Comparing On-Premise IoT Platforms: Empowering University of Things Ecosystems with Effective Device Management

Mevludin Blazevic[a] and Dennis M. Riehle[b]

Institute for IS Research, University of Koblenz, Universitätsstraße 1, Koblenz, Germany

Keywords: Internet of Things, Platform, Smart Campus, LoRaWAN.

Abstract: This paper presents a comparative evaluation of on-premise Internet of Things (IoT) platforms utilizing the Utility Analysis (UA) method within a university campus environment. The market analysis and evaluation are conducted systematically using a scoring procedure, guided by expert interviews to identify functional and non-functional requirements for the IoT device management in the University of Things (UoT) setup. After a market exploration considering the exclusion criteria, ”no on-premise installation” and ”no license-free cost models”, five IoT platforms are assessed against predefined evaluation criteria derived from these requirements. Among the evaluated platforms, the Long-Range Wide Area Network (LoRaWAN) Network Server ChirpStack is the most suitable software solution, demonstrating superior utility value. Chirpstack may be integrated into the university’s own Infrastructure as a Service (IaaS) cloud infrastructure, enhancing data privacy, security, and application control. The primary objective of this study is to identify an optimal IoT platform capable of meeting stakeholder requirements for the exploration of available solutions. Recognizing the critical role of the IoT platform within the Smart Campus/UoT ecosystem, this research contributes to the enhancement of a Smart Campus infrastructure by facilitating efficient IoT sensor and gateway management.

1 INTRODUCTION

The Internet of Things (IoT) refers to the network of interconnected devices embedded with sensors, software, and other technologies, enabling them to collect and exchange data. This interconnected ecosystem enables seamless communication and automation across various domains, revolutionizing how we interact with and manage our physical environments.

As the IoTs expands in significance and prevalence, the importance of IoT platforms as pivotal elements within IoT systems grows as well. These platform solutions differ in complexity, each offering distinct functionalities. IoT platforms are comprehensive software solutions designed to facilitate the management, connectivity, and data processing of interconnected devices within the Internet of Things ecosystem. Consequently, organizations aiming to integrate an IoT platform alongside their current Information Technology (IT) setup encounter the challenge of choosing the most appropriate one for their particular needs from a plethora of available software solutions. Evaluating the functional aspects serves as an important criterion for selection in this process (cf. (Fahmideh and Zowghi, 2020; Guth et al., 2018; Lempert and Pflaum, 2019)).

The objective of this paper is to perform a Utility Analysis (UA) centered on on-premise IoT platforms currently accessible in the market, aiming to establish both functional and non-functional criteria to inform our selection process. Additionally, the paper endeavors to provide a guide based on best practices for selecting an on-premise IoT platform suitable for managing IoT devices and sensors within a University of Things (UoT) or Smart Campus infrastructure and beyond.

A Smart Campus or UoT can be viewed as a subcomponent of a Smart City, while both entities share a similar framework, with a Smart Campus essentially functioning as a small-scale Smart City ((Zhang et al., 2022; Fortes et al., 2019; Silva-da Nóbrega et al., 2022; Vasileva et al., 2018)). Within our real-world implementation of the IoT infrastructure on the university campus, approximately 100 sensors and 7 Long-Range Wide Area Network (LoRaWAN) gateways are deployed. These sensors conduct various measurements encompassing air quality (specifically targeting fine dust pollution), meteorological parameters, temperature, wind speed, and direction, Ultraviolet (UV) radiation, precipitation levels, and hailstone dimensions within the outdoor campus area. Indoors, recorded metrics include air pressure, Carbon Diox-

[a] https://orcid.org/0000-0003-0347-7392

[b] https://orcid.org/0000-0002-5071-2589

Blazevic, M. and Riehle, D.
Comparing On-Premise IoT Platforms: Empowering University of Things Ecosystems with Effective Device Management.
DOI: 10.5220/0012727000003705
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024)*, pages 310-320
ISBN: 978-989-758-699-6; ISSN: 2184-4976

ide (CO_2) levels, temperature, and humidity. Managing these heterogeneous IoT datasets transmitted via LoRaWAN requires structured management to be able to evaluate it appropriately and use it advantageously. Furthermore, an in-house hosted IoT platform is important for registering and overseeing the IoT installed devices and gateways at the university campus alongside the collected data. This presents several benefits for a Smart Campus infrastructure, including the potential to seamlessly integrate the platform with other IoT applications like data platforms and visualization tools. By using a free open-source solution, it also allows the development of extensions or adjustments to the software. In addition, it offers more flexibility in installation and user management. External hosted systems like The Things Network have some restrictions such as a limited number of devices or API keys. The latter is relevant for a Smart Campus application for the integration and interaction with other IoT applications such as data platforms. The research objectives for this paper are described as follows:

RO1: Identification of requirements for an IoT platform for a Smart Campus infrastructure, considering potentially existing IoT infrastructures.

RO2: Execution of a market analysis followed by evaluating appropriate IoT platforms.

In the subsequent section, an overview of the concept of IoT platforms and related work within the Smart Campus/UoT domain is provided. Following this, the Research Methodology for this work is presented. Subsequently, the presentation of all identified stakeholder requirements is given. Utilizing these requirements, evaluation categories are formulated for subsequent analysis. Five IoT platforms identified from the market analysis are evaluated using UA. Finally, the findings of this study are summarized, limitations are acknowledged, and an outlook is provided for further research building upon this work.

2 BACKGROUND

2.1 IoT, Smart Campus and IoT Platforms

A broad spectrum of definitions for the IoT is found across scientific and non-scientific literature, as evidenced by works such as those by Baiyere et al. (2020), Chui et al. (2020), Miorandi et al. (2012), and Rayes and Salam (2017). These definitions commonly emphasize the integration of physical objects with digital technologies. IoT can be thus described as a network of connections between digital technologies and physical objects, enabling the latter to acquire computational capabilities and interact autonomously or with human intervention ((Baiyere et al., 2020)). Moreover, various IoT domains were established, including Smart City, Smart Buildings, Smart Agriculture, Smart Manufacturing, and numerous others ((Gardašević et al., 2017; Ibarra-Esquer et al., 2017). IoT sensors offer a variety of new services accross these domains, for instance, sensor-based smart parking solutions in smart cities ((Riehle et al., 2023)) or smart air-quality monioring in smart buildings ((Arz von Straussenburg et al., 2023)). According to Zhang et al. (2022), a Smart Campus is regarded as a component within the broader domain of a Smart City, encompassing diverse subdomains such as Smart Education, Smart Assessment, Smart Learning, Smart Teaching, and others. These subdomains are supported by different information technologies ((Martínez et al., 2021; Mircea et al., 2021)).

The increasing applications and popularity of IoT and the resulting investments by companies in these technologies have created strong competition in the market, leading to multiple existing IoT standards. In addition, connectivity requirements of IoT devices vary depending on the use case and IoT domain, which means that different protocols are used ((Bhajantri and S., 2020)), which leads to a large number of IoT platforms and connectivity standards such as LoRaWAN on the market ((Barros et al., 2022)). This diversity in protocols, coupled with the multitude of use cases and software companies, leads to a large number of IoT platforms available in the market ((Barros et al., 2022)).

An IoT platform serves as a middleware component within a holistic IoT system, facilitating the exchange of data between edge devices and enterprise applications in both directions. It represents a multilayered technology that facilitates the provisioning and administration of IoT devices and services, effectively overseeing the deployment process for IoT applications in enterprises ((Barros et al., 2022; Fahmideh and Zowghi, 2020; Guth et al., 2018)).

IoT platforms from different manufacturers offer varying core functionalities tailored to diverse application contexts, often lacking comprehensive coverage of all required functions. These platforms receive the data collected by sensors from the IoT devices through protocols such as Wifi, Bluetooth, Zigbee, Z-wave, and LoRaWAN. Serving as middleware components, IoT platforms provide diverse functionalities for data processing and transmission, separating them from systems purely addressing IoT data storage ((Wolters et al., 2023)). While most IoT platforms primarily focus on establishing connections to IoT devices and managing them through device management functionalities, data visualization features are not consistently integrated and are frequently supplemented by third-party software (cf. (Guth et al., 2018; Fahmideh and Zowghi, 2020; Elgedawy and Shoukry, 2022; Toutsop et al., 2021))

2.2 Related Work

A brief exploration of scientific literature using Scopus and specifically targeting the article titles, abstracts, and keywords for ”iot platform comparison” and ”iot platform evaluation” yields merely six findings.

In 2019, Panduman et al. (2019) conducted a comparative examination of five distinct IoT platforms within the Smart Factory domain. Alongside the *Thingsboard* platform, the analysis encompassed the *KAA platform*, *Microsoft Azure IoT*, *AWS IoT*, and *Thingspeak*. The study's findings indicate that Azure IoT and the KAA platform predominantly fulfill the specified criteria, albeit these criteria are specifically tailored to the Smart Factory domain.

In their 2019 work, Berawi et al. (2019) introduced *Chief-Screen 1.0*, a specialized IoT platform for the construction domain. The authors gathered requirements and design considerations through group and expert interviews, integrating them into the platform's development. However, they did not compare *Chief-Screen 1.0* with other platforms.

Kugler et al. (2021) discuss the creation of a method for selecting IoT platforms along given criteria such as security, pricing and usability. They also propose a workflow for setting up and deploying these platforms. However, they do not offer an in-depth comparison of existing IoT platforms on the market.

Like Kugler et al. (2021), García-Valls and Palomar-Cosín (2022) focus on presenting an evaluation methodology for IoT platforms, using healthcare as an illustrative domain. They offer a workflow for selecting and assessing these platforms, specifically conducting performance evaluations on cloud-based platforms in their application example. Furthermore, no market analysis is carried out in their study.

Nasser et al. (2023) also focus on constructing a model for evaluating IoT platforms. Unlike previous studies, their model encompasses both technical and business criteria. Input and design parameters for the evaluation model were established through a literature review. However, the study does not include a comparative analysis of the existing IoT platforms in the market.

3 METHODOLOGY

When selecting the most suitable IoT platform from numerous options, scoring procedures such as utility value analysis are leveraged. Scoring models involve quantitatively assessing objects or subjects based on weighted criteria. UA, a type of scoring, compares decision alternatives against each other ((Kühnapfel, 2021; Cascio, 1996)). Adapted for this research work, the procedure steps outlined by Kühnapfel (2021) are as follows:

In *step 1*, the university describes its objective and outlines the prerequisites for an IoT platform. The objective clarifies the rationale behind employing UA. The requirements and design considerations for the selecting process considering the current IoT infrastructure are gathered through expert interviews and brainstorming techniques (cf. (Geschka and Geschka, 2014; Soest, 2023)) specified requirements are consolidated into a requirements table, which serves to establish inclusion criteria for IoT platforms following the guidelines for requirements engineering in software development by Kassab (2022) and Lamsweerde (2009).

In *step 2*, five decision alternatives are chosen based on predefined exclusion criteria. These criteria are defined through interviews with university stakeholders.

In *Step 3*, the evaluation criteria (decision criteria) are determined based on the identified requirements. The criteria are essential for the success of this methodology and should therefore be chosen carefully and refer to the properties of software and illustrate the usefulness of a decision alternative. It is important to note that there are criteria that are viewed objectively and criteria that can be viewed subjectively.

Step 4 includes the weighting of the decision criteria based on subjective assessment using percentages, where the sum of the individual weights is 100%. In order to find out the importance of the respective criteria, the paired comparison method ((David, 1963)) was used.

In *Step 5*, a scale is defined for evaluating the achievement of the goal criterion. It was decided to employ a numerical ordinal scale ranging from 0 to 4.

Step 6 includes evaluating the decision criteria. Here, points are awarded based on the predefined scoring system. To conduct the evaluation, data was sourced from the manufacturer documentation of each IoT platform and insights gleaned from the test setups of the on-premise installations.

In *Step 7*, the utility value or score is calculated. The points awarded for each criterion are multiplied by their respective weightings to determine the criterion's utility value for a decision alternative. The total utility value is then calculated by summing up these individual utility values.

Step 8 involves making the decision and explaining the result. Here, a decision is made based on the calculated overall utility values and summarized in a short discussion.

4 REQUIREMENTS ELICITATION

To assess an appropriate IoT platform for the university's application context, a thorough requirement analysis is necessary. This involves conducting expert interviews and employing brainstorming techniques ((Geschka and Geschka, 2014; Soest, 2023)). In this context, the administrators of the IoT devices that were previously managed via The Things Network over the past three years are considered experts. With increasing experience working with The Things Network in the Smart Campus area, essential needs have surfaced that surpass the capabilities of The Things Network. Of utmost significance is the need to accommodate storage for any number of sensors, gateways, and Application Programming Interfaces (API) keys. Unfortunately, this is not possible with The Things Network as only a limited number of devices and API keys can be stored. An inhouse hosted on-premise IoT platform offers the advantage by enabling the creation of multiple platform instances tailored for educational purposes, specifically catering to students studying IoT. Therefore, an open-source solution is necessary. These instances provide a hands-on experience during seminars or exercises within lectures. Furthermore, the flexibility to spin up additional instances on the university's cloud infrastructure further enhances accessibility and scalability, empowering students to explore IoT concepts in a practical and interactive environment. The requirements for an IoT platform are closely linked to the operation of the Smart Campus LoRaWAN infrastructure. For this reason, relevant terms such as EUI can be found in the LoRaWAN requirement tables (1 and 2). The Extended Unique Identifier (EUI) or DevEUI is a 64-bit identifier that is provided to a manufacturer of IoT devices and is standardized. The principle is comparable to the concept of MAC addresses for addressing computers on Ethernet. The only difference is the length of the identifier. The IEEE Registration Authority is responsible for assigning an EUI area for manufacturers.[1]

The requirements are categorized into functional and non-functional aspects. Functional requirements outline specific functions that the IoT platform must prioritize implementing (Table 1). Non-functional requirements, on the other hand, pertain to performance standards and quality attributes of the software, ensuring the necessary functionality is delivered (Table 2). The goal was to prioritize the identified requirements based on their importance. This prioritization is crucial for evaluating the defined categories during the subsequent UA. This process is significant due to the presence of exclusion criteria, which, if not met, can result in immediate rejection of the software as they are considered essential or strongly desired by the university environment. Vice-versa, if other requirements of lesser significance are unmet, the selection process does not necessarily lead to rejection but could still influence decision-making among several options. To organize these priorities effectively, the requirements table is segmented into "must-have," "should-have," and "nice-to-have" categories. Must-have requirements hold the highest priority and encompass the exclusion criteria. While not indispensable for the success of the IoT platform, should-have requirements should be implemented if feasible, provided they do not compromise any must-have requirements. Nice-to-have requirements, while less critical, can still contribute significant value if met, and thus, their fulfillment should not be entirely disregarded.

In total, 14 functional and 21 non-functional requirements are defined and categorized into various domains. For instance, functional requirements were denoted by numbers like "FR1" for abbreviation, and non-functional requirements as "NFR". As depicted in Table 1, functional requirements span across five distinct domains: (FR1) *General requirements regarding the functions of the IoT platform*, (FR2) *Data Management)*, (FR3) *Functional requirements regarding interoperability*, (FR4) *Functional requirements for error handling and exception cases* and (FR5) *Functional requirements for managing users and access rights*. General requirements for the IoT platform (FR1) include basic functions that are commonly provided also by other platforms such as the gateway registration via an EUI, the data reception from LoRaWAN gateways and sensor registration. Under (FR2) Data Management we declared the (FR2.1) On Premise-Hosting as a must-have. For data security and compliance, access control to IoT devices and compliance requirements such as the European data protection regulation can be met as data

[1] https://lora-developers.semtech.com/documentation/tech-papers-and-guides/the-book/deveui/

Table 1: Functional requirements for an IoT platform.

No.	Requirement Name	Description	Priority
FR1	General requirements regarding the functions of the IoT platform		
FR1.1	Gateway registration via EUI	The IoT platform must provide registration of IoT gateways via an EUI.	Must-have
FR1.2	Data reception from LoRaWAN gateways	The IoT platform must enable receiving data via registered IoT gateways.	Must-have
FR1.3	Livelog	The IoT platform is intended to provide a live log of the data flowing through the gateways.	Should-have
FR1.4	Sensor registration via EUI	The IoT platform must provide registration of the organization's IoT sensors via an EUI.	Must-have
FR1.5	Payload Formatter	The IoT platform can provide a function to format the received data into a desired format such as JavaScript Object Notation.	Nice-to-have
FR2	Data management		
FR2.1	On Premise-Hosting	The IoT platform must offer the option of being hosted on-premise on a cloud.	Must-have
FR3	Functional requirements regarding interoperability		
FR3.1	Lightweight Directory Access Protocol (LDAP) interface	The IoT platform should have an Lightweight Directory Access Protocol (LDAP) interface to access the organization's own user IDs.	Should-have
FR3.2	API interface	The IoT platform must have an API interface for retrieval of data by other applications via an API key.	Must-have
FR3.3	Webhook	The IoT platform must have webhook integration, to automatically send data to the organization's cloud.	Must-have
FR3.4	MQ Telemetry Transport (MQTT) interface	The IoT platform must provide an MQ Telemetry Transport (MQTT) interface for data transmission.	Must-have
FR4	Functional requirements for error handling and exception cases		
FR4.1	Automatic notification	If an IoT gateway or IoT sensor fails, the IoT platform should send a notification.	Should-have
FR4.2	Monitoring	The IoT platform is intended to provide a monitoring function to provide an overview of the device status of the end devices.	Should-have
FR5	Functional requirements for managing users and access rights		
FR5.1	User management	The IoT platform must have user management with access rights management.	Must-have
FR5.2	Authorization concept	The IoT platform is intended to assign rights to groups to which users can be assigned.	Should-have
FR5.3	Assignment of rights to API key	The IoT platform should enable the assignment of rights to API keys to restrict access from the respective external application.	Should-have
FR5.4	Local user login	In addition to Lightweight Directory Access Protocol (LDAP), the IoT platform should also be able to create local users.	Should-have

governance. Furthermore, the university may have control over effective and efficient data storage and backup procedures due to the on-premise hosting. Lastly, access only to authorized users can be granted by having full control over the application hosting.

Furthermore, within FR3, which encapsulates interoperability requirements, the significance of API interfaces, webhooks, and MQ Telemetry Transport (MQTT) was underscored. Stakeholders highlighted in the requirements survey the need for processing sensor data further in a custom-built IoT data platform, along with data visualization, particularly using the open-source software Grafana. Consequently, the existence of suitable interfaces becomes imperative. Subsequently, FR4 and FR5 outline requirements concerning error handling and user management, respectively. Within these sections, only the inclusion of logic for user storage, whether through installation on the local IoT platform database or Lightweight Directory Access Protocol (LDAP), is designated as a mandatory criterion.

5 IoT PLATFORM SELECTION

The IoT platforms were evaluated using the UA according to Cascio (1996) and Kühnapfel (2021), which was explained in more detail in Section 3.

The aim of this UA is to select, from a pool of potentially suitable IoT platforms available in the market, the one that aligns with the requirements outlined in section 4. Specific criteria are defined, and failure to meet any of these criteria will result in the exclusion of an IoT platform from consideration. In addi-

Table 2: Non-Functional requirements for an IoT platform.

No.	Requirement Name	Description	Priority
NFR1	Security		
NFR1.1	Access control	The system may only be used after successful authentication via the LDAP of the organization or accessible by a locally created user.	Must-have
NFR1.2	Encryption	The IoT platform must implement encryption standards to protect data from unauthorized access.	Must-have
NFR1.3	Password verification	The IoT platform can include functionality to assess the strength of passwords entered by users.	Nice-to-have
NFR1.4	Password Policies	The IoT platform can provide functionality to configure password policies.	Nice-to-have
NFR2	Reliability		
NFR2.1	Fail-safety	The system must be 99% available.	Must-have
NFR3	User friendliness		
NFR3.1	User-friendly interface	The system is designed to offer a user-friendly interface to simplify working on the IoT platform.	Should-have
NFR3.2	Mobile interface	The user interface should be accessible on mobile devices.	Should-have
NFR4	Scalibility		
NFR4.1	Number of API keys	The IoT platform must enable the creation of an unlimited number of API keys.	Must-have
NFR4.2	Number of IoT gateways	The IoT platform must enable the registration of at least 30 gateways.	Must-have
NFR4.3	Number of users	The IoT platform must be free of restrictions regarding the number of users created.	Must-have
NFR4.4	Number of devices	The IoT platform should enable the registration of at least 1000 devices.	Must-have
NFR4.5	Number of Groups (Organizations) / Multitenancy	The IoT platform should be free of restrictions regarding the number of groups or organizations created	Should-have
NFR5	Performance		
NFR5.1	Latency	The IoT platform must have low latency for real-time data processing in IoT applications.	Must-have
NFR6	Legal requirements		
NFR6.1	Selection of frequency ranges	The IoT platform must have a frequency range configuration on which the IoT gateways receive data.	Must-have
NFR6.2	Data protection	Personal sensitive data must be collected and kept following data protection regulations.	Must-have
NFR7	Technical requirements		
NFR7.1	LoRaWAN network architecture	The IoT platform must be based on the LoRaWAN Network architecture.	Must-have
NFR7.2	Network server	The IoT platform must provide a network server for routing the data from the IoT gateway.	Must-have
NFR7.3	Device drivers	The IoT platform should offer the possibility of providing the organization's device drivers to reuse them.	Nice-to-have
NFR7.4	Device driver properties	Device drivers should incorporate features for payload handling, decode/encode functionalities, and settings configuration.	Should-have
NFR8	Financial constraints		
NFR8.1	Use of non-proprietary software	The IoT platform must be installed and accessible without the need for licensing fees.	Must-have

tion, the criteria were weighted according to a percentage in order to include their importance in the evaluation.

As a result of the expert interviews, two significant exclusion criteria were identified which are *(1) No On-Premise Hosting* and *(2) Paid license models*. Installing an on-premise IoT platform on the university's own cloud infrastructure offers several advantages over relying on external platforms like "The Things Network". Firstly, it provides greater control and autonomy over data privacy and security, as sensitive information remains within the university's trusted environment. Secondly, it enables customization and tailoring of the IoT platform to specific needs and requirements without dependency on external service providers. Additionally, it reduces reliance on third-party services, mitigating the risk of service disruptions or changes in terms of service as happened to The Things Network infrastructure in the past. Overall, deploying an on-premise IoT platform enhances data governance, flexibility, and reliability for universities that seek robust and scalable IoT solutions. After considering the two exclusion criteria, the options for suitable IoT platforms can be significantly reduced. Following a brief market survey, only five IoT platforms are found to meet both criteria. On-premise hosting can additionally improve latency due to the infrastructure being located onsite. Moreover, it removes the reliance on a stable internet connection for accessing the IoT platform, which is essential for cloud-based services. Following the completion of the market analysis, the following IoT platforms were identified, taking into consideration the previously mentioned exclusion criteria: *(1) Thingsboard*[2], *(2) ChirpStack*[3], *(3) SiteWhere*[4], *(4) Mainflux*[5], *(5) The Things Stack Sandbox*[6].

Table 3: Cross table for the pair comparison method.

Criteria	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Σ**
1		1	1	1	1	1	1	1	1	8
2			3	2	2	6	7	8	2	3
3				4	3	3	7	8	3	4
4					5	4	7	8	9	2
5						6	7	8	9	1
6							7	8	9	2
7								8	9	5
8									8	7
9										4

According to the requirements identified in the requirements table, the following decision criteria were formed for evaluation: (1) *Range of Functions*, (2) *User Management*, (3) *Interoperability*, (4) *Error Handling*, *(5) Security*, (6) *User-Friendliness*, (7) *Scalability*, (8) *IoT Protocol Support*, and (9) *Technical Aspects*.

(1) *Range of Functions*: This criterion describes all functions that are offered by the IoT platform, fulfilling the requirements across all priority levels.

(2) *User Management* describes the extent to which it is possible to manage users, groups, and the corresponding allocation of rights within the IoT platform is evaluated here. This includes determining the feasibility of establishing an LDAP connection and creating local users, as well as the ability to assign permissions regarding API keys to regulate access for both users and external applications.

(3) *Interoperability*: This aspect examines the IoT platform's capability to communicate with other devices and systems, encompassing the availability of interfaces aligned with requirement FA3 as outlined in the Table 1.

(4) *Error Handling*: This criterion evaluates the extent to which monitoring functions are integrated within the IoT platform and the extent to which notifications are sent in the event of a sensor or gateway failure, for example. This also includes notifications in the event of interrupted data flow or the failure of a service within the platform.

(5) *Security*: This evaluation criterion includes all implemented security precautions within the IoT platform, which protects against unauthorized access to the data by third parties. This refers, for example, to the need for a strong password through password policies and encrypting all traffic.

(6) *User-Friendliness*: To facilitate ergonomic user interactions within the platform, a user-friendly Graphical User Interface (GUI) is essential. This criterion ensures that this requirement is fulfilled.

Table 4: Calculation of the critical weight as a percentage.

Criteria	**Score**	**Conversion**	**Weight**
Range of functions	8	$\frac{score}{36}$	22%
IoT Protocol Support	7		19%
Scalability	5		14%
Technical Aspects	4		11%
Interoperability	4		11%
User Management	3		8%
Error Handling	2		6%
User-Friendliness	2		6%
Security	1		3%
Total	36		100%

(7) *Scalability*: Given that IoT use cases for enhancing research and education at the university are continually evolving, and the IoT infrastructure is expected to expand with additional components, the scalability of the IoT platform becomes vitally important. This scalability accommodates a growing number of sensors, gateways, users, and API keys.

(8) *IoT Protocol Support*: This criterion is used to evaluate whether the IoT platform for the University of Things infrastructure includes an appropriate selection of IoT protocols. The presence of MQTT, LoRaWAN, and Webhook is considered essential.

(9) *Technical Aspects*: This evaluation considers mul-

[2] https://thingsboard.io/docs/getting-started-guides/what-is-thingsboard/

[3] https://www.chirpstack.io/docs/architecture.html

[4] https://sitewhere1.sitewhere.io/overview.html

[5] https://mainflux.readthedocs.io/en/latest/architecture/

[6] https://www.thethingsindustries.com/docs/reference/

tiple technical requirements, including compatibility with the LoRaWAN network architecture and features like Over-the-Air Activation (OTAA) for IoT sensors. Additionally, it assesses the platform's capability to set the license-free frequency range.

The weighting of the decision criteria was carried out in a cross-tab using the paired comparison method ((David, 1963)) according to the principle "Is more important than" (see Table 3). The far right column sums up how often a criterion exceeded another criterion in its relevance.

Table 4 shows the result of the criteria weighting using the cross-tab, sorted according to the ranking of their relevance. The percentages were rounded to whole numbers.

Once the criteria are prioritized based on their significance, an appropriate scale for evaluation is established. An ordinal scale ranging from 0 to 4 is designated for all criteria. If a criterion is not fulfilled, it receives zero points. If the criterion is inadequately met with significant deficiencies, one point is awarded. Adequate fulfillment with deficiencies warrants three points, while a good extent of fulfillment merits three points. Finally, four points are granted for excellent fulfillment. The evaluation of decision criteria is depicted in Table 5. If information regarding an IoT platform was unavailable from the test environment or manufacturer documentation, the criterion was labeled as ”No information.”

The calculation of the utility value for each decision alternative is presented in Table 6. In summary, the open-source software ChirpStack emerged as the top-rated option, achieving a utility value of 3.63. This platform is specifically designed for connecting LoRaWAN end devices and encompasses essential core functions such as device connectivity, management, data transformation, event handling, and API management. Additionally, it offers cross-sectional functionalities including user management, encryption, and platform administration. ChirpStack is deemed the optimal choice due to its similarity to The Things Stack Sandbox, serving as a LoRaWAN network server.

Moreover, ChirpStack includes an application server, join server, and geolocation server for end device positioning. It boasts scalability without limitations on gateways, devices, and users, ensuring compatibility with future expansions of the IoT system and increasing use cases on campus. The integration into existing UoT infrastructure and interoperability with external applications allows for continual extension of functionality by connecting additional IoT applications.

While Thingsboard also presents a viable alternative, it offers a comprehensive suite of IoT functions tailored to industrial IoT, potentially exceeding explicit university requirements. However, it's worth noting that the developers of Thingsboard also provide paid models. The Community Edition, an open-source version of Thingsboard, is available under the Apache 2.0 License, albeit without any support offerings. Nonetheless, ChirpStack provides the option for integrating Thingsboard functionalities if needed in the future.

Apart from Chirpstack, The Things Stack Sandbox is provided as Software as a Service (SaaS) through the cloud by The Things Industries, the manufacturer also provides it as an open-source option for installation on-premise. This alternative is closely behind ChirpStack in the rating with a utility value of 3.54. It offers the same core functions as ChirpStack and The Things Stack Sandbox, but The Things Industries emphasizes that The Things Stack Sandbox is limited in its features compared to the paid enter-

Table 5: Evaluation of the decision criteria.

No.	Criteria	Thingsboard Community Edition	Chirpstack	SiteWhere	Mainflux	The Things Stack Sandbox
1	Range of Functions	2	4	4	2	4
2	User Management	1	2	1	2	4
3	Interoperability	3	4	4	4	3
4	Error Handling	3	1	2	Not specified	1
5	Security	3	3	Not specified	3	3
6	User-Friendliness	2	4	2	1	4
7	Scalability	4	4	2	Not specified	3
8	IoT Protocol Support	4	4	1	4	4
9	Technical Aspects	4	4	1	4	4

Table 6: Calculation of the utility value of the decision alternatives.

Criteria	**Weight**	**Thingsboard**		**Chirpstack**		**SiteWhere**		**Mainflux**		**The Things Stack Sandbox**	
		Rating	Score	Rating	Score	Rating	Score	Rating	Score	Rating	Score
1	22%	2	0.44	4	0.88	4	0.88	2	0.44	4	0.88
2	8%	1	0.08	2	0.16	1	0.08	2	0.16	4	0.32
3	11%	3	0.33	4	0.44	3	0.33	3	0.33	3	0.33
4	6%	3	0.18	1	0.06	2	0.12	0	0	1	0.06
5	3%	3	0.09	3	0.09	0	0	3	0.09	3	0.09
6	6%	2	0.12	4	0.24	2	0.12	1	0.06	4	0.24
7	14%	4	0.56	4	0.56	2	0.28	0	0	4	0.42
8	19%	4	0.76	4	0.76	1	0.19	4	0.76	4	0.76
9	11%	4	0.44	4	0.44	1	0.11	4	0.44	4	0.44
Σ	100%		3		**3.63**		2.11		2.28		3.54

prise version. In addition, according to the manufacturer, this is suitable for small-scale testing purposes and not for use within a larger productive environment. In contrast to The Things Stack Sandbox, ChirpStack is well-suited for larger production environments. ChirpStack is primarily available as an open-source solution, lacking paid enterprise models offering guaranteed support. Compared to The Things Stack Sandbox, ChirpStack has, in addition to the lack of the ability to create user groups, also less granular setting options for user rights, in contrast, it offers more integrations in the applications and the option to create multiple tenants. Apart from a few differences, both IoT platforms are very similar, and basically, both represent a suitable decision alternative for the UoT environment. There is still the possibility that The Things Industries will impose further restrictions on the free versions in the future to switch users to the paid models.

In addition to the required functions, Thingsboard also supports the modeling of entities and relationships from the real world, i.e. assets, devices, and their relationships with each other. Furthermore, it provides real-time data visualization within customizable dashboards. These dashboards support ”multi-tenancy,” ensuring that users from different tenants cannot access data or dashboards from other tenants. This function is crucial in large IoT systems and is also available in ChirpStack. Another key feature of Thingsboard is its ”rule engine,” a powerful and sophisticated tool for processing incoming data. This refers to the filtering, enrichment, and transformation of data and corresponding actions that can be carried out such as triggering alarms, executing REST API calls, and sending push notifications. Within alarm management, users can create, delete, and confirm alarms. Mainflux, an open-source IoT platform, ranks fourth in the utility analysis. While it lacks native support for LoRaWAN, it offers a LoRaWAN adapter as a bridge to the LoRaWAN network. However, the adapter necessitates an existing LoRaWAN network server, such as ChirpStack, to function. Therefore, Mainflux isn’t a viable choice for the university without such implementation. Nonetheless, similar to Thingsboard, it can be integrated with a ChirpStack instance later on to enhance its capabilities.

The SiteWhere IoT platform encompasses all essential core functionalities, including device connectivity, management, data transformation, event handling, API management, and user administration. However, details regarding the maximum capacity for devices and gateways are absent from the documentation. While the scalability of microservices via Kubernetes replication is outlined, there’s no mention of LoRaWAN network integration or support. Given the university’s reliance on LoRaWAN for its existing IoT infrastructure, the absence of this feature renders SiteWhere unsuitable as a decision alternative.

6 CONCLUSIONS

This study involved the development of requirements for an IoT platform tailored to a University of Things setting. It drew upon insights from operating the university campus’s existing IoT infrastructure and interviews with IoT administrators. Subsequently, a market analysis was conducted based on both functional and non-functional requirements, followed by the evaluation of five on-premise installation IoT platforms using utility analysis.

The first research objective involves the collection of requirements for an IoT platform for the management of IoT sensors and gateways for a smart campus/UoT infrastructure. The process involved utilizing both operational experiences and insights from installing the existing IoT infrastructure on the university campus. Additionally, the expertise of IoT administrators responsible for managing the campus IoT infrastructure was leveraged. The requirements were categorized into functional and non-functional types, identifying 21 non-functional and 16 functional requirements. During the requirement gathering phase, the university's IoT experts and stakeholders prioritized effective device management, hosting, and user management. Notably, there was no specific request for IoT data visualization and filtering within the IoT platform, as a separate IoT data platform will be developed for this purpose. A multitenancy function was not declared a must-have for user and device management, as the IoT infrastructure is viewed as a private domain. Nevertheless, multitenancy is declared a should-have to be able to host the IoT platform for possible future research partners with IoT gateways and devices. By leveraging its own Infrastructure as a Service (IaaS) cloud infrastructure and hosting an open-source on-premise IoT platform with multitenancy capabilities, the university not only ensures data sovereignty and security but also establishes a robust foundation for accommodating IoT devices from diverse domains such as Smart City or Smart Region projects. This setup enables integration and collaboration between various stakeholders within the university's ecosystem, fostering IoT applications and knowledge exchange while maintaining control over data privacy and governance as well as European data protection regulations ((Blazevic and Riehle, 2023)).

The second research question involved conducting a market analysis focusing on on-premise IoT platforms. Utilizing exclusion criteria based on on-premise and license-free cost models, five IoT platforms underwent UA. Consequently, Chirpstack emerged as the preferred choice for implementation within the Smart Campus/University of Things environment, fulfilling all essential and several additional criteria. The Things Stack Sandbox demonstrated adequacy solely in the realm of user management. Given that access to the IoT platform for device management is primarily required by IoT administrators, elaborate group and user management functionalities are considered unnecessary in the end.

In future research projects, we recommend optimizing and refining the requirements for an IoT platform, as well as evaluating the use of Chirpstack over a longer period. In addition, the requirements and evaluation criteria should not only be defined for smart campus infrastructures but also expanded in a more abstract sense so that they can also be used for other IoT domains such as smart cities or smart health. Thus, these requirements can be useful for projects when selecting IoT platforms. The benefit of the multi-tenant function would also be interesting for smart region projects that rely on the use of an open-source platform for cost and data protection reasons. Since an IoT platform like Chirpstack is already installed in an in-house cloud infrastructure, this effort is no longer necessary for smart region organizations.

ACKNOWLEDGEMENTS

This research has been supported by the Deutsche Forschungsgemeinschaft (DFG) under Research Grant No. 432399058.

REFERENCES

Arz von Straussenburg, A. F., Blazevic, M., and Riehle, D. M. (2023). Measuring the actual office workspace utilization in a desk sharing environment based on iot sensors. In Gerber, A. and Baskerville, R., editors, *18th International Conference on Design Science Research in Information Systems and Technology, DESRIST 2023, Pretoria, South Africa*, number 13873 in Lecture Notes in Computer Science (LNCS), pages 69–83, Cham. Springer Nature.

Baiyere, A., Topi, H., Wyatt, J., Venkatesh, V., and Donnellan, B. (2020). Internet of Things (IoT) – A Research Agenda for Information Systems. *Communications of the Association for Information Systems*, 47(1):21.

Barros, T. G. F., Da Silva Neto, E. F., Neto, J. A. D. S., De Souza, A. G. M., Aquino, V. B., and Teixeira, E. S. (2022). The Anatomy of IoT Platforms—A Systematic Multivocal Mapping Study. *IEEE Access*, 10:72758–72772.

Berawi, M. A., Sunardi, A., and Ichsan, M. (2019). Chief-Screen 1.0 as the Internet of Things Platform in Project Monitoring & Controlling to Improve Project Schedule Performance. *Procedia Computer Science*, 161:1249–1257.

Bhajantri, L. B. and S., G. (2020). A Comprehensive Survey on Resource Management in Internet of Things. *Journal of Telecommunications and Information Technology*, 4(2020):27–43.

Blazevic, M. and Riehle, D. M. (2023). University of Things: Opportunities and Challenges for a Smart Campus Environment based on IoT Sensors and Business Processes. In *Proceedings of the 8th International Conference on Internet of Things, Big Data and Security IoTBDS - Volume 1*, pages 105–114.

Cascio, W. F. (1996). The Role of Utility Analysis in the Strategic Management of Organizations. *Journal of Human Resource Costing & Accounting*, 1(2):85–95.

Chui, M., Löffler, M., and Roberts, R. (2020). The Internet of Things. *McKinsey Quarterly*.

David, H. A. (1963). *The method of paired comparison*. Hafner Publishing Company, New York.

Elgedawy, I. and Shoukry, L. (2022). SANAD: A Comprehensive IoT Reference Architecture for Integrated Enterprise Platforms. In *2022 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*, pages 182–187.

Fahmideh, M. and Zowghi, D. (2020). An exploration of IoT platform development. *Information Systems*, 87:101409.

Fortes, S., Santoyo-Ramón, J., Palacios, D., Baena, E., Mora-García, R., Medina, M., Mora, P., and Barco, R. (2019). The Campus as a Smart City: University of Málaga Environmental, Learning, and Research Approaches. *Sensors*, 19(6):1349.

García-Valls, M. and Palomar-Cosín, E. (2022). An Evaluation Process for IoT Platforms in Time-Sensitive Domains. *Sensors*, 22(23):9501.

Gardašević, G., Veletić, M., Maletić, N., Vasiljević, D., Radusinović, I., Tomović, S., and Radonjić, M. (2017). The IoT Architectural Framework, Design Issues and Application Domains. *Wireless Personal Communications*, 92(1):127–148.

Geschka, H. and Geschka, M. (2014). Ideenfindung und Konzeptentwicklung.

Guth, J., Breitenbücher, U., Falkenthal, M., Fremantle, P., Kopp, O., Leymann, F., and Reinfurt, L. (2018). A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences. In Di Martino, B., Li, K.-C., Yang, L. T., and Esposito, A., editors, *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*, Internet of Things, pages 81–101. Springer, Singapore.

Ibarra-Esquer, J., González-Navarro, F., Flores-Rios, B., Burtseva, L., and Astorga-Vargas, M. (2017). Tracking the Evolution of the Internet of Things Concept Across Different Application Domains. *Sensors*, 17(6):1379.

Kassab, Mohamad, P. A. L. (2022). *Requirements Engineering for Software and Systems*. Auerbach Publications, New York, 4 edition.

Kugler, S., Czwick, C., Nguyen, H. P. L., and Anderl, R. (2021). Method for the Targeted Selection and Installation of an IoT - Platform. In Trzcielinski, S., Mrugalska, B., Karwowski, W., Rossi, E., and Di Nicolantonio, M., editors, *Advances in Manufacturing, Production Management and Process Control*, Lecture Notes in Networks and Systems, pages 116–123, Cham. Springer International Publishing.

Kühnapfel, J. B. (2021). *Scoring und Nutzwertanalysen: Ein Leitfaden für die Praxis*. Springer Fachmedien, Wiesbaden.

Lamsweerde, A. (2009). *Requirements engineering: from system goals to UML models to software specifications*. John Wiley & Sons, Ltd.

Lempert, S. and Pflaum, A. (2019). Vergleichbarkeit der Funktionalität von IoT-Software-Plattformen durch deren einheitliche Beschreibung in Form einer Taxonomie und Referenzarchitektur. *HMD Praxis der Wirtschaftsinformatik*, 56(6):1178–1203.

Martínez, I., Zalba, B., Trillo-Lado, R., Blanco, T., Cambra, D., and Casas, R. (2021). Internet of Things (IoT) as Sustainable Development Goals (SDG) Enabling Technology towards Smart Readiness Indicators (SRI) for University Buildings. *Sustainability*, 13(14):7647.

Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516.

Mircea, M., Stoica, M., and Ghilic-Micu, B. (2021). Investigating the Impact of the Internet of Things in Higher Education Environment. *IEEE Access*, 9:33396–33409.

Nasser, A. A., Al-Ashwal, M. M. Y., Al-Khulaidi, A. A. G., Al-Naqeep, A. N., and Al-jober, M. (2023). A Hybrid Business-Technical Model for Evaluating IoT Platforms' Functionality, Reliability, and Usability. *International Journal of Engineering Trends and Technology - IJETT*, 71(10):39–59.

Panduman, Y. Y. F., Sukaridhoto, S., and Tjahjono, A. (2019). A Survey of IoT Platform Comparison for Building Cyber-Physical System Architecture. In *2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pages 238–243.

Rayes, A. and Salam, S. (2017). *Internet of things from hype to reality*. Springer Basel.

Riehle, D. M., Arz von Straussenburg, A. F., Blazevic, M., and Wolters, A. (2023). Sensor-based use case advancements in smart parking - pioneering the next generation of smart city applications. In *Proceedings of the 34th Australasian Conference on Information Systems ACIS 2023, 5-8 December 2023, Wellington, New Zealand*, Atlanta, GA. AIS eLibrary.

Silva-da Nóbrega, P. I., Chim-Miki, A. F., and Castillo-Palacio, M. (2022). A Smart Campus Framework: Challenges and Opportunities for Education Based on the Sustainable Development Goals. *Sustainability*, 14(15):9640.

Soest, C. v. (2023). Why Do We Speak to Experts? Reviving the Strength of the Expert Interview Method. *Perspectives on Politics*, 21(1):277–287.

Toutsop, O., Kornegay, K., and Smith, E. (2021). A Comparative Analyses of Current IoT Middleware Platforms. In *2021 8th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 413–420.

Vasileva, R., Rodrigues, L., Hughes, N., Greenhalgh, C., Goulden, M., and Tennison, J. (2018). What Smart Campuses Can Teach Us about Smart Cities: User Experiences and Open Data. *Information*, 9(10):251.

Wolters, A., Blazevic, M., and Riehle, D. M. (2023). Onpremise internet of things (iot) data storage: Comparison of database management systems. In *Proceedings of the 8th International Conference on Internet of Things, Big Data and Security IoTBDS - Volume 1*, pages 140–149.

Zhang, Y., Yip, C., Lu, E., and Dong, Z. Y. (2022). A Systematic Review on Technologies and Applications in Smart Campus: A Human-Centered Case Study. *IEEE Access*, 10:16134–16149.