

**Hochschule Worms**  
**Fachbereich Informatik**  
**Studiengang Angewandte Informatik B.Sc.**

**Gewährleistung von sicherem digitalem Bezahlen bei  
einem Click and Buy Automat**

Exposé für Wissenschaftliche Schreiben

Bruno Macedo da Silva und Dominic Meyer

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

## Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>3</b>
<b>2</b>	<b>Forschungsziele</b>	<b>4</b>
<b>3</b>	<b>Stand der Forschung</b>	<b>6</b>
<b>4</b>	<b>Stand der Technik</b>	<b>9</b>
4.1	Drahtlose Verbindungen und Sicherheit bei Bezahlungen . . . . .	9
4.2	Anwendung von Smartcards und sicheres Bezahlen . . . . .	10
<b>5</b>	<b>Forschungsplann</b>	<b>13</b>
<b>6</b>	<b>Praktische Relevanz</b>	<b>14</b>
	<b>Literaturverzeichnis</b>	<b>15</b>

## Abbildungsverzeichnis

1	Cashless payments via the Deutsche Bundesbank (Bundesbank, 2009, S.52) . . . . .	6
2	Sicherheitseigenschaften von digitalen Zahlungsmethode (Hassan et al. 2020, S8) . . . . .	7
3	Eine Smartcard und deren eingebetete Mikrochip (eigene Quelle) . . . . .	11
4	Authentifizierungsprozess von Smartcards (Tanenbaum, 2009, S.755) . . . . .	11

# 1 Einführung

Seit einigen Jahren entscheiden sich immer mehr Menschen Urlaub auf einem Campingplatz zu machen. 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 Punkt in einem Urlaub. In den letzten anderthalb Jahren stieg die Anzahl von Campingplatzbesuchern rasant. 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. 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.

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-Supermarktes, der mit einem Automaten zu vergleichen ist, eine wesentliche Rolle spielen, um einen Campingplatz und die Gegend drum herum zu modernisieren, die Möglichkeiten zur Grundversorgung zu erweitern und ihn attraktiver für Reisende zu machen.

Die Sicherheit eines digitalen Konzepts stellt eines der wichtigsten Punkte für die Entwicklung eines Systems dar. Vernachlässigungen in diesem Bereich führen zu unberechenbarem Vertrauensverlust seitens der potenziellen Nutzenden und zu finanziellen und moralischen Schäden der direkten Stakeholders. Der folgende Artikel soll beschreiben, welche Schritte auf digitaler Sicherheitsebene eingeleitet werden müssen, um einen akzeptablen und funktionierenden Click and Buy Automat errichten zu können.

## 2 Forschungsziele

In diesem Artikel soll ein Konzept für ein Click-and-Buy-Supermarkt 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.

Um einen elektronischen Supermarkt zu entwickeln, müssen einige Voraussetzungen erfüllt werden. Es sollte eine ausreichende Verfügbarkeit des Netzwerkzugangs gewährleistet werden, eine stabile Software, die den Qualitätsstandards entspricht, ein sicherer Umgang mit Kundendaten, der sich an spezifischen und internationalen Richtlinien orientiert, ein benutzerfreundliches System, das sich an verschiedenen Kundentypen, wie Alters- und Bildungsgruppe anpasst und letztlich ein kryptographisches Verfahren 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].

Zudem soll das System so entwickelt werden, sodass auch Digital Non-Natives, die Möglichkeit haben das System einfach bedienen zu können [Wang et al., 2013]. 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 entscheidende Rolle, dass auch sie mit dem Automaten umgehen können. Deshalb sollten die Bedürfnisse und Einschränkungen dieser Altersgruppe besonders berücksichtigt werden, um ihr Vertrauen zu gewinnen [Lübbecke, 2018] und hauptsächlich gegen Social Engineering 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 Cyberangriffen zeigen, dass der Umgang mit solchen Daten, kritisch zu sehen ist. 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 entwickelt wurde. In dieser Hinsicht sollten bei der Entwicklung spezifische und klare Richtlinien berücksichtigt werden, sodass der sichere Umgang mit personenbezogenen Daten gewährleistet ist [Riebe et al., 2020]. Um diese Vertraulichkeitsverletzung zu vermeiden, spielt die Konzipierung von sicheren bargeldlosen Zahlungsmethoden eine wesentliche Rolle in diesem Artikel.

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

### 3 Stand der Forschung

Die zunehmende Tendenz in Deutschland von bargeldloser Bezahlung erfordert neuen Umgang mit den eingegebenen 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].

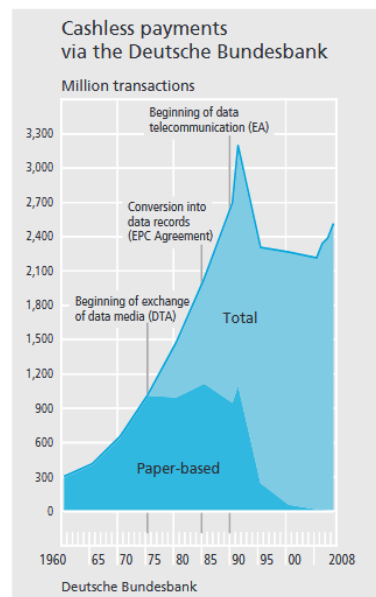


Abbildung 1: Cashless payments via the Deutsche Bundesbank  
(Bundesbank, 2009, S.52)

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 mit Bargeld gehen. Auch das kontaktlose 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.

Immer wenn mit Karte bezahlt wird, gehen die Kunden davon aus, dass die

Zahlungsabwicklung sicher ist. Wie sicher ist das bargeldlose Zahlen heutzutage wirklich?

Aus diesem Grund ist Vertraulichkeit die erste und wichtigste Voraussetzung, dass ein solches System erfüllen muss, um neue potenzielle Kunden zu gewinnen. Unter diesem Begriff soll ein System nur auf autorisierte Informationen zugreifen [Wendzel, 2018]. In dieser Hinsicht ist die Entwicklung einer Click and Buy Maschine so zu konzipieren, dass sie einen sicheren Umgang mit den Kundendaten anbietet. Diese Interaktion zwischen Kunde und systemkritischen Mechanismen wurde von [Hassan et al., 2020] so dargestellt:

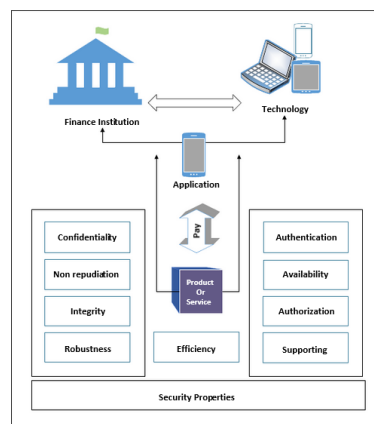


Abbildung 2: Sicherheitseigenschaften von digitalen Zahlungsmethode (Hassan et al. 2020, S8)

Außerdem sollen die anderen Schutzziele der IT-Sicherheit: Integrität, Verfügbarkeit und Authentizität auch berücksichtigt werden, sodass die Systemen einwandfrei und sicher funktionieren. Eine Zahlungsmethode, bei der alle Voraussetzungen erfüllt werden, kann in der Lage sein, das Vertrauen und die Akzeptanz von den Nutzenden zu bekommen [Hassan et al., 2020].

[Henze et al., 2017] nennt solche Maschinen Cyber-Physical System (CPS), weil sie eine Interaktion zwischen Nutzer und einem oder vielen Systemen darstellt. In dieser Zusammenarbeit spielt der Datenaustausch eine wesentliche Rolle, besonders von der Seite der Nutzenden. Diese Technologie zielt

eine günstigere Entwicklung, ohne die Sicherheit zu vernachlässigen. Diese Interaktion findet erfolgreich statt, wenn die genannten Sicherheitsziele erfüllt werden.

Da es um einen dynamischen Sektor geht, bei dem es sehr schnell zu Änderungen kommen kann, [Yildirim and Varol, 2019] muss die Technologie stets weiterentwickelt und angepasst werden, um Vertraulichkeitsverlust seitens der Kunden zu vermeiden. Da die Vertraulichkeit noch nicht zu 100 Prozent gewährleistet werden kann, verweigern viele Kunden das bargeldlose Bezahlen.

**Ab hier können wir dann versuchen, die Informationen aus den Artikeln zu nehmen, solche die du hier hinzugefügt hast und solche, die ich dir am Fr schickte**

**Ich würde diesen Satz in den nächsten Kapitel verwenden und erweitern mit unseren Recherchen, damit wird die Literatur rechtfertigen können** Um das zu bewerkstelligen, ist der aktuelle technische Stand von entscheidender Bedeutung. Ausgehend von dieser Informationen muss das Glasfasernetz eventuell erweitert oder auch neu verlegt werden. Denn das Ziel ist es, technisch gesehen auf dem neusten Stand zu sein, damit das Click and Buy System für die Zukunft abgesichert ist. Außerdem wird durch den Ausbau des Glasfasernetzes die Region insgesamt deutlich attraktiver gemacht, was vielleicht auch Menschen dazu bringt in diese Region zu ziehen. Denn jedem ist klar, dass ein guter Internetausbau essentiell ist, um vielleicht auch mal von zuhause aus zu arbeiten.



## 4 Stand der Technik

Für die Bezahlungsmethoden werden hier zwei/drei verschiedene Arten in Hinsicht auf ihrer Schwachstellen und ihrer Hartungen betrachtet: drahtlose Zahlung und Kartenzahlung.

### 4.1 Drahtlose Verbindungen und Sicherheit bei Bezahlungen

Viele digitale Zahlungen finden über WLAN statt, das kann eine größere Risiko darstellen [Yildirim and Varol, 2019], da WLAN-Verbindungen nicht so sicher sind wie Kabelverbindungen. Maßnahmen zu entwickeln, die sich an verschiedenen Systemen 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 genannten Schwachstellen bei kabellosen Verbindungen reduzieren können. Unter denen werden folgende hervorgehoben:

- Nutzung von modernen kryptographischen Standards für die Validierung von Zertifikaten;

- Erstellung von Loggdatei, sodass jeder Anomalität 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.

Da drahtlose Zahlungen bei Campingplätzen eine wesentliche Rolle spielen kann, muss die Sicherheit solcher Zahlungsart gewährleistet werden. Das kann erfolgreich passieren, wenn Banken und andere Finanz Institutionen sich intensiv mit den verschiedenen Angriffsmöglichkeiten und deren Schutzmaßnahmen beschäftigen.

Zahlungskarten wie Kredit- oder EC-Karte sollen auch Zahlungsmittel bei einem Click and Buy Maschinen zur Verfügung gestellt werden. In Bezug auf diese Modalitäten werden die verschiedenen Aspekte der Sicherheit dieser Zahlungsart unten beschrieben.

## **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 3.

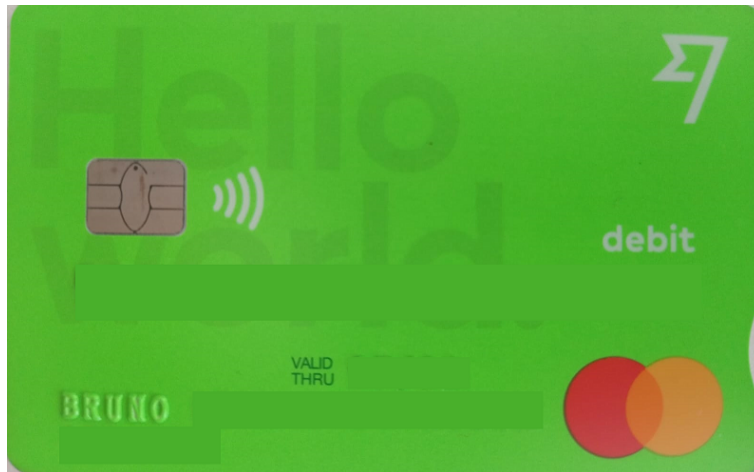


Abbildung 3: Eine Smartcard und deren eingebettete Mikrochip  
(eigene Quelle)

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 traditionellen Magnetstreifenkarten, weil sie verschiedene Authentifizierungsmethoden ermöglichen auch ohne direkte Verbindung zur Bank [Tanenbaum, 2009]. Im folgenden wird der Authentifizierungsprozess einer Smartcard 4 dargestellt.

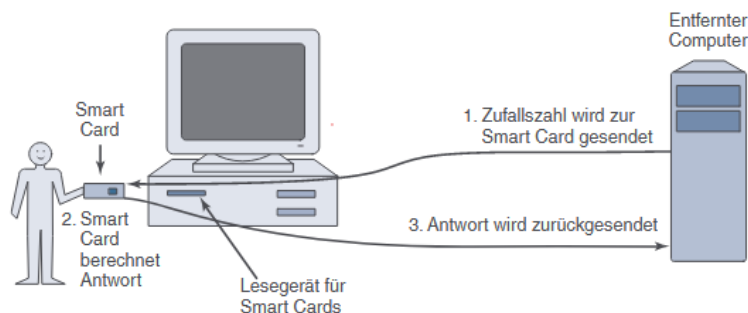


Abbildung 4: Authentifizierungsprozess von Smartcards  
(Tanenbaum, 2009, S.755)

Wenn es um die Sicherheit von Smartcards geht, beschreibt [Steffen, 2012], dass die Angriffe sich auf Hardwareebene konzentrieren. 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 der Kommunikation, sondern versucht sie irgendwie zu stören;
- Hardware Reverse Engineering: Verständnis über die Algorithmen oder Extrahieren des Schlüssels.

Die Schutzmaßnahmen können sich laut [Steffen, 2012] in drei Gruppen einteilen: physikalisch, logisch und organisatorisch. Auf der physikalischen Ebene soll die Hardware robust aufgebaut werden, um Angriffe schwieriger zu machen. Dieser Konstruktion soll komplex mit zusätzlichen Elementen eingebaut werden und Sensoren können auch dazu beitragen, das System auszuschalten bzw. zu blockieren, falls es zu einer verdächtigen Nutzung kommt. Auf der logischen Ebene sollen moderne und starke Verschlüsselungsmechanismen eingesetzt werden, deren Verfahren gegen Sicherheitslücken überprüft wurde. Die Bearbeitungszeit spielt hier eine wesentliche Rolle gegen Angriffe, die auf Seitenkanäle basieren. Letztendlich sollen solche Smartcards auf der organisatorischen Ebene in der Lage sein, Angriffe schnell zu detektieren und zu verhindern. Zu dieser Ebene gehören auch die Sperre der Karte, die Überprüfung von Logdateien, um Klone zu identifizieren, und die Verwendung von Zwei-Faktor-Authentisierung.

## 5 Forschungsplan

Grafische Darstellung des Forschungsvorhabens

Methoden der Datensammlung ==> Besuch einigen Firmen

Methoden der Datendokumentation ==> Aufnahme

Methoden der Datenauswertung ==> Vergleich der Daten der Firma (Anzahl Mitarbeiter, Anzahl Server/Pc, Seit wann benutzt es)

Anhang (Fragenkatalog) ==> Seitwann benutzt, was war vorher, was ist jetzt leichter/schwieriger, Kosten

## 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](https://doi.org/10.1007/978-3-030-31143-8_1).
- [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*.
- [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>.
- [Dua et al., 2014] Dua, A., Rustagi, C., and Bhardawaj, A. (2014). A Novel Approach to Designing Intelligent Vending Machines. *International Journal in IT and Engineering*, 212212.
- [Dullien, 2018] Dullien, T. (2018). Maschinelles Lernen und künstliche Intelligenz in der Informationssicherheit. *Datenschutz und Datensicherheit - DuD*, 42(10):618–622. [https://doi.org/10.1007/978-3-030-31143-8\\_1](https://doi.org/10.1007/978-3-030-31143-8_1).
- [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>.
- [Gomm et al., 1997] Gomm, G. R., Paul, G. R. G., and Paul, S. (1997). Cash alternative transaction system. <https://www.freepatentsonline.com/56>

50761.html.

- [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. John Wiley & Sons, Ltd. <https://onlinelibrary.wiley.com/doi/abs/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, 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 and ., 2018] Kavitha, D. and ., . (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.
- [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.
- [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>.
- [Nießner, 2017] Nießner, M. (2017). *Innovative Technik im Zahlungsverkehr. Ein kompakter Überblick über traditionelle und moderne Zahlungsverfahren*. GRIN Verlag, 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](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.
- [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-ers>

tmals-Bargeld.html.

- [Semenov et al., 2017] Semenov, V. P., Chernokulsky, V. V., and Razmochayeva, 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>.
- [Sommerville, 2010] Sommerville, I. (2010). *Software Engineering*. Addison-Wesley, 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>.
- [Tanenbaum, 2009] Tanenbaum, A. S. (2009). *Moderne Betriebssysteme*. Pearson Studium, 3. aktualisierte auflage edition.
- [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, 1 edition.
- [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, 2 edition.

- [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, 1 edition.
- [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>.