IoT security in smart warehousing: Recent challenges and solutions

Dominik Deschner, Christian Iosif Schlier, Annika Stempfle and Jochen Welte

Hochschule Aalen, Beethovenstraße 1, 73430 Aalen

Abstract. IoT Systems are highly complicated, multi-layered and continuously interconnected computer systems which drive productivity and cost savings in different areas e.g., manufacturing, farming or services. Security is seen as one of the main concerns of the internet of things. As there are so many different perspectives on security in general IoT research, we want to specialize and narrow that topic to the field of smart warehouses, a subcategory of logistics. Thus, we are conducting a structured literature review on the state of research about IoT security in smart warehouses and deduce common requirements and issues.

Keywords: Internet of Things, smart warehouse, IoT security, IT security, logistics, smart manufacturing

1 Introduction

Connected and sensing devices embedded on the Internet of Things (IoT) have become one of the main drivers of efficiency in modern logistics. It creates new possibilities in different domains like traceability, product returns or smart supply chain management [1]. Even for smart cities logistic challenges are of major concern, for example when it comes to efficiently guiding cars and using parking lots [2] or reducing the co2 emission of public transportation [3] and time critical distribution of perishable consumables. Warehouses are a crucial part of the supply chains, and their smartness determines how efficient they can be operated in terms of throughput and cost savings [4]. Smart warehouses are heavily driven by IoT systems which act as a catalyst for challenges like automation, traceability, efficient order picking, smart space allocation or accurate localization of goods [5], [6].

Since security has been identified as a major concern for the Internet of Things as early as its' inception [7] a lot of research has been conducted to identify challenges and possible solutions [8]. IoT is a humongous subject characterized by fast paced innovations from information technology and deeply related to different research disciplines like data science or electronical engineering [9]. Thus, IoT can be described as a melting pot of information technology. This makes it challenging to identify the security relevant components of a concrete type of IoT System and to deduct clear instructions, on what problems have to be addressed and which approaches have already been proposed by research, during system engineering [10].

While *Zhou et al.* [11] state that most studies on IoT security lack applicability Fu et al. [12] showed that valuable insights can be revealed by focusing on a certain environment in which IoT systems are deployed. In this paper we follow this approach and contribute a specialized view on the concrete needs of IoT security in smart warehouses. So, we conduct a literature review on different applications of IoT in smart warehouses and analyze their technological implementation and structure according to the three-layered architecture model. Based on this narrowed view we reevaluate the findings in the current scope of general security which has been surveyed in [13], [14]. So, we bridge the gap between generalized research and solutions in IoT security to the concrete requirements for smart warehouses in the logistics domain.

2 Related work

The research attention of IoT Security and IoT in general is strongly correlated. The research on IoT Security started early [15], [16] with the inception of the internet of things and is dated back more than 15 years ago. Different perspectives on IoT Security challenges were discussed and researched ranging from technical analysis of prevalent vulnerabilities and attacks [17], [18] to more higher-level evaluation of process oriented and architectural implications [19], [20], [21].

Over the years different surveys and reviews summarized the state-of-the-art research and reached a holistic overview about attacks and threats in the IoT [22], [23], [24]. All of the former cited sources explain security mechanisms, attacks, vulnerabilities with a generic IoT system as reference. This system is based off the three- or four-layer IoT architecture reference model which aims to fit and describe all possible instances of IoT platforms and is widely adopted in literature [25], [26]. This not only reveals the humongous nature and diversity of IoT systems but also opposes the question whether concrete insights can be fully deduced by researching abstract architectural layers without knowing the exact system configurations and interactions. On the other hand [27] and [22] surveyed the special security requirements and implications for IoT systems in healthcare. Also, the subcategory of smart home IoT systems has been researched [28] where Lin and Bergmann pointed out that secure auto configuration and lightweight encryption algorithms are crucial to smart home environments [29].

The adoption and different use cases of IoT in logistics are described extensively in [30], [31] and [32] also the adaption in smart warehouses has been surveyed in [4], [33] and [34]. Where all former mentioned authors agree that IoT plays a major role in improving cost and productivity, *Ding et al.* point out that security concerns prevent the wider deployment in logistics [31]. *Abbas et al.* analyzed the security requirements of smart containers and proposed a framework to securely develop IoT applications in the context of smart logistics [35] which provides a rather abstract process recommendation that spares technological. To the best knowledge of the authors there has been no further, generalized research on IoT security in smart logistics or smart warehousing.

3 Setting the stage

In this section we introduce definitions necessary to comprehend the different domains of IoT and IoT security and smart warehousing as well which are touched by our research.

3.1 IoT Layered Architecture or IoT Layer Model

The IoT layered architecture consists of three main levels: Perception Layer, Network Layer, and Application Layer.

- **Perception Layer:** This physical layer captures data using sensors and embedded systems, recognizing geographical factors and intelligent objects in the environment.
- **Network Layer:** Responsible for distributing and storing data, connecting intelligent objects, and facilitating data transport through local and remote transmission.
- **Application Layer:** Interacts with users, offering software resources and defining various IoT applications like Smart Homes, Cloud Computing, and more.

The IoT layered architecture provides a structured framework for organizing IoT components and functions. [36]

3.2 Internet of Things (IoT)

The IoT propels today's digital transformation by combining technologies, protocols, and devices like wireless sensors and innovative wearables. Its impact is particularly notable in healthcare. Embracing various hardware, communication protocols, and services, the IoT offers benefits while also carrying security risks.

Essentially, the IoT is a global network of interconnected objects with unique addresses. It employs sensors, communication protocols, computational power, and data analysis services. From doorbells and sensors to light bulbs and Smart Home devices, the scope of IoT objects is wide-ranging. [37]

3.3 Warehouse

The term "warehouse" refers to a facility where various activities like receiving, storage, monitoring, and distribution of goods take place. The warehouse plays a crucial role in ensuring sales and customer satisfaction. The integration of Internet of Things (IoT) technologies in warehouses enables intelligent identification, tracking, and control using tools like RFID, GPS, and sensors. IoT assists in managing administrative tasks, optimizing operations, and enhancing financial performance and customer satisfaction. [38]

4 Methodology

In this paper, a systematic literature review (SLR) is conducted, to identify the current state of the art of security in IoT-implementing logistical-warehouses. Following [39] and [40] the steps designing the review (in section 4.1) including data abstraction, conducting the review (in section 4.2) are carried out in this section.

4.1 Review – Design

The aim of the paper is to contribute the specialized view on the concrete and current needs of IoT security in smart warehouses. Therefore, the authors strive to particularly identify the security topics that present IoT-Warehouses are confronted with. To effectively illustrate the findings, the relevant points are categorized based on their IoT layer and shared characteristics, which are then subjected to in-depth security analysis. The identified and categorized technical devices and applications are appraised concerning overarching IoT security concerns. The evaluation results will serve to delineate additional research avenues and to heighten awareness of cybersecurity within IoT warehouses.

The identification of the mentioned current IoT security topics in warehouses is rooted in a literature review. For high-quality review-results it is important to identify the literature based on the topic [41]. Therefore, the following steps are executed to select the appropriate literature:

1. Search Terms
2. Selection Criteria
3. Inclusion and exclusion criteria

4.1.1 Search terms

This section outlines the article selection process within the context of this paper's scope. As the research focuses on the Security of IoT-Warehouses the search items “IoT”, “warehouse” and “security” are defined.

The chosen academic database for the literature review is Scopus. As [42] considered Scopus is the most complete academic database, with appropriate search tools. The Scopus database even encompasses most of the literature available in “WoS”, “ACM” and “IEEE”. Therefore, it is posited that the abundant academic literature available in Scopus serves as the solid foundation for a high-quality systematic literature review [41]. After testing multiple combinations of keywords, the search was first narrowed down to English documents containing the keywords “IoT” and “warehouse” in the Article Title, Abstract or Keywords. The query syntax in Scopus was as followed:

(TITLE-ABS-KEY (iot AND warehouse AND security) AND LANGUAGE (english))

108 Documents met these search criteria. Fig. 1 illustrates the distribution of the 108 documents by publication year. It clearly illustrates that the number of published documents per year related to the searched words increased significantly from 2017 to

2023. In the years 2021 and 2022, the number of publications was slightly lower than in previous years before experiencing a sharp increase again in 2023.

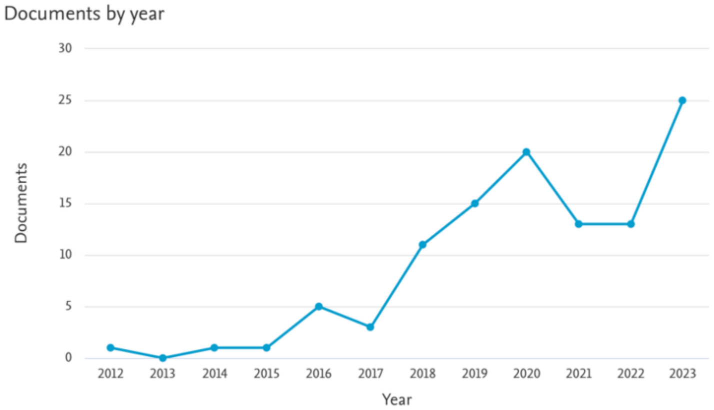

Fig. 1. Annually distributed documents with the key words 'iot', 'warehouse' and 'security' since 2012 [scopus analyze tool]

4.1.2 Selection criteria

As the aim is to identify the current security topics the publication year is now limited to the recent years from 2019 to 2023. Furthermore, the Publication Status was narrowed down to “final” and the document type must be an article or a conference paper. This leads to 66 Documents.

4.1.3 Inclusion and exclusion of criteria

Upon closer examination of the titles of the resulting documents, it becomes evident that the focus of many of documents extends beyond warehousing to encompass broader logistical subjects, such as the entire supply chain or smart cities. To ensure that the focus of the review is on warehouses the search area is being changed. The defined Topics IoT, warehouse and security must now be part of the Document title. This restriction leads to zero results. Considering the research question, the aim is to elaborate security topics in existing IoT warehouse based on current literature. This null set reveals that this specific type of investigation has not yet been conducted, highlighting the need for further research. Consequently, the existing literature on IoT and warehousing will be examined in terms of the techniques and levels employed. Based on these findings, the respective security aspects can then be developed.

For that reason, the next step determines the search topic “security”. This leads to the following final search query syntax in Scopus:

(TITLE (iot AND warehouse) AND LANGUAGE (english)) AND PUBYEAR > 2018 AND PUBYEAR < 2024 AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar"))

It is intended that there are no further search enhancements such as subject area or country. Individual features and requests of warehousing depend highly on the goods which are stored inside of them. Those goods are part of very different industries and countries. Hence, implementing such a restriction would diminish the comprehensiveness of the results. 45 documents meet the defined research criteria.

4.2 Conducting the review

To gain an initial insight into the content of the chosen documents, a Co-Occurrence analysis of Index Keywords using VOS-Viewer software was performed. The result is the net-like-Keyword-arrangement shown in **Fig. 2**:

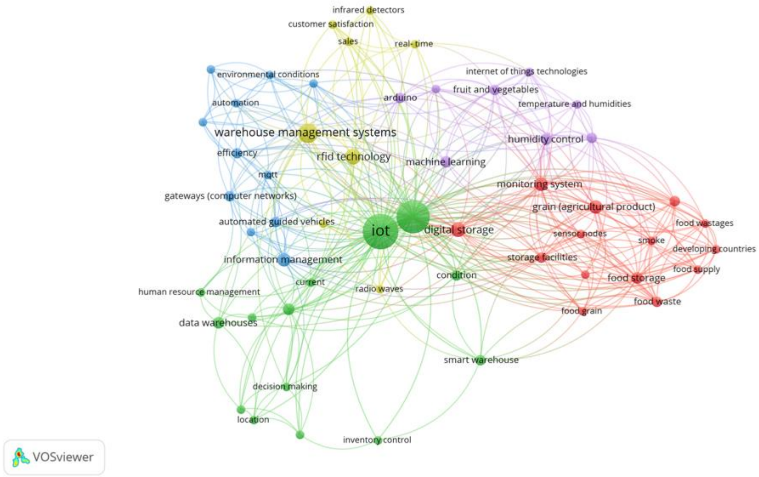

Fig. 2. Visualization of the keywords of the selected documents

Fig. 2 displays the keywords relative to their frequency, within the documents. The frequency of occurrence is represented by the size of the keywords. The connections between these keywords are represented by the curved lines and the coloring. Consistent coloring indicates frequent links between the keywords. These groups with the 'same color' indicate thematic clusters.

As a result of the defined search terms in section 4.1.3, **Fig. 2** illustrates the primary keywords 'iot' and 'warehouses' (large green dots in the center) as most frequently occurring and interconnected. **Table 1**. shows the most frequent keywords adjusted for those two search terms.

keyword	**occurrences**	**total link strength**
warehouse management systems	11	62
rfid technology	7	34
digital storage	6	47
grain (agricultural product)	5	42

monitoring system	5	38
information management	5	30
food storage	4	38
humidity control	4	30
supply chains	4	22
machine learning	4	19

Table 1. Most frequently occurring keywords in the selected literature

In **Table 1** the number in the column ‘occurrences’ represents the number of documents in which the keyword is listed in. The column ‘total link strength’ indicates the number of links of a keyword with another keyword [43]. **Fig. 2** and **Table 1** already provide insight into which might be the most relevant topics in the selected literature, like warehouse management systems, monitoring of storage und controlling actions.

Now it is necessary to examine the specific content and topics of the documents with a screening. The text screening of the documents starts by evaluating the relevance of each document according to the research question based on their title and abstract. After this evaluation and document access verification, 29 documents have been classified as relevant (cf. **Table 2**). The other documents didn’t mainly address the IoT-subject of a logistical warehouse (12 documents) or the authors couldn’t get the full-text access to the documents (4 documents). Next step is the full text screening of the relevant documents. For an overview of IoT deployment in warehouses, the following criteria **maturity level** and **techniques used on each IoT layer** are elaborated for each document. The assessment of maturity level is divided into three levels. Level I includes existing hardware (e.g. sensors) that collects information which is sent to an IoT Platform. Level II includes the functions of Level I as well as an automatically managed reacting response which is actuated by a device. Level III includes the functionalities of Level I and II but the complexity of the data handling, and network structure are high. To clarify the difference between Level II and III we name examples for each level: Activating a fan in a warehouse after a temperature rises above a defined level is Level II. Level III is classified as literature that considers or enables more complex IoT architectures, like communication between several different locations and structures.

Each document is only assigned to the highest maturity level it meets. The result of this maturity level assessment is listed in **Table 2**. It displays the assignment of each examined document of the SLR to a maturity level. It provides an initial overview of the complexity of the IoT elements within the examined warehousing domain.

Maturity Level I collecting and transmitting data	**Maturity Level II** I + reacting to the received data)	**Maturity Level III** II + higher complexity (possible)
[44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56]	[57], [58] [59] [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70]	[71], [72]

Table 2. classification of selected literature by maturity level

5 Results

After the selection of literature and its first clear categorization according to its maturity levels, the results of the detailed full text literature review are proceeded in this section. This detailed examination is oriented towards the objective of presenting the current state of IoT deployment in warehouses to subsequently identify specific security issues later.

Consequently, the literature listed in **Table 2** was further analyzed to determine the specific techniques used on each respective IoT level. The results of the analysis are displayed in **Table 3**. We systematically categorized the devices and techniques mentioned in the documents into their respective IoT layers: perception, network, and application. The number behind each named technique indicates the number of documents it is referred to this IoT-Layer. Alongside listing the respective techniques of each layer in the System Assets column, the Business Assets column details the purposes for which the techniques are utilized.

The layer-categorization served as the basis for a subsequent thematic summarization in each layer. Within the perception layer we classified and numbered the mentioned hardware devices according to their distinct functions, encompassing sensing, positioning, visioning, and actuating. The network layer encompasses the three following types of communication, Device2Device, Device2Cloud and Cloud2device. These terms describe which parties are communicating with each other. For example, in Device2Device, communication occurs between the devices themselves. In Device2Cloud, the device shares information with the cloud, while in Cloud2Device, information flows from the cloud toward the device. The used techniques do not specifically limit the way of communication. Therefore, the techniques are listed generally and are not assigned to one exact communication type. At the application layer we considered the techniques used for data processing, user interface and Data storage. The result of this detailed full-Text analysis is shown in **Table 3**:

Layer	System Assets		Business Assets
Perception	Sensing	DHT-11 (8), DHT-22 (2), LM35 (1), DS18B20 (1), LM235 Temperature, Humidity (1), Moisture sensor (2), MQ2 (3), MQ4 (1) MQ135 (1), MIG-811 - Co2, MOX Gas sensor (1), IR sensors XBee™ RF modules by MaxStream (1), Fire Infrared Radiation sensitive sensor (2), ADIO-PIR Infrared sensors (1), Sensing recognition, Machine Vision (1), Location, GPS – sensors (2), SW420 (1), KY-002 (1), Vibration sensor (4), HS135 (1), HC-SR501 (1) Motion Sensitivity sensor (2), Sound sensor (1), TCS3200 RGB Color sensor (1), Accelerometer ADXL345 (1), Speed, Distance (1), Weight sensors (1), QR Code (1), RFID, SKU identification sensors, RFID (8)	Real time monitoring: cold storage system for humidity, weight, temperature, pressure, light intensity, proximity, infrared IR, accelerometer, ultrasonic, touch, smoke, gas, alcohol, level, moisture, PH, vibration, speed, distance, fire, gps, color
	Positioning	Movement sensor, Location sensor, RFID-Tags RFID-RC522 Reader (10)	Range, Local, Gas, IR Measurements
	Visioning	PIR Sensor - detects infrared radiation (3), Objective lens (1), Electronical optical system (1), QR Code (1), IP-camera, Supersonic.	Motion detection, video, audio, infrared
	Actuating	Brushless DC Fan (2), Heat Bulb (1), Servo Motor (1), DC Motor (1), Robotized machines (1), Ultrasonic rodent repellent (1), AGV Forklift (1), Picking Robot (1), Stacking Robot (1), Engine (1), Light Repellent device (2), Ventilator (1)	Device commands
Network	Device-to-device Device-to-cloud Cloud-to-device	Bluetooth (4), Wi-Fi (18), ZigBee (1), Connection via USB cable (1), LoRa LPWAN Long Range – Low Power Wide Area Network (1), ESP 8266 (1), Blockchain (2), 5G/4G/GSM/LTE (4), RFID (8), NFC (1), LAN (1)	Transmitted data
Application	Data processing User interface Data Storage	Web application (7), Mobile application (8), Smart Warehouse Management System (1), Node-red dashboard (1), MQTT Broker (9), Rn Monitor Web/App (1), Olap dashboard (1), LoRa WAN (2), Blynk Cloud-Server (2), SQL Lite Database (Data Warehouse) (2), OLAP Server Cloud (1), ThingSpeak Platform (1), Local Blockchain (1), Node MCU (1)	Application data, perception data, application process Perception and application data

Table 3. Mapping between architectural layer, technology and business asset in smart warehouse IoT systems

6 Discussion

During our research we reviewed different implementations and use cases of the internet of things in context of the smart warehouse where we were not only able to identify common use cases as shown in **Table 3** but could also extract the architectural focus and IoT maturity level of those solutions. All examined systems leverage the perception layer to sense and interact with their surroundings or other local components of the IoT appliance. RFID technology is used outstanding often in the perception layer to identify physical objects or to achieve accurate indoor positioning. Wireless network connections like Wi-Fi, Bluetooth, Zigbee or GSM are predominantly used to transfer data between the perception layer and the application layer. MQTT is most often used to authenticate devices and route their messages.

About half of the surveyed systems process data locally on the edge layer and forego a dedicated cloud application layer. Nearly all systems are deployed to the user in the form of modern web apps that are either restricted to local access in the warehouse area or globally via the cloud the. There seems to be tendency for IoT systems in smart warehouses to be applied more locally than smart home or industrial application, which are characterized by global scaling and distribution and decentralized data processing in the cloud. Unidirectional message and control flow from perception to application layer is most common in the reviewed systems, where complex machine-to-machine communication or cloud-to-device interactions or globally distributed systems are rarely found in the smart warehouse (also cf. **Table 2**). From our review we deduce the following three assumptions about IoT systems in smart warehouses:

1. The systems are mostly self-contained and have low interaction with third-party systems
2. Local wireless technologies like RFID, Wi-Fi or Bluetooth are key technologies
3. Messages are flowing mostly unidirectionally from device to application layer without triggering complex workflows or reactions

The vision of smart supply chains, of which the smart warehouse is an integral part, requires a high degree of communication between the different fulfillment parties and their information systems [73] but the reviewed IoT systems seem to be unaffected from this trend. The findings about the form and functionality of the IoT in the smart warehouse help us to provide a focused view on possible security threats and challenges, which we will discuss in the following. We found that one of the key drivers of IoT vulnerabilities namely heterogeneity [74], [75] in the perception layer is not of concern, since the systems are mostly closed and focused on a single purpose. Unlike smart home systems where a wide range of different and arbitrary device types need to be supported [76], we can focus on the security of a few well-known components in the warehouse. Also, the mediocre complexity of the use cases potentially impacts the security in a positive way as indicated by *Chowdhury and Zulkernine [77]*. Also, warehouses are not public places and are subject to access restrictions, which reduces the likelihood of an attacker gaining physical access to manipulate or replace a component of the system. This also acts as a barrier for an attacker to leverage side channel, inference or hardware attacks [75].

The comprehensive use of wireless technologies like RFID opens up a certain threat potential as a wide range of attacks exist against it [78], [79] [80]. But countermeasures can be taken since the field of RFID security has been thoroughly researched. Nevertheless, the possibility to rely on insecure defaults and still be vulnerable to threats exists and needs to be excluded by using appropriate countermeasures [81], [82]. The trend of hosting the application layer of warehouse IoT systems locally and not in the cloud narrows the effective attack vectors to the local network but also transfers the responsibility of securing the network environment to the warehouse operator. The application layer is mainly deployed in the form of web applications, which means that different attacks like SQL injections, cross site scripting or remote code execution [83] can be possibly carried out and corresponding countermeasures have to be taken.

Our research shows that practitioners should focus on guarding against vulnerabilities in the application layer and firmware of the components as well as the used wireless technology while building IoT applications in the smart warehouse because the most threat potential originates from there. As a second step detailed threat modelling should be conducted to reveal further security challenges of the concrete application, which is supported by the potential smaller size of warehouse appliances [84].

7 Conclusion

We contributed a specialized view on the current state of IoT in the context of smart warehousing in the larger landscape of smart logistics and supply chains and gave an overview about different use cases employed. We found that the use of IoT is in an initial stage where systems are not tightly interconnected or integrated within different information systems and the diversity of deployed components remains low. Our research reveals that wireless network technology is heavily used and that a secure standard of RFID can greatly benefit the security of IoT systems in the warehouse.

The analysis of Index Keywords using VOS-Viewer software proved to be a valuable tool in visually representing the frequency and interconnections of keywords within the selected documents, facilitating a holistic understanding of the literature landscape. This visualization effectively highlighted the centrality of 'iot' and 'warehouses' as the predominant keywords, emphasizing their significance in the context of IoT deployment in smart warehousing.

Furthermore, we deduced common security challenges that are likely to be found in those systems. Also, by categorizing IoT architecture layers and discussing the assets associated with each layer, the analysis offers a structured view of the technical components involved. It is evident that while IoT systems in smart warehouses are relatively closed and focused on specific purposes, they still face security challenges, particularly in areas such as wireless communication and the use of web applications.

Exceptions are inherent in the generalized perspective we provided. When designing or securing an IoT application in the smart warehouse our findings cannot replace an in-depths analysis of the concrete system but can serve as a starting point. Also, our research is limited by the literature constrained by the search parameters we set for the review. The focus on research in the closer past excludes older literature that could have impact on our findings. Also did we limited the research to academic contribution.

Finally, our research serves as a foundation for understanding the current state of IoT in smart warehousing. Also, future research should aim to track and analyze these developments to provide more nuanced and updated insights into the state of IoT in this sector.

References

[1] Y. Song, F. R. Yu, L. Zhou, X. Yang, and Z. He, “Applications of the Internet of Things (IoT) in Smart Logistics: A Comprehensive Survey,” *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4250–4274, 2021, doi: 10.1109/JIOT.2020.3034385.

[2] F. Al-Turjman and A. Malekloo, “Smart parking in IoT-enabled cities: A survey,” *Sustainable Cities and Society*, vol. 49, p. 101608, 2019, doi: 10.1016/j.scs.2019.101608.

[3] S. Tadić, M. Krstić, M. Kovač, and N. Brnjac, “Evaluation of Smart City Logistics Solutions,” *PROMTT*, vol. 34, no. 5, pp. 725–738, 2022, doi: 10.7307/ptt.v34i5.4122.

[4] I. Affia and A. Aamer, “An internet of things-based smart warehouse infrastructure: design and application,” *JSTPM*, vol. 13, no. 1, pp. 90–109, 2022, doi: 10.1108/JSTPM-08-2020-0117.

[5] M. G. Khan, N. U. Huda, and U. K. U. Zaman, “Smart Warehouse Management System: Architecture, Real-Time Implementation and Prototype Design,” *Machines*, vol. 10, no. 2, p. 150, 2022, doi: 10.3390/machines10020150.

[6] W. Ding, “Study of Smart Warehouse Management System Based on the IOT,” in *Advances in Intelligent Systems and Computing*, vol. 180, *Intelligence computation and evolutionary computation: Results of 2012 International Conference of Intelligence Computation and Evolutionary Computation, ICEC 2012, held July 7, 2012, in Wuhan, China*, Z. Du, Ed., Berlin, Heidelberg: Springer, 2013, pp. 203–207.

[7] R. A. Dolin, “Deploying the "Internet of things",” in *International Symposium on Applications and the Internet, 2006: SAINT 2006 ; 23 - 27 Jan. 2006, [Phoenix, Arizona ; proceedings*, Phoenix, AZ, USA, 2006, 4 pp-219.

[8] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the Internet of Things: perspectives and challenges,” *Wireless Netw*, vol. 20, no. 8, pp. 2481–2501, 2014, doi: 10.1007/s11276-014-0761-7.

[9] D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.

[10] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013, doi: 10.1016/j.comnet.2012.12.018.

[11] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, 2019, doi: 10.1109/JIOT.2018.2847733.

[12] K. Fu *et al.*, “Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things,” Jul. 2020. [Online]. Available: https://arxiv.org/pdf/2008.00017

[13] P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T.-H. Kim, “A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review for Existing Solutions, Future Implications, and Research Challenges,” *IEEE Access*, vol. 9, pp. 25344–25359, 2021, doi: 10.1109/ACCESS.2021.3057766.

[14] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, “A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review,” (in eng), *Sensors (Basel, Switzerland)*, vol. 23, no. 8, 2023, doi: 10.3390/s23084117.

[15] R. H. Weber, “Internet of Things – New security and privacy challenges,” *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010, doi: 10.1016/j.clsr.2009.11.008.

[16] C. P. Mayer, “Security and Privacy Challenges in the Internet of Things,” (in en), 2009, doi: 10.14279/tuj.eceasst.17.208.205.

[17] I. Butun, P. Osterberg, and H. Song, “Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 616–644, 2020, doi: 10.1109/COMST.2019.2953364.

[18] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges,” in *20th IEEE Symposium on Computers and Communication (ISCC): 20th IEEE Symposium on Computers and Communication (ISCC) took place 6-9 July 2015 in Lanarca, Cyprus*, Larnaca, 2015, pp. 180–187.

[19] M. Abomhara and G. M. Kien, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,” *JCSM*, vol. 4, no. 1, pp. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.

[20] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, “IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey,” (in eng), *Sensors (Basel, Switzerland)*, vol. 18, no. 9, 2018, doi: 10.3390/s18092796.

[21] M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,” in *2015 IEEE World Congress on Services (SERVICES 2015): New York City, New York, USA, 27 June - 2 July 2015*, New York City, NY, USA, 2015, pp. 21–28.

[22] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[23] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[24] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things,” *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, 2017, doi: 10.1109/JIOT.2017.2694844.

[25] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, “Perception layer security in Internet of Things,” *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019, doi: 10.1016/j.future.2019.04.038.

[26] N. M. Kumar and P. K. Mallick, “The Internet of Things: Insights into the building blocks, component interactions, and architecture layers,” *Procedia Computer Science*, vol. 132, pp. 109–117, 2018, doi: 10.1016/j.procs.2018.05.170.

[27] A. Chacko and T. Hayajneh, “Security and Privacy Issues with IoT in Healthcare,” *EAI Endorsed Transactions on Pervasive Health and Technology*, vol. 0, no. 0, p. 155079, 2018, doi: 10.4108/eai.13-7-2018.155079.

[28] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, “Security and privacy issues for an IoT based smart home,” in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO): May 22-26, 2017, Opatija, Croatia : proceedings*, Opatija, Croatia, 2017, pp. 1292–1297.

[29] H. Lin and N. Bergmann, “IoT Privacy and Security Challenges for Smart Home Environments,” *Information*, vol. 7, no. 3, p. 44, 2016, doi: 10.3390/info7030044.

[30] D. Crnjac Milić, I. Dujmenović, and M. Peko, “An Approach to the Application of the Internet of Things in Logistics,” *Teh. glas. (Online)*, vol. 17, no. 1, pp. 134–140, 2023, doi: 10.31803/tg-20220609190233.

[31] Y. Ding, M. Jin, S. Li, and D. Feng, “Smart logistics based on the internet of things technology: an overview,” *International Journal of Logistics Research and Applications*, vol. 24, no. 4, pp. 323–345, 2021, doi: 10.1080/13675567.2020.1757053.

[32] A. Rejeb, S. Simske, K. Rejeb, H. Treiblmaier, and S. Zailani, “Internet of Things research in supply chain management and logistics: A bibliometric analysis,” *Internet of Things*, vol. 12, p. 100318, 2020, doi: 10.1016/j.iot.2020.100318.

[33] D. Zhang, L. G. Pee, and L. Cui, “Artificial intelligence in E-commerce fulfillment: A case study of resource orchestration at Alibaba’s Smart Warehouse,” *International Journal of Information Management*, vol. 57, p. 102304, 2021, doi: 10.1016/j.ijinfomgt.2020.102304.

[34] X. Liu, J. Cao, Y. Yang, and S. Jiang, “CPS-Based Smart Warehouse for Industry 4.0: A Survey of the Underlying Technologies,” *Computers*, vol. 7, no. 1, p. 13, 2018, doi: 10.3390/computers7010013.

[35] A. W. Abbas, S. Nawaz Khan Marwat, S. Ahmed, A. Hafeez, K. Ullah, and I. U. Khan, “Proposing Model for Security of IoT Devices in Smart Logistics: A Review,” in *Idea to innovation for building the knowledge economy: 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies : iCoMET 2019 : January 29-30, 2020*, Sukkur, Pakistan, 2020, pp. 1–4.

[36] N. Chaurasia and P. Kumar, “A comprehensive study on issues and challenges related to privacy and security in IoT,” *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 4, p. 100158, 2023, doi: 10.1016/j.prime.2023.100158.

[37] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, “A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis,” (in eng), *Sensors (Basel, Switzerland)*, vol. 20, no. 13, 2020, doi: 10.3390/s20133625.

[38] M. Dotoli, N. Epicoco, M. Falagario, N. Costantino, and B. Turchiano, “An integrated approach for warehouse analysis and optimization: A case study,”

Computers in Industry, vol. 70, pp. 56–69, 2015, doi: 10.1016/j.compind.2014.12.004.

[39] D. Moher, A. Liberati, J. Tetzlaff, and Douglas G., *Preferred Reperoting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement*.

[40] H. Snyder, “Literature review as a research methodology: An overview and guidelines,” *Journal of Business Research*, vol. 104, pp. 333–339, 2019, doi: 10.1016/j.jbusres.2019.07.039.

[41] J. Webster and Watson Richard T., “Analyzing the Past to Prepare for the Future: Writing a Literature Review,” *MIS Quarterly*, no. 26.2, 2002. [Online]. Available: https://www.jstor.org/stable/4132319

[42] A. Valente, M. Holanda, A. M. Mariano, R. Furuta, and D. Da Silva, “Analysis of Academic Databases for Literature Review in the Computer Science Education Field,” in pp. 1–7.

[43] Nees Jan van Eck and Ludo Waltman, “VOSviewer Manual,”

[44] L. J, L. S. V. S, M. R, and M. R, “Automated food grain monitoring system for warehouse using IOT,” *Measurement: Sensors*, vol. 24, p. 100472, 2022, doi: 10.1016/j.measen.2022.100472.

[45] V. Parkhi, N. Chavhan, S. Chandak, B. Chaware, and P. Bongarde, “An IoT Based Environment Monitoring & Controlling System for Food Grain Warehouse,” in pp. 217–227.

[46] V. Bakyalakshmi, M. Anithamary, R. Bharathy, and U. Jhanani Shree, “Systematized Warehouse Based On IoT,” *J. Phys.: Conf. Ser.*, vol. 1818, no. 1, p. 12226, 2021, doi: 10.1088/1742-6596/1818/1/012226.

[47] N. K. Nagrale, V. N. Nagrale, and A. Deshmukh, “Iot Based Smart Food Grain Warehouse,” in pp. 1–5.

[48] A. Rahman, Ermatita, and D. Budianta, “Data Warehouse Design for Soil Nutrients with IoT Based Data Sources,” in pp. 181–186.

[49] M. Meyliana, E. Fernando, Surjandy, and C. Cassandra, “Architecture Blockchain Technology with IoT for Monitoring Drug Warehouse,” in pp. 77–81.

[50] M. K. Hasan, M. Junjie, A. K. M. Ahasan Habib, A. Al Mamun, T. M. Ghazal, and R. A. Saeed, “IoT-Based Warehouse Management System,” in pp. 1–6.

[51] G. Rajesh, B. Saroja, A. Gurulakshmi, and R. S. Malladi, “Enhanced Time-to-Time Monitoring and Surveillance in Agriculture Warehouse for Diverse Harvest Crop Yields through IoT Gadget,” in pp. 172–175.

[52] R. Azevedo, J. P. Silva, N. Lopes, A. Curado, L. J. Nunes, and S. I. Lopes, “Designing an IoT-enabled Data Warehouse for Indoor Radon Time Series Analytics,” in pp. 1–6.

[53] Z. Yutan and H. Gengbao, “Exploration and analysis of intelligent IoT based on the difficult environment of warehouse indoor positioning,” in pp. 418–421.

[54] A. Shukla, G. Jain, K. Chaurasia, and U. Venkanna, “Smart Fruit Warehouse and Control System Using IoT,” in pp. 40–45.

[55] K. Srilatha, D. Rushikeshwar, and N. Bhaskar Chowdary, “Smart Warehouse Monitoring System using Internet of Things (IoT),” in pp. 1–6.

[56] R. Silapunt, W. Panpanyatep, and G. Boonsothonsatit, “Design and Development of the Smart Object for the IoT-enabled Smart Warehouse,” in

Proceedings of the 2022 International Electrical Engineering Congress: (iEE-CON 2022), Khon Kaen, Thailand, 2022, pp. 1–4.

[57] Y. Feng and D. Luo, “IoT-based Intelligent Management System of Personnel Archives Warehouse,” *CADandA*, pp. 147–157, 2023, doi: 10.14733/ca-daps.2023.S10.147-157.

[58] S. Stadler, E. R. Borrero, J. Zauner, and C. Hanshans, “Development and Implementation of an OpenSource IoT Platform, Network and Data Warehouse for Privacy-Compliant Applications in Research and Industry,” *Current Directions in Biomedical Engineering*, vol. 7, no. 2, pp. 507–510, 2021, doi: 10.1515/cdbme-2021-2129.

[59] K. Mohanraj*, S. Vijayalakshmi, N. Balaji, R. Chithrakkannan, and R. Karthikeyan, “Smart Warehouse Monitoring Using Iot,” *IJEAT*, vol. 8, no. 6, pp. 3597–3600, 2019, doi: 10.35940/ijeat.F9355.088619.

[60] B. K. RAİ, “IoT Based Humidity and Temperature Control System for Smart Warehouse,” *Gazi University Journal of Science*, vol. 36, no. 1, pp. 173–188, 2023, doi: 10.35378/gujs.993959.

[61] J. Jose, B. K. Samhitha, M. Maheswari, M. Selvi, and S. C. Mana, “IoT based Smart Warehouse and Crop Monitoring System,” in pp. 473–476.

[62] S. Banerjee, A. K. Saini, H. Nigam, and V. Vijay, “IoT Instrumented Food and Grain Warehouse Traceability System for Farmers,” in pp. 1–4.

[63] K.-C. Chien, D.-Z. Zhuang, and W.-G. Teng, “Assisting Order Picking and Inventory Tracking in Warehouses with an IoT Gateway,” in pp. 51–57.

[64] L. Wang, A. D. J., and T. Vadivel, “Research on Logistic Warehouse Scheduling Management With IoT and Human-Machine Interface,” *International Journal of Information Systems and Supply Chain Management*, vol. 15, no. 4, pp. 1–15, 2022, doi: 10.4018/IJISSCM.305846.

[65] W.-T. Sung and C.-Y. Lu, “Smart Warehouse Management Based on IoT Architecture,” in *2018 International Symposium on Computer, Consumer and Control: IS3C 2018 : 6-8 December 2018, Taichung, Taiwan*, Taichung, Taiwan, 2018, pp. 169–172.

[66] F. Men, J. Guo, and Y. Luan, “IoT Warehouse Management System Based on ACO Path Planning,” in pp. 1008–1013.

[67] V. Ranjith, E. N. Sriravinaa, S. Subashree, and K. Raguvaran, “Development of IoT Enabled Vegetable Stockpile Warehouse Monitoring System to Support Farmers,” in *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, Coimbatore, India, Jun. 2023 - Jun. 2023, pp. 1006–1013.

[68] A. Sagaya Selvaraj and S. Anusha, “RFID Enabled Smart Data Analysis in a Smart Warehouse Monitoring System using IoT,” *J. Phys.: Conf. Ser.*, vol. 1717, p. 12022, 2021, doi: 10.1088/1742-6596/1717/1/012022.

[69] A. Bukhamseen, M. Alabdullah, K. Bin Gaufan, and M. Mysorewala, “A Warehouse Storage and Retrieval System Using IoT and Autonomous Vehicle,” in *2023 9th International Conference on Automation, Robotics and Applications (ICARA)*, Abu Dhabi, United Arab Emirates, Feb. 2023 - Feb. 2023, pp. 346–350.

[70] S. P. Manisha and K. Haripriya H., “Design-And-Development-Of-Automated-Storage-And-Retrieval-System-asrs-For-Warehouse-Using-Iot-And-Wireless-Communication,” pp. 105–108, 2019. [Online]. Available: http://www.ijstr.org/final-print/sep2019/Design-And-Development-Of-Automated-Storage-And-Retrieval-System-asrs-For-Warehouse-Using-Iot-And-Wireless-Communication.pdf

[71] L. Heng and Y. Kaiyou, “Research on Smart Warehouse of Emergency Supplies Based on Cloud Computing and IoT,” in pp. 693–697.

[72] R. Prasad Tripathy, M. Ranjan Mishra, and S. R. Dash, “Next Generation Warehouse through disruptive IoT Blockchain,” in pp. 1–6.

[73] L. Wu, X. Yue, A. Jin, and D. C. Yen, “Smart supply chain management: a review and implications for future research,” *The International Journal of Logistics Management*, vol. 27, no. 2, pp. 395–417, 2016, doi: 10.1108/IJLM-02-2014-0035.

[74] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, “Edge Computing Security: State of the Art and Challenges,” *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019, doi: 10.1109/JPROC.2019.2918437.

[75] S. K. K, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, “Security Enhancements to System on Chip Devices for IoT Perception Layer,” in *iNIS 2017: 2017 IEEE International Symposium on Nanoelectronic and Information Systems : proceedings : 18-20 December 2017, Bhopal, India*, Bhopal, 2017, pp. 151–156.

[76] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, “Smart home security: challenges, issues and solutions at different IoT layers,” *J Supercomput*, vol. 77, no. 12, pp. 14053–14089, 2021, doi: 10.1007/s11227-021-03825-1.

[77] I. Chowdhury and M. Zulkernine, “Using complexity, coupling, and cohesion metrics as early indicators of vulnerabilities,” *Journal of Systems Architecture*, vol. 57, no. 3, pp. 294–313, 2011, doi: 10.1016/j.sysarc.2010.06.003.

[78] R. Jain, D. Kumar Chaudhary, and S. Kumar, “Analysis of Vulnerabilities in Radio Frequency Identification (RFID) Systems,” in *Proceedings of the 8th International Conference Confluence 2018 on Cloud Computing, Data Science and Engineering: 11th-12th January 2018, Amity College, Noida, Uttar Pradesh, India*, Noida, 2018, pp. 453–457.

[79] A. Juels, “RFID security and privacy: a research survey,” *IEEE J. Select. Areas Commun.*, vol. 24, no. 2, pp. 381–394, 2006, doi: 10.1109/JSAC.2005.861395.

[80] T. V. Morozova and V. V. Gurov, “Research in RFID vulnerability,” in *Proceedings of the 2017 IEEE Russia Section Young Researchers in Electrical and Electronic Engineering Conference (2017 ElConRus): February 1-3, 2017, St. Petersburg, Russia, 2017*, St. Petersburg and Moscow, Russia, 2017, pp. 501–503.

[81] G. Avoine and P. Oechslin, “A Scalable and Provably Secure Hash-Based RFID Protocol,” in *Third IEEE International Conference on Pervasive Computing and Communications: Including workshops papers ; Kauai Island, Hawaii, 8 - 12 March 2005*, Kauai Island, HI, USA, 2005, pp. 110–114.

[82] P. Gope, R. Amin, S. K. Hafizul Islam, N. Kumar, and V. K. Bhalla, “Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment,” *Future Generation Computer Systems*, vol. 83, pp. 629–637, 2018, doi: 10.1016/j.future.2017.06.023.

[83] B. Reddy Bhimireddy, A. Nimmagadda, H. Kurapati, L. Reddy Gogula, R. Rani Chintala, and V. Chandra Jadala, “Web Security and Web Application Security: Attacks and Prevention,” in *9th International Conference on Advanced Computing and Communication Systems: March 17th & 18th, 2023*, Coimbatore, India, 2023, pp. 2095–2096.

[84] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, “STRIDE-based threat modeling for cyber-physical systems,” in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Torino, Italy, 26-29 September 2017 : conference proceedings*, Torino, 2017, pp. 1–6.

Division of participation

Dominik Deschner

- Topic proposal & summary
- Abstract (completely)
- Structural & academic proposal for the chapter “setting the stage”
- Introduction (completely)
- Related work (completely)
- Discussion (completely)
- Text screening
- Conclusion together with Christian Schlier

Christian Iosif Schlier:

- Literature research
- Text screening
- Results, part of text together with Annika Stempfle
- IoT Layer Table Nr.3
- Presentation together with Annika Stempfle
- Conclusion together with Dominik Deschner

Annika Stempfle:

- Topic identification and delimitation
- Methodology (completely)
- Text screening
- Results, part of text together with Christian Schlier
- Presentation together with Christian Schlier

Jochen Welte:

- Terminology research (IoT, logistics, cybersecurity)
- Text screening
- Setting the stage
- IoT security topic research and topic preparation