Digital Business University
of Applied Sciences

Cyber- & IT-Security (M.Sc.)

Informationstechnik für Cyber- & IT-Security

Wintersemester 2024/25

IoT-Protokolle und Standards: Interoperabilität und Herausforderungen in Smart-Home-Systemen

Studienarbeit

Eingereicht von:
Elias Häussler

Matrikelnummer:
200094

Dozent:
Prof. Dr. Mukayil Kilic

28. Januar 2025

Inhaltsverzeichnis

Abkürzungsverzeichnis

API	Application Programming Interface
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IoT	Internet of Things
KI	Künstliche Intelligenz
MAC	Message Authentication Code
P2P	Peer-to-Peer
RFC	Request for Comments
SASL	Simple Authentication and Security Layer
SDK	Software Development Kit
STOMP	Simple Text Oriented Messaging Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Modules
WPAN	Wireless Personal Area Network
XEP	XMPP Extension Protocol
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

1 Einleitung

Smarte Beleuchtung, intelligente Verkehrsampeln, Wearables – Überall im Alltag begegnen uns mittlerweile intelligente Geräte und smarte Technologien, die unser Leben komfortabler, sicherer und ökologisch wertvoller machen sollen. Begriffe wie *Smart Home* oder *Smart City* sind uns geläufig und für viele aus dem Alltag nicht mehr wegzudenken. Und das aus einem guten Grund: Spätestens mit der Einführung des Internets wurde deutlich, welch enormen Vorteil vernetzte Systeme für den Menschen und seinen Planeten haben. Hinter all diesen Technologien steckt ein äußerst komplexes Konstrukt an unterschiedlichen technischen Implementierungen des *Internet of Things (IoT)*. Diese enorme Vielfalt hat jedoch auch Schattenseiten, bedingt durch die rasante Entwicklung und die daraus resultierende Zunahme an heterogenen Systemen.

1.1 Problemstellung

Weil viele Hersteller das Potenzial des IoT erkannt haben, entwickelten sie in kürzester Zeit eigene Lösungen, allen voran für *Smart-Home-Systeme*. Sind einzelne IoT-Geräte zwar in kleineren IoT-Netzwerken häufig noch kompatibel zueinander, so gelangen sie bei der Integration mehrerer smarter Lösungen häufig schnell an ihre Kompatibilitätsgrenzen. Die so entstandenen heterogenen Systeme sind nicht mehr vollumfänglich in der Lage, miteinander zu interagieren und Interoperabilität zu gewährleisten, was häufig ein gesamtes IoT-Netzwerk instabil und zumeist ineffizient macht.

Diesem Problem soll auf den Grund gegangen und es sollen Lösungen erarbeitet werden, wie Interoperabilität im IoT – und speziell in Smart-Home-Systemen – gewährleistet werden kann.

1.2 Inhalte der Arbeit

In dieser Arbeit werden zur Darstellung des Problems und möglicher Lösungsansätze unterschiedliche IoT-Protokolle und Standards vorgestellt. Hierfür werden in Kapitel 2 zunächst grundlegende Begriffe für das Verständnis der nachfolgenden Kapitel geklärt. Außerdem wird auf die behandelten Kommunikationsanforderungen eingegangen, für die in Kapitel 3 ausgewählte IoT-Protokolle und Standards vorgestellt werden. Ergänzend werden in Kapitel 4 die größten Herausforderungen in Bezug auf Interoperabilität in IoT-Systemen aufgezeigt und Lösungsansätze skizziert. Die Arbeit schließt in Kapitel 5 mit einer Zusammenfassung der vorgestellten Inhalte und gibt Ausblicke auf mögliche Weiterentwicklungen im Bereich des IoT.

2 Grundlagen

2.1 Internet of Things (IoT)

Der Begriff des *Internet of Things (IoT)* hat eine längere Vergangenheit als häufig angenommen. In seiner heutigen Form beschreibt er „eine Entwicklung, bei der physische Dinge vernetzbar und so in (bestehende) Informationsnetzwerke integriert werden“ (Wagner, 2020, S. 4). Dabei werden Objekte um *Sensoren* und *Aktuatoren* ergänzt, durch die sie imstande sind, „mit ihrer Umwelt zu interagieren, Informationen zu sammeln, miteinander zu kommunizieren und so die gewonnenen Daten untereinander auszutauschen“ (Wagner, 2020, S. 4). Die hierfür benötigte Hardware folgt dem Prinzip der *Miniaturisierung*: Sensoren und Aktuatoren müssen möglichst klein gebaut werden, um auch in (Kleinst-)Geräten verbaut werden zu können, die dadurch zu *smarten* Objekten im IoT werden (Wagner, 2020).

2.2 Smart-Home-Systeme

Ein populäres Einsatzgebiet des IoT sind sog. *Smart-Home-Systeme*. Hierbei handelt es sich um einen Oberbegriff für die intelligente Vernetzung unterschiedlicher Haushaltssysteme, durch die „zum einen die Wohnqualität und Sicherheit gesteigert, zum anderen aber auch der Energieverbrauch gesenkt werden“ soll (Wagner, 2020, S. 7). Bekannte Beispiele für vernetzte Geräte in Smart-Home-Systemen sind etwa der smarte Kühlschrank, der erkennt, wann bestimmte Lebensmittel zur Neige gehen, Geräte zur effizienten Temperatursteuerung der Heizung (auch *Smart Heating* genannt) oder smarte Überwachungssysteme wie Kameras und Türschließanlagen (Wagner, 2020).

2.3 Kommunikationsanforderungen

Damit smarte Geräte untereinander kommunizieren können, tauschen sie Daten über verschiedene *IoT-Protokolle* aus. Nicht selten werden dabei sehr unterschiedliche Protokolle und Datenformate verwendet, was ein Zusammenspiel in schon kleineren IoT-Systemen schwierig gestalten kann (Matevska et al., 2023). Allgemein ist das Wachstum des IoT enorm angestiegen; die Anzahl smarter Geräte im IoT wird für 2033 auf über 39 Milliarden geschätzt (Statistisches Bundesamt, 2024). Dadurch wächst der Anspruch an eine einfache Handhabung der Geräte und durch den Einsatz immer neuerer Technologien auch an deren Kommunikationsfähigkeiten. Im Fokus steht dabei die **Interoperabilität**, also das Zusammenspiel heterogener Systeme, um die Kommunikation ebendieser untereinander zu gewährleisten. Von hoher Relevanz sind aber auch die **Skalierbarkeit** und **Sicherheit** der Systeme (Matevska et al., 2023). Es existieren darüber hinaus noch deutlich mehr Anforderungen; diese Arbeit beschränkt sich jedoch auf die drei genannten im Kontext von Smart-Home-Systemen.

3 IoT-Protokolle und Standards

In der Welt des IoT gibt es an unterschiedlichen Stellen die Notwendigkeit des Datenaustauschs. Hierfür existiert eine Vielzahl an Protokollen und Standards für die Kommunikation auf Geräte-, Anwendungs- und Netzwerkebene. Drei populäre IoT-Protokolle und Standards werden nachfolgend vorgestellt, um zu verdeutlichen, welche Möglichkeiten für die Interoperabilität heterogener Systeme im IoT existieren.

3.1 ZigBee

ZigBee ist ein Funkfrequenz-Kommunikationsstandard, der hauptsächlich für die Nutzung in einem *Wireless Personal Area Network (WPAN)* entwickelt wurde. Charakteristisch ist dabei der Einsatz eines *Koordinators*, der für den Aufbau und die Pflege des Netzwerks verantwortlich ist und jedes im Netzwerk befindliche Gerät verwaltet (Gill et al., 2009). Im Vergleich zu anderen Kommunikationsstandards wie *Wi-Fi* oder *Bluetooth* ist die Nutzung eines auf ZigBee basierenden Smart-Home-Systems vor allem in drei Punkten vorteilhaft (nach Gill et al. (2009)):

1. Die maximale Datenübertragungsrate beträgt lediglich 250 KBit/s, was zu einer besonders **effizienten Kommunikation** zwischen den Netzwerkgeräten führt und immer noch weit über den Anforderungen der meisten Steuersysteme liegt.

2. **Niedrige Installationskosten** ermöglichen einen lohnenswerten Einsatz schon bei einer geringen Anzahl an Geräten.

3. Die hohe Energieeffizienz trägt außerdem zu **niedrigen Betriebskosten** bei.

3.2 Z-Wave

Das für die drahtlose Kommunikation entwickelte proprietäre Protokoll *Z-Wave* gilt gemeinhin als eines der sichersten Protokolle im IoT-Bereich. Es basiert auf dem *S2 Security*-Framework, welches symmetrische Verschlüsselung in Kombination mit *Message Authentication Code (MAC)* verwendet (Braghin et al., 2023). Dadurch bietet es Paketverschlüsselung sowie Integritätsschutz und stellt zudem verschiedene Dienste zur Geräteauthentifizierung bereit (Fouladi & Ghanoun, 2013). Neben Sicherheit stellen die Entwickler*innen vor allem Interoperabilität in den Fokus des Z-Wave-Standards: Alle im Z-Wave-Ökosystem entwickelten und zertifizierten Produkte sollen miteinander kompatibel sein, was laut eigener Aussage auf mittlerweile über 4500 unterschiedliche Produkte zutrifft (Z-Wave Alliance, 2025). Da es sich um ein proprietäres Protokoll handelt, ist die Skalierbarkeit hingegen begrenzt. Die Spezifikation und das *Software Development Kit (SDK)* sind nicht öffentlich zugänglich und müssen kostenpflichtig erworben werden (Fouladi & Ghanoun, 2013).

3.3 MQTT

Ein nach dem *Publish-Subscribe*-Pattern entwickeltes Netzwerkprotokoll ist *MQTT* (ursprünglich *Message Queuing Telemetry Transport*). Dabei handelt es sich um ein sehr weit verbreitetes, leichtgewichtiges Protokoll, das dynamische Skalierbarkeit, Ressourceneffizienz und eine einfache Implementierung bietet. Das Publish-Subscribe-Pattern verfolgt dabei vor allem das Ziel, skalierbare Lösungen für die zunehmende Anzahl an Geräten im IoT zu schaffen (Bender et al., 2021).

Im Grundsatz funktioniert Publish-Subscribe wie folgt: Ein Herausgeber (*Publisher*) sendet eine Nachricht an einen Kanal (*Event Channel*). Dieser ist dafür verantwortlich, die Nachricht an jeden Abonnenten (*Subscriber*) zu versenden, der an der Nachricht interessiert ist. In MQTT werden hierzu *MQTT-Clients* als Publisher eingesetzt, die eine Verbindung zu einem als Event Channel fungierenden *MQTT-Broker* herstellen und darüber Nachrichten veröffentlichen. Einzelne Nachrichten beziehen sich hierbei immer auf bestimmte *Topics* und werden vom MQTT-Broker an diejenigen MQTT-Clients weitergeleitet, die entsprechende Topics abonniert haben (Bender et al., 2021).

Die Umsetzung des Publish-Subscribe-Patterns in einem MQTT-Netzwerk ist schematisch in Abbildung 1 dargestellt.

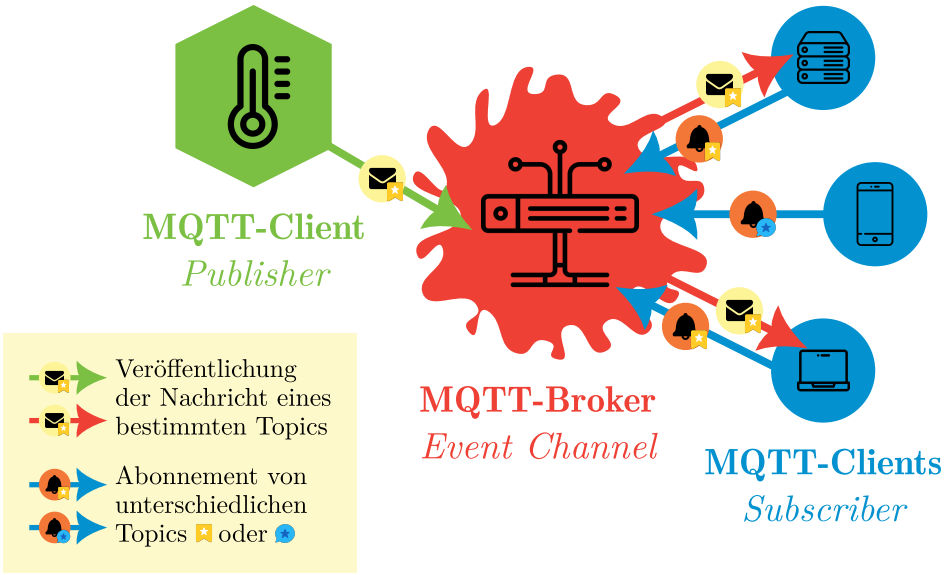

Abbildung 1: Schematische Darstellung eines MQTT-Netzwerks

Da das MQTT-Protokoll öffentlich verfügbar ist, existieren auch eine Reihe von Open Source-Lösungen. Einer der bekanntesten und am weitesten verbreiteten MQTT-Broker ist *Mosquitto*, der durch seinen einfachen Aufbau ein schnelles Aufsetzen größerer MQTT-Netzwerke ermöglicht. Mosquitto bietet auch eine Bibliothek für MQTT-Clients an und erfährt in diesem Bereich ebenso eine hohe Verbreitung. Andere Broker wie *EMQX* oder *VerneMQ* sind ebenfalls weit verbreitet; *Paho MQTT* und *MQTT.js* gelten als beliebte Client-Implementierungen (Bender et al., 2021).

3.4 Simple Text Oriented Messaging Protocol (STOMP)

Wie MQTT folgt auch das *Simple Text Oriented Messaging Protocol (STOMP)* dem Publish-Subscribe-Pattern. Dabei dient ein *STOMP-Server* als Broker, der ähnlich wie ein MQTT-Broker eingehende Nachrichten an die entsprechenden Clients verteilt. Clients können hierbei ebenfalls als Publisher und Subscriber im Netzwerk eingesetzt werden. STOMP-Nachrichten ähneln dem Aufbau von *Hypertext Transfer Protocol (HTTP)*-Nachrichten und können von einem STOMP-Server verändert werden, was im Vergleich zu einem MQTT-Broker einen größeren Leistungsumfang darstellt (Wytrębowicz et al., 2021). STOMP ist frei verfügbar und bereits in einigen bekannten Brokern wie etwa *RabbitMQ* oder *Apache ActiveMQ* implementiert (STOMP, 2025).

3.5 Extensible Messaging and Presence Protocol (XMPP)

Anders als die bisher vorgestellten Standards und Protokolle charakterisiert das *Extensible Messaging and Presence Protocol (XMPP)* vor allem die strikte Implementierung bestehender Standards, die von der *Internet Engineering Task Force (IETF)* vorgegeben sind. So werden neben vielen weiteren *Request for Comments (RFC)* beispielsweise *RFC 6120*, *RFC 6121* und *RFC 7622* in der Spezifikation benannt. Dabei folgt das Protokoll dem *Client-Server*-Prinzip und ermöglicht durch seinen Kommunikationsmechanismus die Entwicklung eines *Peer-to-Peer (P2P)*-Netzwerks aller teilnehmenden Clients. Erwähnenswert ist zudem, dass XMPP auf dem *Transmission Control Protocol (TCP)* aufbaut und auch mit HTTP und WebSockets genutzt werden kann (Wytrębowicz et al., 2021).

Unter dem *XMPP Extension Protocol (XEP)* veröffentlicht die IETF fortlaufend eine Reihe standardisierter XMPP-Erweiterungen[1], die deren Nutzung in vielen unterschiedlichen Einsatzgebieten ermöglichen soll. Einige der Erweiterungen sind dabei speziell auf die Anwendbarkeit im IoT ausgelegt. Durch die Standardisierung der gesamten Spezifikationen rund um XMPP und die Nutzung von *Extensible Markup Language (XML)* als Nachrichtenformat wird die Implementierung des Protokolls erheblich vereinfacht (Malik et al., 2018; Wytrębowicz et al., 2021).

Um die Sicherheit der Kommunikation zu gewährleisten, unterstützt XMPP das *Transport Layer Security (TLS)*-Protokoll für die verschlüsselte Kommunikation zwischen Client und Server sowie *Simple Authentication and Security Layer (SASL)* für die Benutzerauthentifizierung (Malik et al., 2018). Mit *XEP-0384* wurde zudem eine Erweiterung für Ende-zu-Ende-Verschlüsselung vorgestellt, welche bereits als *XEP-0027* mit OpenPGP realisiert wurde.

[1] Eine Übersicht aller Erweiterungen kann unter https://xmpp.org/extensions/ eingesehen werden.

4 Herausforderungen

Die rasche Entwicklung des IoT ist einerseits für Endanwender lukrativ und bietet immer mehr Gestaltungsspielraum beim Aufbau von Smart-Home-Systemen. Auf der anderen Seite werden Gerätehersteller und Anwendungsentwickler*innen vor eine Masse an technologischen Hürden gestellt, die nur schwer zu durchschauen sind und sehr herausfordernd sein können.

4.1 Technologische Hürden

Heterogene Systeme sorgen für geringere Interoperabilität zwischen einzelnen IoT-Geräten. Zwar existiert eine Vielzahl an IoT-Protokollen, mit denen genau dieses Problem umgangen werden soll, jedoch führt die Vielfalt dieser Protokolle in Kombination mit einer fehlenden Standardisierung immer häufiger zu Kompatibilitätsproblemen zwischen verschiedenen IoT-Geräten und -Plattformen. Hinzu kommt, dass einige Hersteller proprietäre Protokolle verwenden, was die Integration unterschiedlicher Systeme zusätzlich erschwert (Saleem et al., 2018).

Da nahezu jedes erdenkliche Haushaltsgerät mittlerweile in ein Smart-Home-System integriert werden kann, erhöht sich durch die zunehmende Anzahl von IoT-Geräten und deren zumeist steter Erreichbarkeit der gesamte Datenverkehr und sorgt für eine zunehmende Belastung von Netzwerkinfrastrukturen. Häufig verfügen viele dieser Geräte nur über begrenzte Rechenleistung, wodurch skalierbare Lösungen nur schwer umsetzbar und große Datenmengen nur schwer zu bewältigen sind (Saleem et al., 2018).

4.2 Sicherheitsaspekte

Hinreichend bekannt sind außerdem die vielen sicherheitsrelevanten Herausforderungen, die durch IoT-Netzwerke und im Besonderen durch Smart-Home-Systeme entstehen. Dies sind unter anderem (nach Saleem et al. (2018)):

- **Schwachstellen in Geräten**: Häufig weisen IoT-Geräten Sicherheitslücken auf, weil unzureichende Authentifizierungsmechanismen verwendet sowie Firmware- und Software-Updates vernachlässigt werden.
- **Mangelhafte Verschlüsselung**: Viele IoT-Geräte dienen als Einstiegspunkt in ein gesamtes Netzwerk, da keine oder nur mangelhafte Verschlüsselungstechnologien verwendet werden. Dies gefährdet die Integrität und Vertraulichkeit des gesamten Systems.
- **Fehlende Regulierung**: Die Sicherheitsniveaus zwischen verschiedenen Herstellern variieren teilweise deutlich, da keine klaren Vorgaben für einheitliche Sicherheitsstandards bei IoT-Geräten existieren. Es mangelt an allgemeinen Regeln, Prozessen, Verfahren, Audits und Rechenschaftspflichten.

4.3 Lösungsansätze

Obwohl die Entwicklung des IoT exponentiell stark anwächst und die damit einhergehenden Herausforderungen enorm sind, bieten sich auch hier Lösungen an, um technologische Hürden abzubauen und die Sicherheitsaspekte umfangreich zu adressieren.

4.3.1 Standardisierung

Um größtmögliche Interoperabilität zu gewährleisten und das Vorhandensein heterogener Systeme auf ein Minimum zu reduzieren, bietet sich die Einführung und Anwendung einheitlicher IoT-Protokolle an. Kommunikationsprotokolle wie MQTT sind bereits sehr weit verbreitet und könnten mehr als nur ein *de-facto*-Standard werden, sodass die Interaktion zwischen verschiedenen IoT-Geräten erleichtert wird. Ebenfalls denkbar ist eine *semantische Interoperabilität*, bei der gemeinsame Datenmodelle etabliert und genutzt werden, sodass unterschiedliche Systeme die ausgetauschten Daten eindeutig verstehen können. Alternativ wäre der Einsatz von *Middlewares* als Vermittler zwischen heterogenen Systemen denkbar; auch die Bereitstellung standardisierter *Application Programming Interface (API)*-Lösungen würde dazu beitragen, dass unterschiedliche Systeme besser miteinander interagieren können (Albouq et al., 2022).

4.3.2 IoT-Schichtenmodell

Tawalbeh et al. (2020) schlagen die Einführung eines IoT-Schichtenmodells vor, das für jede Schicht spezifische Sicherheits- und Datenschutzkomponenten identifiziert. Das Modell sieht folgende Schichten vor:

3. **Cloud-Schicht** (obere Schicht): Auf dieser Schicht erfolgt die zentralisierte Speicherung und Verarbeitung aller gesammelten Daten aus dem IoT-Netzwerk. Dies beinhaltet unter anderem auch Schlüssel für Ver- und Entschlüsselung sowie Authentifizierungsmaßnahmen.

2. **Edge-Schicht** (mittlere Schicht): Hier finden Datenverarbeitungs- und Analyseprozesse statt. Die hierfür genutzten Edge-Geräte (beispielsweise ein *Raspberry Pi*) werden mittels Verschlüsselung und Zugriffskontrollen geschützt und verwenden sichere Kommunikationsprotokolle.

1. **IoT-Knoten** (untere Schicht): Diese Schicht ist besonders anfällig für Angriffe, da sie die physischen IoT-Geräte umfasst. Daher sind hier besondere Maßnahmen, wie etwa sichere Boot-Prozesse (*Secure Boot*) und hardwarebasierte Sicherheitsmechanismen wie *Trusted Platform Modules (TPM)* notwendig.

5 Zusammenfassung

5.1 Ergebnisse

Je populärer das IoT wird und je mehr Menschen Zugang zu Smart-Home-Systemen erhalten, desto schneller wird sich auch die hierfür benötigte Technologie weiterentwickeln. Der Mensch als Nutznießer ist gleichzeitig Treiber des Fortschritts und Wachstums. Hersteller werden dadurch zunehmend vor Herausforderungen gestellt, weil die rasante Geschwindigkeit ihre Spuren hinterlässt. Es entstehen heterogene Systeme, die durch den häufigen Mangel an Interoperabilität zwar leistungsstarke IoT-Lösungen darstellen, jedoch große Schwächen in der breiten Anwendung aufzeigen können.

Protokolle und Standards sollen helfen, einen Rahmen für standardisierte Vernetzung im IoT zu schaffen und Herstellern, Entwickler*innen und Anwender*innen wieder mehr Sicherheit zu geben. Eine Reihe solcher IoT-Protokolle existiert bereits und viele finden auch heute schon breite Anwendung. MQTT und XMPP sind nur zwei Beispiele für weit verbreitete Kommunikationsprotokolle, die für eine niedrigere technologische Einstiegshürde in das IoT sorgen. Jedoch ist auch hier die Fülle an verfügbaren, teils proprietären Lösungen problematisch, weil trotz der vorhandenen Möglichkeiten noch kein einheitlicher Standard existiert. Ohne Standardisierung bleibt den Herstellern und Entwickler*innen nur die Möglichkeit, auf populäre *de-facto*-Standards zurückzugreifen, um eine möglichst breite Masse zu erreichen und neben Interoperabilität auch Skalierbarkeit und Sicherheit als notwendige Anforderungen größtmöglich in den Entwicklungsprozess einzubeziehen.

5.2 Ausblick

Zikria et al. (2021) diskutieren in ihrer Arbeit einen durch *Künstliche Intelligenz (KI)* gesteuerten Ansatz, um dynamische und adaptive Technologien zu ermöglichen. Durch den Einsatz von KI sollen Herausforderungen wie Echtzeit-Datenanalyse und die Bewältigung großer Datenmengen erleichtert werden. In puncto Skalierbarkeit wäre dies sicherlich ein wichtiger Schritt.

Ein IoT-Schichtenmodell, wie von Tawalbeh et al. (2020) vorgeschlagen, kann außerdem helfen, zukünftige Entwicklungen koordinierter auszurichten. Allerdings wird die Problematik dadurch eher von den Herstellern auf die Anwender*innen verlagert, was nicht unbedingt zielführend sein muss. Etwas weiter gehen Palau et al. (2021), indem sie ein schichtbasiertes Framework vorstellen, das modular aufgebaut ist und neben technischer Interoperabilität (mittels unterschiedlicher Protokolle) einen besonderen Schwerpunkt auf semantische Interoperabilität legt. Dadurch soll sichergestellt sein, dass die Bedeutung der Daten zwischen einzelnen Plattformen einheitlich bleibt.

All diese Entwicklungen machen deutlich, dass das IoT noch viel Potenzial für eine bessere Vernetzung mit weniger technologischen Hürden bereithält.

Literaturverzeichnis

Albouq, S. S., Abi Sen, A. A., Almashf, N., Yamin, M., Alshanqiti, A., & Bahbouh, N. M. (2022). A survey of interoperability challenges and solutions for dealing with them in IoT environment. *IEEE Access*, *10*, 36416–36428.

Bender, M., Kirdan, E., Pahl, M.-O., & Carle, G. (2021). Open-source mqtt evaluation. *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 1–4.

Braghin, C., Lilli, M., & Riccobene, E. (2023). A model-based approach for vulnerability analysis of IoT security protocols: The Z-Wave case study. *Computers & security*, *127*.

Fouladi, B., & Ghanoun, S. (2013). Security evaluation of the Z-Wave wireless protocol. *Black hat USA*, *24*, 1–2.

Gill, K., Yang, S.-H., Yao, F., & Lu, X. (2009). A zigbee-based home automation system. *IEEE transactions on consumer electronics*, *55*(2), 422–430.

Malik, M. I., McAteer, I. N., Hannay, P., Syed, N. F., & Baig, Z. (2018). XMPP architecture and security challenges in an IoT ecosystem. *Australian Information Security Management Conference*. https://ro.ecu.edu.au/ism/219/

Matevska, J., Soldin, M., Bures, T., Batista, T., Muccini, H., Raibulet, C., Raibulet, C., Bureš, T., Batista, T., & Muccini, H. (2023). Enabling IoT Connectivity and Interoperability by Using Automated Gateways. In *Software Architecture. ECSA 2022 Tracks and Workshops* (S. 300–317, Bd. 13928). Springer International Publishing AG.

Palau, C. E., Fortino, G., Montesinos, M., Exarchakos, G., Giménez, P., Markarian, G., Castay, V., Fuart, F., Pawłowski, W., Mortara, M., Ibáñez-Sánchez, G., Castay, V., Mortara, M., Gevers, F., Fortino, G., Pawłowski, W., Giménez, P., Bassi, A., Markarian, G., ... Fuart, F. (2021). *Interoperability of Heterogeneous IoT Platforms: A Layered Approach* (1st Edition 2021). Springer International Publishing AG.

Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018). IoT standardisation: Challenges, perspectives and solution. *Proceedings of the 2nd international conference on future networks and distributed systems*, 1–9.

Statistisches Bundesamt. (2024). Anzahl der mit dem Internet der Dinge (IoT) verbundenen Geräte weltweit von 2022 bis 2033 [Online; abgerufen am 19. Januar 2025]. https://de.statista.com/statistik/daten/studie/1420315/umfrage/anzahl-der-iot-geraete-weltweit/

STOMP. (2025). Implementations [Online; abgerufen am 24. Januar 2025]. https://stomp.github.io/implementations.html

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

Wagner, B. J. (2020). *Konnektivität von Assistenzsystemen* (1st ed. 2020). Springer Fachmedien Wiesbaden.

Wytrębowicz, J., Cabaj, K., & Krawiec, J. (2021). Messaging Protocols for IoT Systems—A Pragmatic Comparison. *Sensors (Basel, Switzerland)*, *21*(20), 6904–.

Zikria, Y. B., Ali, R., Afzal, M. K., & Kim, S. W. (2021). Next-generation internet of things (iot): Opportunities, challenges, and solutions. *Sensors*, *21*(4), 1174.

Z-Wave Alliance. (2025). Interoperability - Z-Wave Alliance [Online; abgerufen am 23. Januar 2025]. https://z-wavealliance.org/interoperability/

Eigenständigkeitserklärung

Ich trage die Verantwortung für die Qualität des Textes sowie die Auswahl aller Inhalte und habe sichergestellt, dass Informationen und Argumente mit geeigneten wissenschaftlichen Quellen belegt bzw. gestützt werden. Die aus fremden Quellen direkt oder indirekt übernommenen Texte, Gedankengänge, Konzepte, Grafiken usw. in meinen Ausführungen habe ich als solche eindeutig gekennzeichnet und mit vollständigen Verweisen auf die jeweilige Quelle versehen. Alle weiteren Inhalte dieser Arbeit (Textteile, Abbildungen, Tabellen etc.) ohne entsprechende Verweise stammen im urheberrechtlichen Sinn von mir.

Hiermit erkläre ich, dass ich die vorliegende Studienarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle sinngemäß und wörtlich übernommenen Textstellen aus fremden Quellen wurden kenntlich gemacht.

Die vorliegende Arbeit wurde bisher weder im In- noch im Ausland in gleicher oder ähnlicher Form einer anderen Prüfungsbehörde vorgelegt.

Erklärung zu (gen)KI-Tools

Verwendung von (gen)KI-Tools

Ich versichere, dass ich mich (gen)KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Ich verantworte die Übernahme jeglicher von mir verwendeter Textpassagen vollumfänglich selbst. In der Übersicht verwendeter (gen)KI-Tools habe ich sämtliche eingesetzte (gen)KI-Tools, deren Einsatzform sowie die jeweils betroffenen Teile der Arbeit einzeln aufgeführt. Ich versichere, dass ich keine (gen)KI-Tools verwendet habe, deren Nutzung der Prüfer bzw. die Prüferin explizit schriftlich ausgeschlossen hat.

Hinweis: Sofern die zuständigen Prüfenden bis zum Zeitpunkt der Ausgabe der Aufgabenstellung konkrete (gen)KI-Tools ausdrücklich als nicht anzeige-/kennzeichnungspflichtig benannt haben, müssen diese nicht aufgeführt werden.

Ich erkläre weiterhin, dass ich mich aktiv über die Leistungsfähigkeit und Beschränkungen der unten genannten (gen)KI-Tools informiert habe und überprüft habe, dass die mithilfe der genannten (gen)KI-Tools generierten und von mir übernommenen Inhalte faktisch richtig sind.

Übersicht verwendeter (gen)KI-Tools

Die (gen)KI-Tools habe ich, wie im Folgenden dargestellt, eingesetzt.

(gen)KI-Tool	**Einsatzform**	**Betroffene Teile der Arbeit**
ChatGPT	Generierung von ersten Ideen für eine geeignete Gliederung	Gesamte Arbeit
	Generierung von Zusammenfassungen der Literatur von *Albouq et al. (2022)* & *Saleem et al. (2018)*	Kapitel 4
	Generierung von Zusammenfassungen der Literatur von *Palau et al. (2021)* & *Zikria et al. (2021)*	Kapitel 5

Münster, 28. Januar 2025

Elias Häußler