex mit zusätzlichen Elementen erstellt werden.

Letztendlich sollen Smartcards in der Lage sein, Angriffe schnell zu detektieren und zu verhindern. Zu dieser Ebene gehört auch das Sperren der Karte, falls die Karte unautorisiert genutzt wurde, die Überprüfung von Logdateien, um Klone zu identifizieren und die Verwendung von Zwei-Faktor- Authentisierung.

5 Forschungsplan

Die Literatur bezüglich Netzwerksicherheit, bargeldlose Zahlungsverfahren und Vending Machines ist in den letzten 20 Jahren deutlich umfangreicher geworden. Da diese Begriffe viele und fast unendliche Konzepte decken, gehen wir hier auf spezifische Aspekte dieser Begriffe ein und zwar auf die Sicherheit von drahtlosen Zahlungsmethode und von Smartcards. Folgende Quelle tragen zu der Suchen nach vertrauenswürdigen Informationen bei:

- ScienceDirect
- Researchg Gate
- IEEE Xplore
- Google Scholar.

Die Recherche fasst sich hauptsächlich in der Sammlung aus dem spezialisierten Literatur von Konzepten, Sicherheitslücken und Gegenmaßnahmen von den oben genannten Elementen zusammen:

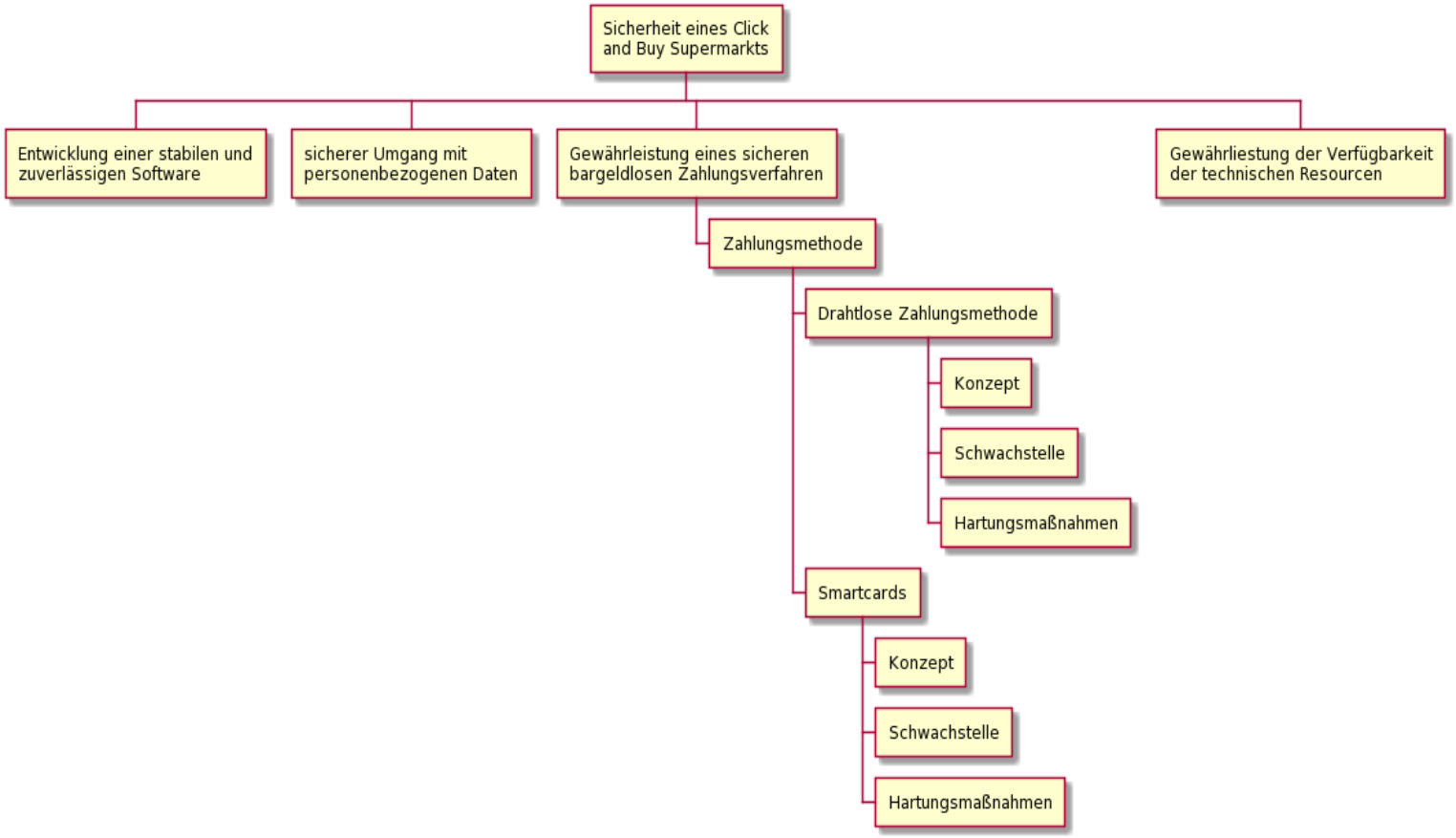

Abbildung 9: Forschungsfrage (eigenes Bild)

6 Praktische Relevanz

Keine Ahnung.

Mit der erfolgreichen Implementierung des xxxxxxxx können wir folgenden Ziele innerhalb eines Unternehmens erreichen: Meine Liste PUNKT:

- Punkt 1
- Punkt 2
- Punkt 3
- Punkt 4

Literaturverzeichnis

[Aquilina and Saliba, 2019] Aquilina, Y. and Saliba, M. A. (2019). An automated supermarket checkout system utilizing a SCARA robot: preliminary prototype development. *Procedia Manufacturing*, 38:1558–1565. 29th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM 2019), June 24-28, 2019, Limerick, Ireland, Beyond Industry 4.0: Industrial Advances, Engineering Education and Intelligent Manufacturing.

[Bankar, 2019] Bankar, S. (2019). Automated Supermarket Run System. *Journal of Advanced Research in Embedded System*, 6(3 and 4). https://thejournalshouse.com/index.php/ADR-Journal-Embedded-Systems/article/view/223.

[Bremser et al., 2019] Bremser, C., Piller, G., and Rothlauf, F. (2019). How Smart Cities Explore New Technologies. In Pankowska, M. and Sandkuhl, K., editors, *Perspectives in Business Informatics Research - 18th International Conference, BIR 2019, Katowice, Poland, September 23-25, 2019, Proceedings, series=Lecture Notes in Business Information Processing*, volume 365, pages 1–15. Springer. https://doi.org/10.1007/978-3-030-31143-8_1.

[Bundesamt für Sicherheit in der Informationstechnik, 2020] Bundesamt für Sicherheit in der Informationstechnik (2020). Social Engineering – der Mensch als Schwachstelle. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html.

[Bundesbank, 2009] Bundesbank, D. (2009). Cashless payments in Germany and the role of the Deutsche Bundesbank: Developments and key trends over the past 50 years. *Deutsche Bundesbank Eurosystem - Monthly Report*.

[Bundeskriminalamt, 2020] Bundeskriminalamt (2020). Cybercrime Bundeslagebild 2020. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html;jsessionid=1A921B916A930B1DEB3130BCF4399153.live291?nn=28110.

[Dahlberg et al., 2008] Dahlberg, T., Mallat, N., Ondrus, J., and Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications*, 7(2):165–181. https://doi.org/10.1016/j.elerap.2007.02.001.

[Datenschutz, 2021] Datenschutz (2021). Datenschutz im Internet: Privatsphäre als höchstes Gut bewahren. *Datenschutz.org*. https://www.datens

chutz.org/datenschutz-im-internet/.

[Dijaya et al., 2019] Dijaya, R., Suprayitno, E., and Wicaksono, A. (2019). Integrated Point of Sales and Snack Vending Machine based on Internet of Things for Self Service Scale Micro Enterprises. *Journal of Physics: Conference Series*, 1179:012098. http://dx.doi.org/10.1088/1742-6596/1179/1/012098.

[Dullien, 2018] Dullien, T. (2018). Maschinelles Lernen und künstliche Intelligenz in der Informationssicherheit. *Datenschutz und Datensicherheit - DuD*, 42(10):618–622. https://doi.org/10.1007%2Fs11623-018-1012-3.

[Farrell, 1996] Farrell, J. (1996). Smartcards become an international technology. In *Proceedings 13th TRON Project International Symposium /TEPS '96*, pages 134–140. https://doi.org/10.1109/TRON.1996.566204.

[Ghosh and C., 2014] Ghosh, P. and C., C. (2014). E-commerce: 'click and buy' – an easy way of shopping (with respect to indian market). *International Journal of Innovative Research Development*, 3:416–431. http://52.172.159.94/index.php/ijird/article/viewFile/58573/45795.

[Gomm et al., 1997] Gomm, G. R., Paul, G. R. G., and Paul, S. (1997). Cash alternative transaction system. https://www.freepatentsonline.com/5650761.html.

[Graefe, 2021a] Graefe, L. (2021a). Anzahl der Neuzulassungen von Caravans und Reisemobilen in Deutschland von 2013 bis 2020. https://de.statista.com/statistik/daten/studie/662102/umfrage/neuzulassungen-von-caravans-und-reisemobile-in-deutschland/.

[Graefe, 2021b] Graefe, L. (2021b). Anzahl der Übernachtungen von Gästen in Beherbergungsstätten in Deutschland von September 2019 bis September 2021. https://de.statista.com/statistik/daten/studie/73548/umfrage/uebernachtungen-in-beherbergungsstaetten-und-auf-campingplaetzen/.

[Graefe, 2021c] Graefe, L. (2021c). Übernachtungen in Beherbergungsstätten in Deutschland bis September 2021. https://de.statista.com/statistik/daten/studie/73548/umfrage/uebernachtungen-in-beherbergungsstaetten-und-auf-campingplaetzen/.

[Hassan et al., 2020] Hassan, M. A., Shukur, Z., Hasan, M. K., and Al-Khaleefa, A. S. (2020). A Review on Electronic Payments Security. *Symmetry*, 12:22. http://dx.doi.org/10.3390/sym12081344.

[Henze et al., 2017] Henze, M., Hiller, J., Hummen, R., Matzutt, R., Wehrle,

K., and Ziegeldorf, J. H. (2017). *Network Security and Privacy for Cyber-Physical Systems*, chapter 2, pages 25–56. https://doi.org/10.1002/9781119226079.ch2.

[Hiroyuki, 2004] Hiroyuki, U. (2004). Lowering elderly Japanese users resistance towards computers by using touchscreen technology. *Universal Access in the Information Society*, 3(3-4):276–288. https://www.proquest.com/scholarly-journals/lowering-elderly-japanese-users-resistance/docview/201543463/se-2?accountid=15921.

[Iqbal et al., 2012] Iqbal, Q., Whitman, L. E., and Malzahn, D. (2012). Reducing Customer Wait Time at a Fast Food Restaurant on Campus. *Journal of Foodservice Business Research*, 15(4):319–334. https://doi.org/10.1080/15378020.2012.706176.

[Isaac and Zeadally, 2012] Isaac, J. T. and Zeadally, S. (2012). An anonymous secure payment protocol in a payment gateway centric model. https://doi.org/10.1016/j.procs.2012.06.097.

[Isaac and Zeadally, 2014] Isaac, J. T. and Zeadally, S. (2014). Design, implementation, and performance analysis of a secure payment protocol in a payment gateway centric model. *Computing*, 96:587–611. https://doi.org/10.1007/s00607-013-0306-4.

[Itako, 2004] Itako, E. (2004). Automatic vending machine and sales method thereof. https://www.freepatentsonline.com/6754559.html.

[Jadhav et al., 2018] Jadhav, S., Pawar, N., Kharade, N., and Lengare, P. S. (2018). Automatic Vending Machine. *International Journal of Innovative Science and Research Technology (IJISRT)*, 3:376–378. https://www.ijisrt.com/automatic-vending-machine.

[Kavitha, 2018] Kavitha, D. (2018). Modern shopping cart with automatic billing system using load sensor. *International Journal of Engineering and Technology*, 7(2.33). https://www.sciencepubco.com/index.php/ijet/article/view/14846.

[Keller et al., 2017] Keller, J., Gabriele, and Wendzel, S. S. (2017). Ant Colony-Inspired Parallel Algorithm to Improve Cryptographic Pseudo Random Number Generators. In *IEEE Symposium on Security and Privacy Workshops*, pages 17–22.

[Khodawandi et al., 2003] Khodawandi, D., Pousttchi, K., and Wiedemann, D. G. (2003). Akzeptanz mobiler Bezahlverfahren in Deutschland. In *Mobile Commerce - Anwendungen und Perspektiven, Proceedings zum 3. Workshop Mobile Commerce*, pages 42–57, Bonn. Gesellschaft für Informatik e.V.

[Langdon et al., 2013] Langdon, P., Clarkson, J., and Robinson, P. (2013). Designing inclusive interactions. *Universal Access in the Information Society*, 12:233–235. https://doi.org/10.1007/s10209-013-0289-0.

[Lauzi, 2017] Lauzi, M. (2017). Smart-City: Die Stadt der Zukunft. *VDI Rheingau Regional Magazin*, 2:12–18.

[Luber and Schmitz, 2017] Luber, S. and Schmitz, P. (2017). Was ist Kryptographie? *Security Insider*. https://www.security-insider.de/was-ist-kryptographie-a-642288/.

[Lübbecke, 2018] Lübbecke, H. (2018). Akzeptanz und Übernahme von Informatikprodukten durch Ältere. *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)*, 4:31–34. https://www.fiff.de/publikationen/fiff-kommunikation/fk-2018/fk-2018-4/fk-2018-4-content/fk-4-18-p31.pdf.

[Me, 2003] Me, G. (2003). Payment security in mobile environment. In *ACS/IEEE International Conference on Computer Systems and Applications, 2003. Book of Abstracts.*, pages 34–. http://dx.doi.org/10.1109/AICCSA.2003.1227468.

[Nießner, 2017] Nießner, M. (2017). *Innovative Technik im Zahlungsverkehr. Ein kompakter Überblick über traditionelle und moderne Zahlungsverfahren.* GRIN Verlag, Norderstedt, 1 edition.

[Opiela and Garey, 2010] Opiela, M. S. and Garey, R. E. (2010). Electronic postal money order method and system. https://www.freepatentsonline.com/7849015.html.

[Patil et al., 2020] Patil, A. B., Mahajan, G., Phale, V., and Mane, S. (2020). Vending Machine with Cash and Cashless Payment Support. *International Journal in IT and Engineering*, 07:341–348.

[Renaudin et al., 2004] Renaudin, M., Bouesse, F., Proust, P., Tual, J., Sourgen, L., and Germain, F. (2004). High security smartcards. In *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, volume 1, pages 228–232 Vol.1. http://dx.doi.org/10.1109/DATE.2004.1268853.

[Riebe et al., 2020] Riebe, T., Haunschild, J., Divo, F., Lang, M., Roitburd, G., Franken, J., and Reuter, C. (2020). Die vorratsdatenspeicherung in europa. *Datenschutz und Datensicherheit - DuD*, 44:316–321. http://www.peasec.de/paper/2020/2020_Riebeetal_VDSinEuropa_DuD.pdf.

[Rihaczek, 2013] Rihaczek, K. (2013). Datenschutz & Computer. *Datenschutz*

und Datensicherheit, 37(9):561. https://doi.org/10.1007/s11623-013-0236-5.

[Schaeffler, 2008] Schaeffler, J. (2008). *Digital Signage: Software, Networks, Advertising, and Displays a Primer for Understanding the Business*. Focal Press, Burlington.

[Seibel, 2019] Seibel, K. (2019). Die deutsche Liebe zum Bargeld verblasst – wegen nur einer Karte. *Die Welt*. https://www.welt.de/wirtschaft/article193063435/Zahlungsmittel-Karte-schlaegt-in-Deutschland-erstmals-Bargeld.html.

[Semenov et al., 2017] Semenov, V. P., Chernokulsky, V. V., and Razmochaeva, N. V. (2017). The cashless payment device for vending machines — Import substitution in the sphere of vending. In *2017 International Conference Quality Management,Transport and Information Security, Information Technologies (IT QM IS)*, pages 798–801.

[Shen et al., 2019] Shen, L., Qiu, C., Wu, X., Han, C., and Hu, L. (2019). Design of removable vending machine and research on the key implementation technology. *The Journal of Engineering*, 2019(13):402–405. https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/joe.2018.9021.

[Sibanda et al., 2020] Sibanda, V., Munetsi, L., Mpofu, K., Murena, E., and Trimble, J. (2020). Design of a high-tech vending machine. *Procedia CIRP*, 91:678–683. https://www.sciencedirect.com/science/article/pii/S2212827120308829.

[Siepermann, 2018] Siepermann, M. (2018). Gabler wirtschaftslexikon: Stichwort: Digital native. https://wirtschaftslexikon.gabler.de/definition/digital-native-54496.

[Sommerville, 2010] Sommerville, I. (2010). *Software Engineering*. Pearson, Boston, 9 edition.

[Steffen, 2012] Steffen, A. (2012). Sicherheit Smartcard-basierter Zugangskontrollsysteme. Master's thesis, Ruhr-Universität Bochum, Universitätsstraße 150, 44801 Bochum. https://www.emsec.ruhr-uni-bochum.de/media/attachments/files/2012/04/Master-Arbeit-public.pdf.

[Tanembaum, 2009] Tanembaum, A. S. (2009). *Moderne Betriebssysteme*. Pearson, München.

[Wang et al., 2013] Wang, Q. E., Myers, M. D., and Sundaram, D. (2013). Digital Natives und Digital Immigrants. *Wirtschaftsinformatik*, 55(6):409–420. https://link.springer.com/article/10.1007/s11576-013-0390-

2#citeas.

[Wendzel, 2018] Wendzel, S. (2018). *IT-Sicherheit für TCP/IP- und IoT-Netzwerke*. Springer Vieweg, Wiesbaden.

[Wendzel et al., 2021] Wendzel, S., Mazurczyk, W., Caviglione, L., and (Eds.), A. H. (2021). Emerging Topics in Defending Networked Systems. *Special Issue at Future Generation Computer Systems (FGCS)*.

[Wendzel and Plötner, 2007] Wendzel, S. and Plötner, J. (2007). *Praxisbuch Netzwerk-Sicherheit: Risikoanalyse, Methoden und Umsetzung; für Unix-Linux und Windows; VPN, WLAN, Intrusion Detection, Disaster Recovery, Kryptologie*. Galileo Computing, Bonn.

[Wendzel et al., 2017] Wendzel, S., Tonejc, J., Kaur, J., and Kobekova, A. (2017). *Cyber Security of Smart Buildings*, chapter 16, pages 327–351. John Wiley & Sons, Ltd. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119226079.ch16.

[Woehe and Kurz, 2021] Woehe, J. M. and Kurz, E. (2021). *Krisen in Digitalprojekten erfolgreich managen*. Hanser, München.

[Yildirim and Varol, 2019] Yildirim, N. and Varol, A. (2019). A Research on Security Vulnerabilities in Online and Mobile Banking Systems. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–5. http://dx.doi.org/10.3390/sym12081344.