# Architectural Views for Social Robots in Public Spaces: Business, System, and Security Strategies

Samson Oruma[1,3*], Ricardo Colomo-Palacios[2] and Vasileios Gkioulos[3]

[1*]Department of Computer Science and Communication, Østfold University College, Bra veien 4, Halden, 1757, Viken, Norway.
[2]Escuela Técnica Superior de Ingenieros Informáticos, Universidad Politécnica de Madrid, C. de los Ciruelos, 28660 Boadilla del Monte, 28040, Madrid, Spain.
[3]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Teknologivegen 2, Gjøvik, 2802, Innlandet, Norway.

*Corresponding author(s). E-mail(s): samsonoo@hiof.no;
Contributing authors: ricardo.colomo@upm.es;
vasileios.gkioulos@ntnu.no;

**Abstract**

This study delineates a suite of architectural views and a security perspective tailored to guide the deployment and integration of Social Robots in Public Spaces (SRPS). It commences with a business context view that utilizes the customer-producer-supplier model, underscoring the value of SRPS to various stakeholders and illustrating how robots can enhance user experiences and drive economic benefits. The system context view details the intricate interactions among the social robot, stakeholders, public spaces, and external systems, highlighting essential considerations for successful deployment, from technical configurations to stakeholder engagement. The functional view elaborates on the operational dynamics of the robot within its environment, focusing on user interaction and data management capabilities. Additionally, the security perspective delves into security considerations vital for safeguarding the SRPS across various domains, including identity and access management, application and network security, and data privacy. The paper also contextualizes these views through a city ferry use case, demonstrating their practical application and reinforcing the importance of multifaceted planning and analysis in real-world settings. This approach provides

a strategic framework views for developing SRPS that are viable, efficient, and secure, fostering successful adoption in diverse public environments.

**Keywords:** Architectural views, system integration, stakeholder engagement, security perspectives, public space automation, social robots.

# 1 INTRODUCTION

As the integration of social robots into public spaces gains momentum [1], it becomes increasingly important to thoroughly understand the operational, systemic, and security implications involved [2]. Architectural view diagrams emerge as indispensable tools in the planning, design, and implementation of these systems, ranging from simple information systems to complex ecosystems like Social Robots in Public Spaces (SRPS) [3]. These diagrams play a critical role in delineating system boundaries, fostering a shared understanding among stakeholders of the system's scope, and identifying essential interactions with external entities to ensure smooth integration and functionality [4, 5]. They provide a simplified overview of complex systems, enhancing communication and comprehension among stakeholders, pinpointing vital components, facilitating risk management, and guiding the development and integration process [6]. Additionally, they are instrumental in supporting the system's maintenance and scalability, simplifying the evaluation of changes and the incorporation of new components. Ultimately, architectural context diagrams are key to boosting stakeholder collaboration, steering development efforts, and securing the system's sustainability and adaptability [5].

While research has highlighted the promising prospects of adopting social robots in service operations [7], hospitality [8, 9], and from the perspective of business managers [10], there remains a significant gap in exploring the business model, particularly the business process architecture and the core value proposition of SRPS, which is crucial for attracting investment in this burgeoning field [11, 12]. Previous studies have acknowledged the complexity of the heterogeneous and interrelated system components within SRPS, with some focusing on achieving safety behaviours [13], and others on cognitive mechanisms for managing internal and external states [14], emotion recognition [15], intelligent response [16], and systems facilitating real-time interaction through multimedia processing [17]. Despite these focused efforts, the overarching system architecture of SRPS has yet to be represented in the literature. Additionally, the critical issues of security and privacy within SRPS have been addressed by several studies, pointing out various threat actors, types of attacks, failure management strategies, software vulnerabilities, and detection methods [18–20]. However, a study encompassing all security domains relevant to this multifaceted and emerging technology has been notably absent, highlighting a pivotal area for future research.

This conceptual study presents three foundational architectural views essential for deploying SRPS, each addressing critical aspects of their integration and function. The business context architecture view leverages a customer-producer-supplier model to underline SRPS's core value propositions, showcasing the mutual benefits for users and

businesses [11, 12]. The system context architecture details the essential interactions between social robots, stakeholders, and public spaces, highlighting the importance of external system integration and adherence to operational constraints for successful SRPS deployment. The system context architecture view [21] delves into the vital interactions between social robots, stakeholders, and public spaces, underscoring the importance of external system integration and operational constraints for successful SRPS deployment. Meanwhile, the functional view focuses on the operational capabilities and interactions of the social robot within its environment [22]. The security context architecture provides an in-depth analysis of the various security domains relevant to SRPS, including Identity and Access Management (IAM) [23], Endpoint security [24], Network security [25], Data security [26], and more, crafting a strategy to protect SRPS in complex public environments. These architectural views offer a robust blueprint for developing, deploying, and securing SRPS, ensuring their effective operation and integration into public spaces.

Each architectural view and security perspective, while distinct, are interrelated, providing insights into the approach required to implement SRPS effectively, as illustrated through the case study of a city ferry social robot. This paper aims to contribute to the field of information security society by offering robust architectural views that support the practical realisation of SRPS, ensuring their functional, secure, and beneficial integration into public life [27].

This research contributes to social robotics, smart cities, and public space management through its architectural views and practical application in a city ferry use case. These contributions are summarized as follows:

1. **Introduces Architectural Views:** Develops three interrelated architectural views—business context, system context, and functional views, expanding upon existing literature with innovative methodologies for analyzing service-oriented social robots in public spaces.
    - *Business Context View:* Demonstrates a business model tailored for SRPS, employing the customer-producer-supplier framework to elucidate the economic and social value for involved stakeholders.
    - *System Context View:* Provides a detailed examination of interactions between the social robot, stakeholders, and the surrounding environment, including external systems and public spaces, which highlights the technical and environmental implementation requirements.
    - *Functional View:* Focuses on the operational capabilities and interactions of the social robot within its environment, emphasizing practical functionalities and user interaction mechanisms.
2. **Security Perspective:** Analyzes essential security domains pertinent to SRPS, such as identity and access management, endpoint security, network, application, data, and cloud security, thereby deepening the understanding of protective strategies.
3. **City Ferry Case Study:** Implements the aforementioned views in a city ferry scenario, showcasing their practical relevance and serving as a prototype for future deployments of social robots in public settings.

4. **Foundation for Future Research and Development:** Establishes a robust foundation for continuous research, promoting further exploration and technological advancements in the integration of social robots into public spaces.

This paper is structured to navigate the architectural views for SRPS, facilitating a deep dive into each component. Section 2, Related Work, contextualizes our contributions within existing literature. Section 3, Materials and Methods, details the methodologies used to develop our framework architectural views. Section 4, Business Context Architecture View, introduces and applies this framework to the city ferry social robot use case. Section 5, System Context Architecture View, and Section 6, Functional Architecture View, further elaborate on the technical and operational specifics of SRPS, respectively. Section 7, Security Perspective, addresses the security measures tailored for SRPS. Section 8, Implementing Architectural Views in a City Ferry Social Robot, demonstrates the practical application of these frameworks. The discussion in Section 9 synthesizes our findings and implications, leading to Section 10, Conclusion, where we summarize the study's outcomes and suggest directions for future research.

# 2 RELATED WORK

The deployment of SRPS has garnered significant attention in recent years, leading to a rich body of literature that explores various facets of this emerging field. This section reviews related works that contribute to understanding the business, system, and security aspects of SRPS, providing a foundation upon which this paper builds.

## 2.1 BUSINESS PROCESS MODELING FOR SRPS

The burgeoning field of service robots in public spaces necessitates a robust architectural framework to integrate these technologies effectively into everyday social and business contexts. The literature extensively discusses various aspects of SRPS, from technological innovations to user interactions and the implications of integrating these systems into public spaces. This discourse highlights the critical need for architectural views that address both the technical and socio-economic dimensions of SRPS deployment.

Vishwakarma et al. [7] provide a systematic literature review and a thematic analysis that identifies the core research clusters around service robots, particularly their impact on human perceptions and interactions. This underscores the importance of a business context architecture that not only articulates the value propositions of SRPS but also aligns with stakeholder expectations and needs. Ding et al. [28] further emphasize the significance of human-robot interactions in shaping customer acceptance, suggesting that the design of SRPS must consider these dynamic interactions to foster user acceptance and integration into daily activities.

Song et al. [9] integrate robot and customer characteristics into a modified Technology Acceptance Model, highlighting the influence of functional and social perceptions on user acceptance. This supports the need for a system context architecture that

details the interactions within SRPS, ensuring that both technical and human factors are harmoniously integrated to enhance user experience and system functionality.

Yang and Chew [8] and Nakanishi et al. [29] both address the application of SRPS in specific settings, pointing out the operational challenges and the potential enhancements that intelligent robots bring to service industries. These studies reinforce the necessity of a functional view that focuses on the operational capabilities of SRPS, ensuring they meet both business and consumer expectations effectively.

Together, these works underscore the complexity of integrating SRPS into public and service environments, highlighting the critical role of a business context architecture in navigating the challenges and opportunities presented by social robots. Collectively, they inform the development of SRPS by emphasising technological innovation, stakeholder engagement, and the nuanced dynamics of human-robot interaction, thereby providing a robust foundation for the proposed architectural frameworks in our study.

## 2.2 SYSTEM INTERACTION AND INTEGRATION

Several related works underscore the critical need for a well-defined system context architecture in deploying SRPS, highlighting various safety, interaction, and adaptability approaches. Scianca et al. [13] focus on safety behaviours adaptable to context and sensory information, establishing a foundation for secure robot operation. Infantino et al. [14] explore a software architecture facilitating social interaction through cognitive mechanisms, emphasising the importance of monitoring robots' internal and external states. Liu et al. [30] propose a framework for dynamic behaviour control in human-robot interaction, addressing role conflicts and collaboration strategies. Asprino et al. [31] introduce a reference software architecture to overcome common challenges in social robotics, leveraging a bottom-up approach for acceptability and personalisation. Foggia et al. [17] present a flexible, hardware-independent architecture for social robotics, focusing on real-time interaction and multimodal data processing. Tanevska et al. [16], and Heredia et al. [15] propose frameworks for personalised and adaptive interactions and emotion recognition, respectively, enhancing the user experience through intelligent response mechanisms. Martínez-Rojas et al. [32] discuss AI-powered Robot Process Automation (RPA) robots for cognitive tasks, while Pramila et al. [33] delve into medical assistive robots, showcasing applications in healthcare. Finally, Stange et al. [34] highlight the need for interaction architectures that enable robots to autonomously generate coherent behaviours and verbal self-explanations. Collectively, these works illustrate the multifaceted approaches to developing SRPS, reinforcing the importance of a system context architecture that integrates these diverse elements for successful deployment in public spaces.

## 2.3 SECURITY STRATEGIES FOR SRPS

In justifying the need for a security context architecture for SRPS, recent scholarly works provide insights into the multi-layered security challenges and propose innovative solutions. Botta et al. [18] delve into robot cybersecurity, discussing various attack types, impacts, and mitigation techniques, highlighting the evolving challenges

in artificial intelligence, cloud robotics, and robot forensics. Oruma et al. [19] offer a systematic mapping study of SRPS security, proposing guidelines tailored for SRPS by analysing existing standards and identifying gaps for unique operational environments.

Kirca et al. [20] introduce a runtime verification architecture for anomaly detection in ROS-based robotic systems, demonstrating its effectiveness against common cyber-attacks through experimental setups. Concurrently, Oruma and Petrovic [35] discuss security threats from various dimensions, including cybersecurity and physical threats, and recommend solutions for 5G network designs tailored to SRPS.

Yaacoub et al. [36] survey security vulnerabilities across multiple robot domains, offering a qualitative risk assessment and solutions like encryption and intrusion detection. Oruma et al. [37] focus on the security of SRPS, categorising threats and analysing the attack surface, advocating for security-by-design principles and user awareness. Hristozov et al. [38] propose a method for switching between architectures based on environmental conditions, enhancing adaptability and failure management in robotic systems.

Malavolta et al. [39], Dieber et al. [40], and DeMarinis et al. [41] explore ROS-based system architectures, vulnerabilities, and penetration testing tools, underscoring the importance of securing these systems against unauthorised access and cyberattacks. Afanasyev et al. [42] review IoT and robotics integration challenges, proposing a layered system architecture for the Internet of Robotic Things. Khalid et al. [43] introduce a framework to protect collaborative robotic cyber-physical systems from cyberattacks, focusing on real-time monitoring and system health reconfiguration.

DiLuoffo et al. [44] analyse the Data Distributed Service (DDS) security standard in ROS 2, highlighting its limitations and the impact of security configurations on system performance. Lastly, Batth et al. [45] conceptualise the Internet of Robotic Things, proposing an architecture integrating IoT, cloud computing, and artificial intelligence with robotics, reviewing enabling technologies and potential applications.

Collectively, these works underscore the multifaceted nature of security in deploying SRPS, advocating for a security context architecture that addresses the intricate web of cybersecurity, physical integrity, and ethical considerations. They emphasise the necessity of developing robust, adaptable, and secure frameworks to safeguard SRPS against emerging threats, thereby providing a solid foundation for our study's proposed architecture.

In summary, while the existing literature provides valuable insights into individual aspects of SRPS deployment, there is a discernible need for integrated frameworks that consider the business, system, and security dimensions concurrently. Our paper aims to fill this gap by presenting architectural frameworks that address the complexities of introducing social robots into public spaces, drawing on the strengths and addressing the limitations of the related work discussed above.

# 3 MATERIALS AND METHODS

Developing the concepts discussed herein involved an interdisciplinary approach [46], incorporating insights from cybersecurity, software, social robotics, public space experts, and end-user participation in a Norwegian city ferry project featuring a social

robot [47]. Detailed observations of expected public space environments and workflow interactions were made to understand the current situation thoroughly, identifying unique challenges and constraints [48]. This effort was part of the SecuRoPS project, which aimed to gather requirements for deploying autonomous mobile service robots in city ferry settings through collaborative sessions with professionals and stakeholders across disciplines. The involvement of experts from various fields was crucial to mitigate misunderstandings across domains, thereby validating the requirements derived. Initial discussions, primarily focused on the city ferry attendant scenario, laid the groundwork for expanding the project's scope to encompass broader public space interactions. Feedback from additional experts and end users related to the city ferry project enabled the iterative refinement of our risk classification concept, ensuring its relevance and accuracy in reflecting stakeholders' real-world experiences and expertise. Despite the limitation posed by the small group size (10 experts and 29 end-user responses), the discussions on fundamental and high-level aspects of social robot interaction in public spaces (addressing security, privacy, safety, and acceptance) yielded valuable insights applicable across various public space settings.

The SecuRoPS project benefits from the support of a transdisciplinary team led by the Institute for Energy Technology (IFE)[1], which oversees work package 2 - WP2 (Digital Threat Landscape) and WP4 (Use Case Development and Piloting), integrating research, education, and industry insights in Norway. The team comprises professionals in cybersecurity and robotics; Høgskolen i Østfold (HIØ)[2], focused on cybersecurity and software, leading WP3 (SecuRoPS Framework Design) and WP5 (Dissemination and Exploitation); SNØ Designstudio[3] from Fredrikstad Municipality, tasked with redesigning the social robot hardware to align with user preferences; and the Institut de Robòtica i Informàtica Industrial (IRI)[4], responsible for acquiring the social robot from PAL Robotics and adapting its user interaction design in WP6 (Industrial Design of Social Robot). The project's empirical research aimed to understand public perceptions of SRPS, focusing on trust, privacy concerns, and desired functionalities within Norwegian culture.

Our approach to developing the security risk classification began with a top-down analysis of the fundamental aspects of public spaces, including the physical environment [49] and human-robot interactions and workflows [50]. Recognizing that public spaces vary significantly in purpose and design (e.g., city ferries, shopping malls, museums, airports), we concluded that risk analysis must account for these differences and the specific interactions and workflows involving the social robot. To address this, we introduced independent risk categories, each representing a spectrum from low to high risk, with corresponding design requirements for city ferry robots based on the identified risk levels for each scenario [51].

The architectural views (comprising business context, system context, and functional views), alongside the security perspectives discussed in this paper, align with the methodologies suggested by Rozanski and Woods in their book on software systems architecture [52]. This involves engaging with stakeholders through meticulously

[1] https://ife.no/en/front-page/
[2] https://www.hiof.no/
[3] https://snodesignstudio.com/
[4] https://www.iri.upc.edu/

structured viewpoints and perspectives to ensure comprehensive system understanding and security. To visually represent these architectural views effectively, we employed Simon Brown's C4 model [53] for visualizing software architecture, which offers a clear and structured approach to diagramming software architecture, enhancing clarity and stakeholder communication throughout this study.

# 4 BUSINESS CONTEXT ARCHITECTURE VIEW

A business context architectural view diagram outlines the relationships and interactions between a business system and external entities within its operational environment [21, 54]. This diagram, essential during the initial phases of information system planning, simplifies understanding for stakeholders by representing the system as a "black box" and focusing on its external interactions rather than internal functionalities. It highlights how the system integrates into the broader business ecosystem, showing the system's role in supporting business processes, aligning with business objectives, and interacting with external stakeholders, thereby emphasizing the system's business implications rather than technical specifics [55]. It is instrumental in defining the system's boundary, differentiating between its internal components and external entities like business owners, customers, and partners. It underscores the importance of core value propositions by elucidating the benefits and services provided to each stakeholder and detailing how the system enhances broader business operations and contributes to business goals [52]. This diagram serves a pivotal role in presenting a clear interface of the system with the external world, marking essential inputs and outputs, thereby aiding in requirement gathering, stakeholder communication, and understanding dependencies. Moreover, it facilitates risk management by identifying potential external risks and assists in integration planning to ensure that the system aligns seamlessly with other systems and business processes.

In our study, we adopted Brown's C4 Model [53] to visualize the software architecture of the proposed business context architecture view for service-oriented Social Robots in Public Spaces (SRPS). This decision was influenced by the limitations of the Unified Modeling Language (UML) [56], which is traditionally used in software architecture but lacks specific provisions for context diagrams. Rozanski and Woods [52] have criticized UML for its assumption that system context will be encapsulated within a use case diagram, a method that often yields overly complex diagrams and struggles with the absence of a use case list and the difficulty in abstracting system details to treat it as a black box. Consequently, the C4 Model was chosen for its clearer and more effective approach to depicting system interactions within its environment, addressing the shortcomings of UML in representing the context architectural view.

Figure 1 presents a business context architecture view grounded in the customer-producer-supplier (CPS) business model as outlined by Burdett [57]. This diagram illustrates the interactions between key stakeholders [58] (producers, customers, suppliers, and community residents) and pivotal systems such as the social robot, data processing and storage, public space, integrated services (API), and IT support. Each element's role and responsibility are briefly described to enhance comprehension. This system orchestrates interactions, service delivery, and data exchange among different

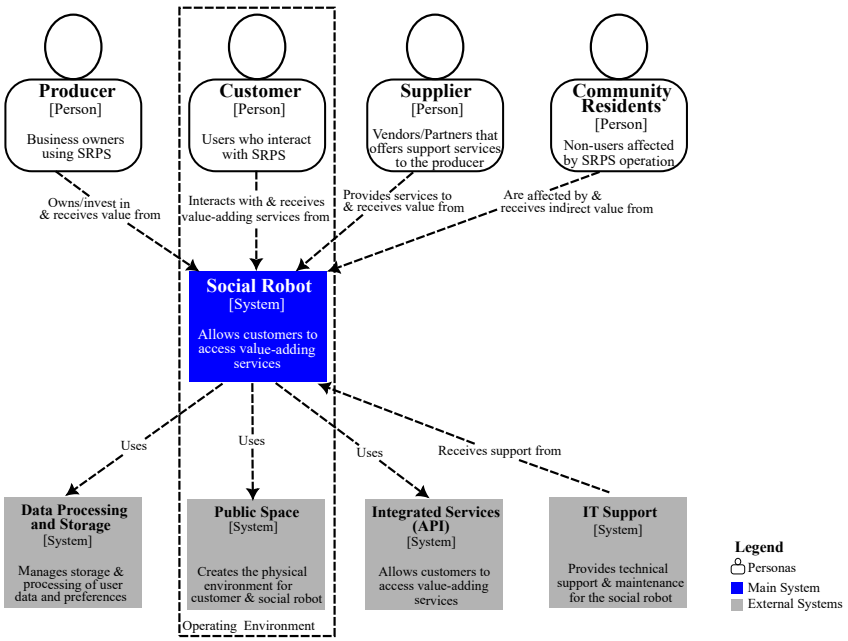


**Fig. 1** Business Context Architectural View for Service-Oriented Social Robots in Public Space

external systems and personas, fostering a service-oriented environment. The diagram clearly marks the operational boundary, representing the physical environment where the social robot interacts with customers. It illustrates the direct connections and interactions among various personas and systems, while also showcasing the flow of value and services throughout the ecosystem [59]. The relationships and interactions depicted in the diagram are clarified as follows:

- The **Producer** owns and invests in the social robot system while receiving business value from the system.
- The **Customer** interacts with the social robot system, receiving value-adding services that enhance their experience and satisfaction.
- The **Supplier** provides services to the social robot system, benefiting from the business value generated through this support.
- **Community Residents**, including bystanders or local residents in the vicinity of the social robot's operational area, are indirectly impacted by its functions and also derive indirect value from its presence.
- The social robot system utilizes the **Data Processing and Storage System** for efficient data processing and management.
- It (The social robot system) operates within the **Public Space System**, which is marked as its immediate environmental context.
- It connects with the **Integrated Services (API) System** for accessing external data and functionalities essential for its operations.
- Additionally, the **IT Support System** provides necessary technical support ensuring its effective functionality.

Table 1 presents a summary of the description, responsibilities, concerns, and requirements of the elements within the business context architectural view of service-oriented social robots [60].

**Table 1** Overview of Descriptions, Responsibilities, Concerns, and Requirements for Elements in Business Context View

| Elements | Description | Responsibilities | Concerns | Requirements |
|---|---|---|---|---|
| Customer | Users who interact with the social robot in public spaces. | To engage with the social robot for information, services, & entertainment. | Concerns about the security & privacy of personal data. | Need for value-adding services, accessibility options, & security of personal data. |
| Producer | Business owners using the social robot for service-oriented tasks. | To manage & oversee the operation & use of the robot to benefit their business. | User acceptance, compliance with laws, & data security. | Ensuring the social robot's effective operation & the safety of its data & physical unit. |
| Supplier | Vendors & partners providing services supporting the producer. | To supply necessary services & products that aid the social robot's functions. | Integration with the social robot's systems & timely payments. | Seamless integration & system reliability. |
| Community Resident | Local residents & bystanders in the robot's operational public space. | Observers of the robot's interaction within the space, potentially indirect users. | Privacy concerns, & impact on public space utilization. | Transparency in data collection and usage. |
| Social Robot | The main system between users & external systems in public spaces. | To provide user-specific information & services by interacting directly with users. | Managing data security, user privacy, & opera -tional efficiency. | Reliable connectivity, user-friendly interface, & robust data protection measures. |
| Data Processing & Storage | Manages storage & processing of user data. | To store, process, & retrieve user data as needed by the social robot. | Security of stored data & efficiency of data processing. | High storage capacity, fast processing, & stringent security measures. |
| Integrated Services (API) | Facilitates the interaction between the social robot & external systems. | To provide a conduit for data exchange between the social robot & other services. | Reliability of API connections and data accuracy. | Stable API connections and timely data updates. |
| IT Support | Provides technical support & maintenance for the social robot. | To ensure the social robot operates efficiently without technical issues. | Quick resolution of technical problems and system downtime. | Efficient trouble -shooting and regular maintenance capabilities. |
| Public Space | Dynamic & evolving environment where the social robot & customers interact. | Creates an environment under which social robots & customers interact. | Governed by social norms, laws, and environmental factors like weather. | Effective adaptation to changing conditions & compliance with social, legal & ethical standards. |

## 4.1 Personas

A brief overview of the personas involved in the business architectural view is presented below.

### 4.1.1 Producer

Producers are business owners who deploy social robots for service-oriented tasks within public spaces. They focus on the robot's ability to educate, inform, and entertain, aiming for user acceptance and compliance with laws like GDPR [61]. Concerns include the security of data in transit and at rest, and the physical safety of the robot from theft or damage in unsupervised public settings. The producers seek to derive business value, either financial or strategic, from the robot's interactions, which could offer competitive insights or help in planning future societal projects [62].

### 4.1.2 Customer

Customers are the direct users of the social robot, interacting through inquiries and service requests [28]. They represent diverse demographics, including differences in age, height, gender, language, and physical abilities (such as the use of wheelchairs or hearing aids). Their expectations include value-added services, prompt system responses, accessibility features like touch screens and voice input, multilingual support, and stringent measures for the security and privacy of their data, along with control over how it is used.

### 4.1.3 Supplier

Suppliers are business vendors and partners who support the social robot with various services. They require seamless integration with the robot, consistent system availability, opportunities for promotions, referrals to local businesses, and reliable financial transactions with the producers [59].

### 4.1.4 Community Resident

Although not direct users of the robot, are affected by its presence and operation in public spaces. Their concerns centre on potential privacy infringements and the desire for more transparent communication regarding data collection and usage. They also value the benefits of producers' corporate social responsibility (CSR) initiatives and the societal improvements driven by analytical insights from user interactions with the robot [63].

Table 2 outlines the business value propositions provided by service-oriented social robots within public space systems, highlighting the benefits and services offered to each stakeholder [11, 12]. This component of the business context architecture view demonstrates how the system supports business objectives, detailing the value delivered to various personas within the business architectural framework view.

## 4.2 Systems

The descriptions, responsibilities, concerns, and requirements of the five systems within the business context architecture are outlined following subsections [60].

**Table 2** Business Value Proposition for Stakeholder

| Personas | Business Value Proposition |
|---|---|
| Producer | Enhances customer engagement and satisfaction, provides analytics for better business decisions, and opens new revenue streams through innovative service offerings. |
| Customer | Offers convenient, personalized, and interactive services that enhance the user experience and satisfaction in public spaces. |
| Supplier | Creates opportunities for suppliers to integrate their services and products more closely with innovative technology, potentially increasing demand and customer reach. |
| Community Resident | Improves the quality of public spaces, enhances local amenities, and possibly contributes to community safety and social engagement through interactive information dissemination. |

### 4.2.1 The Social Robot System

The Social Robot is central to the business context architecture as the primary information system, serving as the interface between users and various external software systems [7]. Equipped with a user interface subsystem having a touch screen and speech input capabilities, the robot provides services designed to inform, educate, and entertain users. It processes inquiries and service requests, tailoring responses based on user data and preferences it collects. To enhance user experience and service delivery, the robot integrates with API services (Service Integration System), fetching relevant data from external systems. It stores this data either onboard or in an external data storage system, managing high computational demands by relying on external resources to optimize battery life during operations if necessary. The robot maintains a robust and reliable connection with these external systems to ensure seamless service delivery [64]. As a data custodian, the robot ensures that all user data and preferences are stored and utilized with explicit customer consent in accordance with applicable laws (GDPR). For returning users, it retrieves personalized settings from its database to customize interactions. Moreover, the robot is designed to be accessible and user-friendly for diverse user groups while safeguarding the privacy of bystanders and other non-users in its operating environment, despite its limited computing power and battery life.

### 4.2.2 Data Processing and Storage System

This system is pivotal for managing the data that the social robot collects, processes, and stores. It is responsible for ensuring that user data is securely stored, efficiently retrieved, and appropriately managed to comply with privacy regulations and customer consent. The primary concerns of the data processing and storage system include data security, privacy, integrity, and availability [65]. The requirements for this system include robust encryption protocols, reliable backup mechanisms, and effective data lifecycle management strategies to handle data from various inputs such as touchscreens and speech recognition interfaces, ensuring that data remains accessible and secure at all times.

### 4.2.3 Integrated Service (API) System

The Integrated Services System serves as the conduit through which the social robot interfaces with external services, using APIs to access and integrate diverse data

streams from various service providers, such as producer's services and suppliers. Its responsibility is to facilitate seamless integration and smooth data exchange between the robot and external systems, enhancing service delivery and user experience. Concerns for the API System [66] include maintaining high availability, ensuring data consistency, and managing potential bottlenecks in data flow. Requirements involve implementing resilient, scalable API management platforms that can handle varying loads and provide consistent performance, along with security measures to protect against unauthorized access and data breaches.

### 4.2.4 IT Support System

This system is tasked with the ongoing maintenance and technical support of the social robot, ensuring that hardware and software components function optimally and are regularly updated [67]. The IT Support System's responsibilities include value-adding use case creation, security of the social robot, troubleshooting, system updates, and the management of technical issues that arise during the robot's operation [68]. Concerns centre around minimizing downtime, rapidly resolving operational glitches, and maintaining system health. The requirements for the IT Support System include a skilled technical team capable of rapid response, tools for monitoring system performance, and protocols for regular maintenance and software updates to keep the system efficient and up-to-date while adding business value to end users [69].

### 4.2.5 Public Space System

The Public Space System [70] encompasses the dynamic and evolving environment where the social robot operates, including the physical space such as city parks or pedestrian areas, as well as ambient conditions (weather, noise levels, and crowd density) that impact the robot's functionality. It also integrates the legal and ethical norms governing the area, like GDPR compliance for data protection in public areas, and considers the presence of threat actors such as cybersecurity threats and natural hazards that pose risks to the main system. The primary responsibilities of this system are ensuring that the social robot operates harmoniously within these public domains, respecting personal space, adhering to social norms, and safeguarding against these threats [71]. Concerns for this system include managing environmental variability, preventing disruptions from cybersecurity threats like hacking or data breaches, and mitigating risks from natural hazards such as floods or fires. Requirements for the Public Space System include robust design and programming of the robot to handle environmental and security challenges, mechanisms to monitor and adapt to real-time changes and threats in the public space, and compliance with all regulatory and ethical standards to ensure safe, respectful, and secure operations within the community.

# 5 SYSTEM CONTEXT ARCHITECTURE VIEW

The system context architecture view offers an examination of the technical and operational characteristics of the system within its environment, detailing system interfaces, data exchanges with external entities, and essential external dependencies [21].

Although it shares the same elements as the business architecture view (personas and systems) its focus shifts toward the **technical** and **operational details** of each element. We employ the level 2 view (container view) of the C4 model [53] to delve into the components of each entity previously depicted as black boxes in Figure 1. This context view serves the same purpose as the business architecture view: to assist in identifying stakeholders [58], detailing their responsibilities, and capturing their concerns, all of which are crucial for developing complete system requirements. As emphasized by Rozanski and Woods, [52], our primary interest lies in stakeholders with specific concerns related to the main system, the social robot [60]. A brief overview of each element follows, providing clarity on their roles and interactions within the system.

## 5.1 Personas

In the system context architecture view, our focus for the personas is on uncovering the operational details. We aim to identify who the active stakeholders are, outline their responsibilities, determine which stakeholders have specific concerns about the systems [58], and understand the requirements for each element previously outlined in Figure 1. An incomplete analysis of these operational details during requirement gathering can lead to overlooking crucial aspects of the system [52]. Therefore, we provide a more in-depth exploration (level 2 or container view) of each persona below, ensuring an understanding of their roles and interactions within the system.

### 5.1.1 Producer

Building upon the initial description of the producer in the business context architecture view (see Section 4.1.1), the deeper level 2 (container) view reveals that the producer can be either a business entity or an individual investor who owns the main system. When conceptualized as a business entity, the producer encompasses diverse teams or departments including Information Technology (IT), Operations, Legal, Public Relations (PR), Accounting and Finance (Accounts), Human Resources (HR), Ethics and Compliance, and Research and Development (R&D), as illustrated in Figure 2. If the producer is an individual investor, they may rely on external support such as contractors, consultants, advisors, or freelancers for similar functions. Each stakeholder group, whether internal or external, presents unique perspectives, concerns, and requirements concerning the main system, which are essential to acknowledge and address. Our focus remains on stakeholders who have direct **concerns** related to the main system's functionality and security [60].

### 5.1.2 Customer

Building upon the business context architecture (Section 4.1.2), the system context view offers a detailed Level 2 (container) analysis, where customers are segmented based on demographic, geographic, psychographic, behavioural, and need-based characteristics [72] as shown in Figure 3. Each segmentation reveals deeper insights:

- **Demographic:** Includes age, gender, education, occupation, ideology, marital status, and religion.

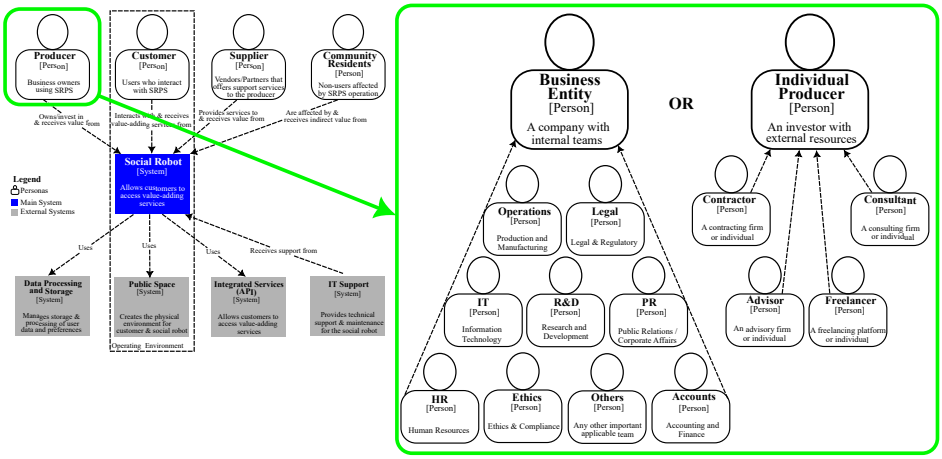


**Fig. 2** Producer Element in System Context Architecture View (Level 2 view)

- **Geographic:** Encompasses location and language.
- **Psychographic:** Covers lifestyle, interests, values, and personality traits.
- **Behavioural:** Involves service preferences, usage frequency, loyalty status, and feedback.
- **Need-based:** Addresses specific health needs, service requirements, and accessibility considerations.

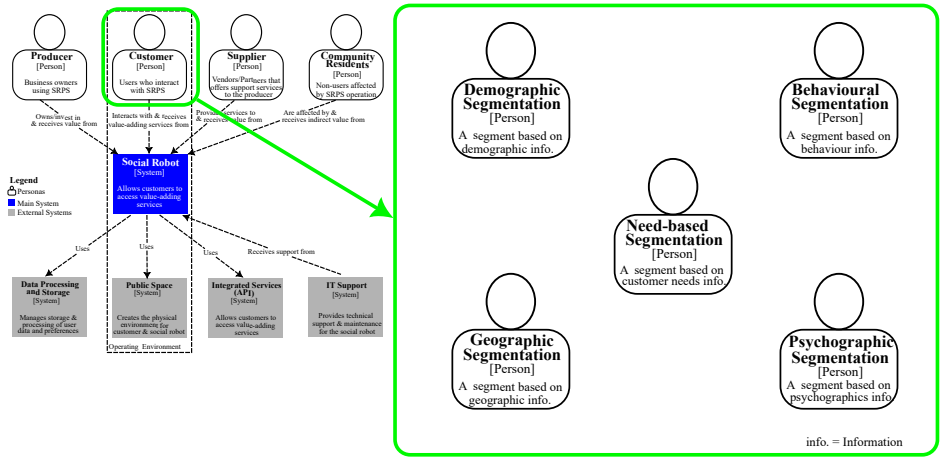


**Fig. 3** Customer Element in System Context Architecture View (Level 2 view)

This segmentation strategy not only facilitates the capture of diverse customer needs and concerns but also aids in crafting personalized interactions within the public space. Such detailed segmentation proves instrumental during the testing phases of use cases, where specific user samples are targeted. While primarily a business tactic,

this detailed customer analysis is crucial in the system context view, where the focus shifts to a more granular examination of each element previously outlined as a 'black box' in the business context view.

**Table 3** Examples of Customer Segmentation for Service-Oriented SRPS

| Customer Segment | Examples |
|---|---|
| Demographic | Age, Gender, Education, Occupation, Ideology, Marital Status, and Religion. |
| Geographic | Location, and Language. |
| Psychographic | Lifestyle, Interest, Value, Personality Traits, and Attitude. |
| Behavioural | Service Preferences, Usage Frequency, Loyalty Status, and Feedback. |
| Need-based | Health Needs, Service Needs, Delivery Needs, Accessibility Needs |

Table 3 provides a breakdown of customer segments, illustrating how each can be expanded to align closely with more specific customer needs and requirements. For instance, the **age** segment includes categories such as children (0-12 years), youth (13-24 years), adults (25-64 years), and senior citizens (65+ years). This segmentation is refined further:

- **Children** are subdivided into *toddlers* (1-3 years), *preschoolers* (4-6 years), and *school-aged* children (7-12 years).
- **Youth** are segmented into *adolescents* (13-17 years) and *young adults* (18-24 years).
- **Adults** are divided into *working professionals* (25-44 years) and *middle-aged* adults (45-64 years).
- **Senior Citizens** are classified into *early seniors* (65-74 years) and the *elderly* (75+ years).

This segmentation strategy can be applied to other examples within various segments to enhance the understanding of customer needs and concerns. This detailed approach not only facilitates targeted interaction but also drives the requirement-gathering process more effectively.

### 5.1.3 Supplier

In the system context view, the Supplier role is expanded to encompass a broad array of service and product providers that support the operational and functional needs of the social robot. This includes Hardware Vendors, Software Vendors, Technology Suppliers including AI specialists, User Experience (UX) Designers, Public Space Managers/Administrators, Robot Operators, Third-party Service Providers, Insurance Companies, and Infrastructure & Facility Managers [73]. Each type of supplier contributes critical components, from physical hardware and software solutions to user interface design and operational management. They ensure the robot is well-integrated, functional, and compliant with current standards and practices. Their responsibilities also involve continuous support and updates, managing integration with public space infrastructure, and ensuring robust security and operational reliability [64]. The focus is on creating

a supportive ecosystem that maintains the social robot's functionality and enhances user interaction while addressing integration challenges and compliance requirements.

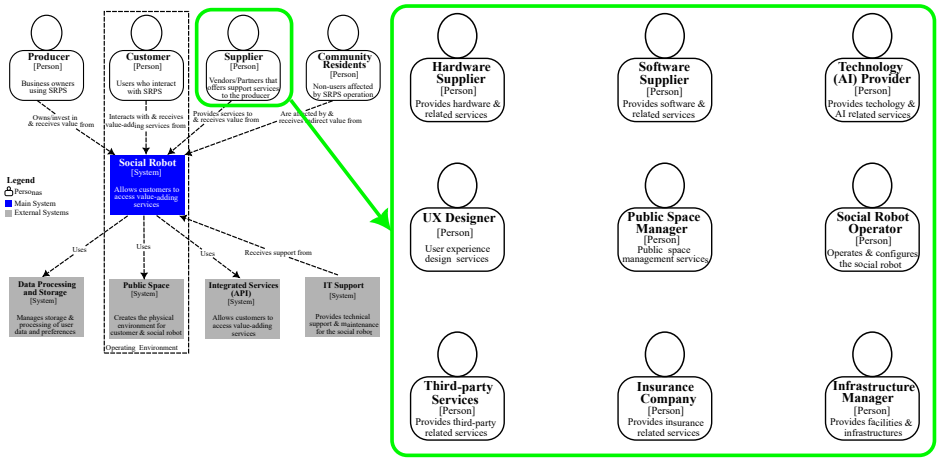


**Fig. 4** Level 2 System Context View of Supplier Elements

Figure 4 presents a level 2 overview of the supplier element. A brief description of the various suppliers for a service-oriented social robot operating in public space is presented below:

1. **Hardware Suppliers/Vendors:** These suppliers provide the physical components required for the construction and maintenance of social robots. This includes sensors, actuators, robotic limbs, electronic control units, and power modules (batteries).
2. **Software Vendors:** They develop, test and provide the software that drives the robot's operations. This includes operating systems, application software, Robot Operating System (ROS) packages, and security software.
3. **Technology (including AI) Suppliers:** These suppliers provide advanced technological solutions, particularly in artificial intelligence, to enhance the robot's decision-making and data processing capabilities. They might supply machine learning models that enable the robot to recognize and interpret human emotions or natural language processing tools for understanding and generating human language.
4. **User Experience (UX) Designers:** UX designers focus on optimizing the robot's interface and interactions to ensure they are intuitive and engaging for all user demographics [74]. They might design interactive dialogues for the robot or develop user-friendly interfaces that accommodate users with disabilities.
5. **Public Space Managers/Administrators:** These are responsible for overseeing the integration of social robots within public settings like parks, malls, or squares. They coordinate with local authorities and businesses to ensure the robots operate smoothly within these environments, addressing logistical and regulatory challenges.

6. **Robot Operators:** They handle the day-to-day operations of social robots, ensuring they function as intended, performing routine checks and overseeing interactions to prevent or resolve issues. They might also be involved in training the robots or updating their software as needed.
7. **Third-party Services Providers:** This broad category includes any additional services that support the robot's operations indirectly, such as cloud computing providers [75], who host the robot's data or analytics services that evaluate the robot's interaction data to improve performance, and local businesses aiming to leverage the social robot for promotional activities and referrals.
8. **Insurance Companies:** These providers offer insurance products that cover various risks associated with operating robots in public spaces, such as damages from malfunctions or liabilities arising from accidents involving the robots [76].
9. **Infrastructure & Facility Managers:** They ensure that the physical and digital infrastructure of public spaces is suited to accommodate and support social robots. This might include modifying physical paths to accommodate robot navigation or enhancing Wi-Fi systems to ensure uninterrupted robot communication, or providing infrastructure as a service [73].

### 5.1.4 Community Resident

The Community Residents in the system context view are categorized to include Bystanders, Passers-by, Cybersecurity Threat Actors, Regulators, Privacy/Digital Rights Advocates, Ethicists and Social Scientists, Law Enforcement or Security Agencies, and the Media [77]. This detailed categorization helps to address the varied interactions these groups have with the social robot system within their public environments. Each subgroup presents unique perspectives and concerns, from ensuring the robot operates within ethical and legal boundaries to addressing privacy issues and managing security risks. For instance, privacy advocates focus on the robot's data handling practices, while ethicists and social scientists might evaluate the societal impact of robot deployment. Law enforcement ensures the robot's operations do not compromise public safety, and the media might scrutinize the robot's influence on public perception and community dynamics. This detailed view facilitates an approach to managing community relations and regulatory compliance, ensuring the social robot system responsibly integrates into diverse public settings.

Figure 5 provides a Level 2 overview of the community resident element within the system context architecture view for a service-oriented social robot operating in public spaces. Below is a brief description of the diverse components comprising this element:

1. **Bystanders:** Individuals who are present in the vicinity where the social robot operates but do not directly interact with it. Examples include people observing the robot's activities or those incidentally in the background during robot-human interactions.
2. **Passers-by:** These are transient individuals who move through the robot's operational area without stopping to engage. They might glance at or briefly notice the robot but continue on without any direct contact.

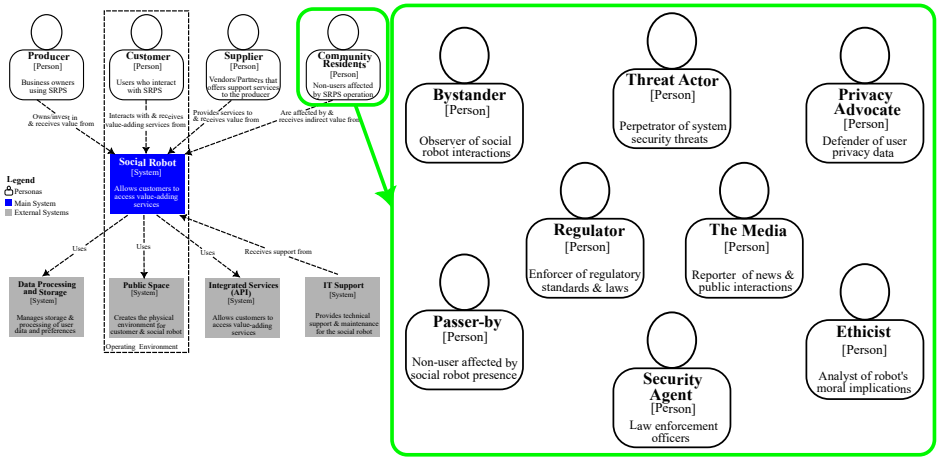


**Fig. 5** Level 2 System Context View of Community Resident Elements

3. **Regulators:** Government or agency officials responsible for ensuring that the deployment of social robots adheres to legal and regulatory standards. Examples include local government officials monitoring compliance with public safety regulations or federal agencies overseeing privacy protections.
4. **Threat Actors:** This group consists of individuals or entities that present security risks to the system. Their intentions range from exploiting system vulnerabilities for malicious purposes, such as hacking into the robot's data systems to physically harming the social robot through theft, vandalism, or direct sabotage.
5. **Privacy/Digital Rights Advocates:** Activists or organizations that focus on the implications of robotics on personal privacy and digital rights. They typically work to ensure that the technology respects user consent and data protection laws, such as GDPR.
6. **Ethicists and Social Scientists:** Professionals who study the ethical, social, and cultural implications of deploying robots in public spaces. They analyze how robots affect human behaviour, societal norms, and ethical standards.
7. **Security Agents:** Law enforcement or private security personnel who oversee the physical security of public spaces where robots are deployed. They ensure the safety of both the robot and the public from physical threats or disruptions.
8. **The Media:** Journalists and reporters who cover technological advancements and their societal impacts. In the context of social robots, they might report on the robot's deployment, public reception, effectiveness, and any controversies or successes associated with its use.

## 5.2 Systems

### 5.2.1 The Social Robot System

The internal Level 2 view of the social robot system, illustrated using the C4 model, delineates seven integral subsystems and their interconnections essential for operational functionality in public spaces. These subsystems comprise sensors, actuators, a

user interface module, an electronic processing and control module, an internal storage module, a network communication and expansion module, and a power module. Each component is briefly described below, highlighting its role and significance in the system's overall performance [1].

***Sensors***

Sensors are pivotal for enabling the robot to perceive its surroundings, integrating devices such as cameras for visual input, microphones for sound detection, and touch sensors for tactile interaction. Additional sensors, like Sonar, Lidar, laser line generators, Inertia Units (incorporating gyrometers and accelerometers), Magnetic Rotary Encoders (MRE), and Contact or Tactile Sensors, gather environmental data [78]. This data is relayed to the Electronic Processing and Control Unit, where it is analyzed to formulate appropriate responses.

***Actuators***

Actuators are crucial for translating processed commands into physical actions, allowing the robot to interact with its environment [79]. These include electric motors that facilitate movement, robotic arms for manipulating objects, loudspeakers for audio output, and Light Emitting Diodes (LEDs) for visual signals. Actuators vary in type, including mechanical, pneumatic, and hydraulic options. They operate under instructions from the Electronic Processing and Control Unit, such as a motherboard or Raspberry Pi, to execute tasks that directly affect their surroundings.

***User Interface Module***

This module enables seamless interaction between the robot and its users, featuring a touchscreen for tactile input and display, and speech recognition technology for understanding voice commands. Additionally, it includes loudspeakers for audio output and a microphone for capturing spoken responses. Serving as the primary interface, this module allows users to communicate with and control the robot, with all input and output processes coordinated by the Electronic Processing and Control Unit.

***Electronic Processing and Control Unit Module (Microcontroller)***

This module serves as the robot's central processing hub, orchestrating all system operations. It processes inputs from sensors and the user interface, formulates appropriate responses or actions, and dispatches commands to actuators and other system components. By integrating and managing data flow, this unit ensures seamless and coordinated functionality across the robot's subsystems.

***Network Interface Module***

This module facilitates the exchange of data between the robot and external systems, including API services and cloud resources [66, 80]. It is essential for receiving updates, synchronizing data, and accessing additional computational power. The module ensures continuous communication with the Integrated Services System, thereby augmenting the robot's operational capabilities. Connectivity options in this module

include Ethernet and WiFi, while expansion ports may feature HDMI, USB 2.0 and 3.0, audio input/output, and control buttons for reset, recovery, and power functions.

### *Internal Storage Module*

This module is responsible for storing data such as user preferences, operational logs, and interaction histories, collected or processed by the robot. It plays a critical role in retaining records that are vital for enhancing services, personalizing user interactions, and facilitating troubleshooting. Typically integrated within the mainboard or Raspberry Pi, this storage ensures the robot maintains essential data access and retrieval capabilities.

### *Power Module (Battery Pack)*

This module provides essential energy to all robotic components, ensuring the robot operates continuously and reliably in public spaces. It manages battery life effectively, allowing the robot to function for extended periods without needing a recharge. Efficient power management is crucial for sustaining uninterrupted service delivery in dynamic public environments.

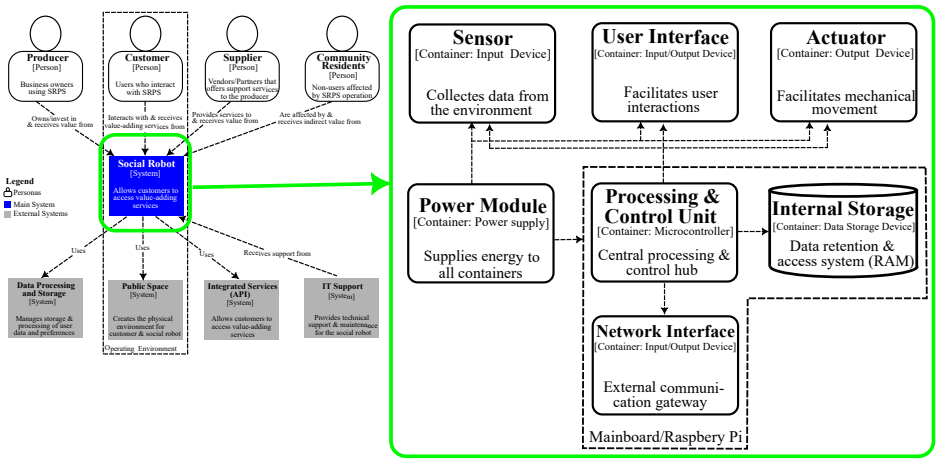


**Fig. 6** Level 2 System Context View of the Social Robot System

Figure 6 displays a streamlined view of the social robot's subsystem, where the mainboard or Raspberry Pi serves as the central unit integrating both the internal storage and network interface modules. Arrows indicate that the power module supplies battery power to all components, including the mainboard, while the microcontroller orchestrates the robot's operations. The effectiveness and efficiency of the social robot in public spaces depend on the flawless integration and constant interaction among these subsystems.

### 5.2.2 Public Space System

The Level 2 view of the public space system, as illustrated in Figure 7, delineates the diverse set of factors influencing the operation of social robots in public spaces, categorized into four main groups. This categorization aids in understanding the complex and multifaceted environment within which social robots operate [1]. It also underscores the urgency and importance of adaptive and robust design and operational strategies in the development of social robots. The groups are:

***Environmental Factors***

Concentrates on elements tied to the built environment and necessary infrastructure for robot functionality. This includes temperature control, humidity management, infrastructural aids for navigation, network connectivity, and structural stability for emergencies such as fires or floods, ensuring optimal operation in controlled settings.

***Climatic Factors***

This category covers natural weather conditions that affect robot operations, such as rainfall, sunshine, wind, varying weather patterns, and earthquake risks. These factors demand that the robot be adaptable to a broad spectrum of outdoor conditions.

***Social and Regulatory Factors***

This category includes a broad range of social norms, value systems, legal regulations, and ethical guidelines that collectively dictate how robots integrate and function within public spaces. It considers the societal expectations and the legal framework that govern the deployment and interaction of robots with the public, ensuring that operations are both socially acceptable and compliant with relevant laws. These factors are crucial in shaping the design, behaviour, and operational protocols of robots to align with community standards and ethical considerations.

***Human Interaction Factors***

This term pertains to the direct impacts of human activities on robots, including noise disturbances, physical interactions (potentially involving abuse or vandalism), diversity in language for effective communication, personal space considerations, and security risks such as theft, abuse, vandalism, and hacking.

### 5.2.3 Data Processing and Storage System

The Data Processing and Storage System serves as the central repository and processing hub for all data collected by the social robot. Given the advanced technological demands and the significant data volume, including computational requirements necessary for tasks like social navigation, perception, cognition, natural language processing, and sophisticated human-robot interactions encompassing emotional and social norm processing, it is impractical to manage these functions onboard the robot or through a single supplier [81]. This system is critical for efficiently handling extensive data arrays, from user interactions to operational logs, and includes several key components:

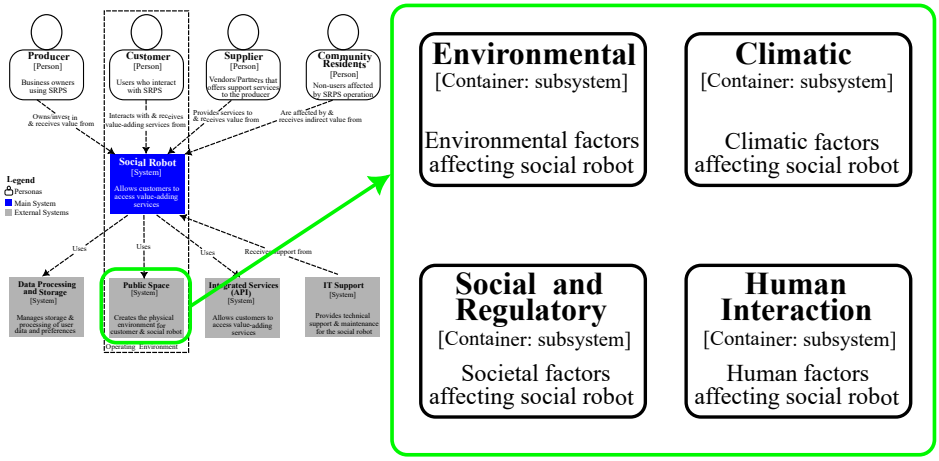


**Fig. 7** Level 2 System Context View of the Public Space System

- **Data Warehouse** Stores historical data for long-term analysis, helping in trend analysis and decision support.
- **Operational Database** Handles real-time data processing and storage, ensuring quick access to recent interaction data for immediate processing needs.
- **Data Processing Engines** These consist of advanced AI-powered computational engines designed to process incoming data swiftly. They apply algorithms and transform data according to predefined rules, essential for real-time decision-making and response generation. Each engine may specialize in specific tasks, including speech-to-text conversion, text-to-speech synthesis, multilingual support, behaviour recognition, and emotion detection, ensuring targeted and efficient data handling for various functionalities.
- **Backup and Recovery System** Ensures data integrity and availability with regular backups and robust recovery solutions to prevent data loss and support data restoration efforts.

Figure 8 presents the Level 2 container view of the Data Processing and Storage System, highlighting its two main subsystems: the Database and the Processing Engines. Each subsystem's role and function have been previously detailed, emphasizing their critical contributions to data management and computational tasks.

### 5.2.4 Integrated Services (API) System

The Integrated Services System, using APIs, bridges the social robot with external data sources and services, enhancing its functionality by integrating a variety of external systems [66]. Its main components are shown in Figure 9 include:

- **API Gateway:** Manages and routes incoming and outgoing API calls to appropriate services, providing a single point of entry for all integrations.
- **Service Directory:** Catalogs all available external services, allowing the robot to dynamically discover and interact with new services as they become available.

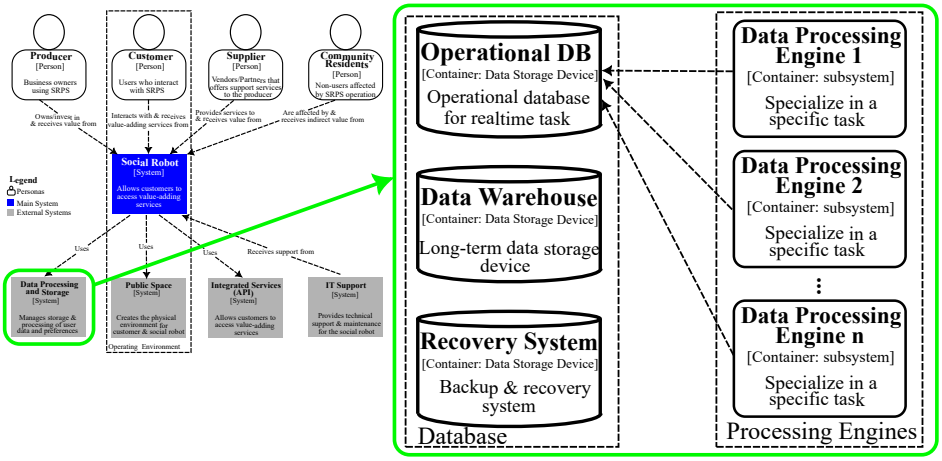


**Fig. 8** Level 2 System Context View of the Data Processing and Storage System

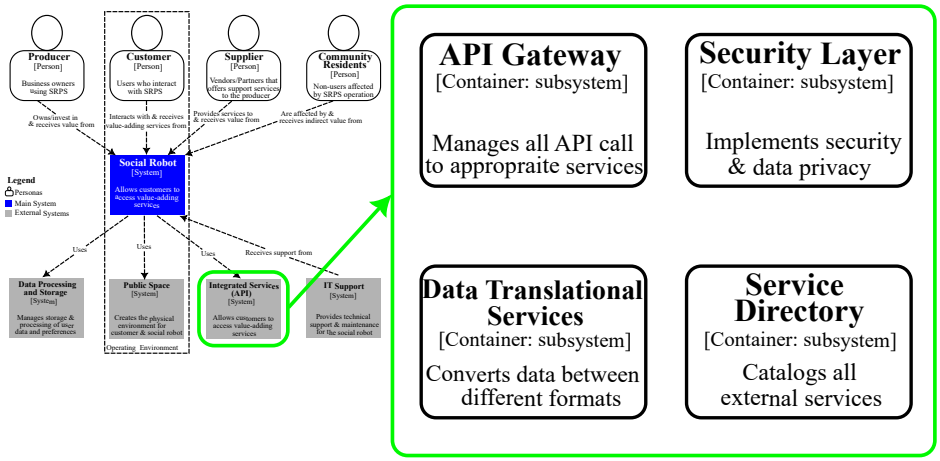


**Fig. 9** Level 2 System Context View of the Integrated Services (API) System

- **Data Translation Services:** Converts data between formats, ensuring compatibility between the robot's internal data structures and external service formats.
- **Security Layer:** Implements authentication and authorization protocols along with input data validation to secure data exchanges, preventing unauthorized access and ensuring data privacy.

### 5.2.5 IT Support System

The IT Support System provides ongoing technical support and maintenance for the social robot, ensuring its continuous and efficient operation [69]. This system is divided into several functional areas as shown in Figure 10:

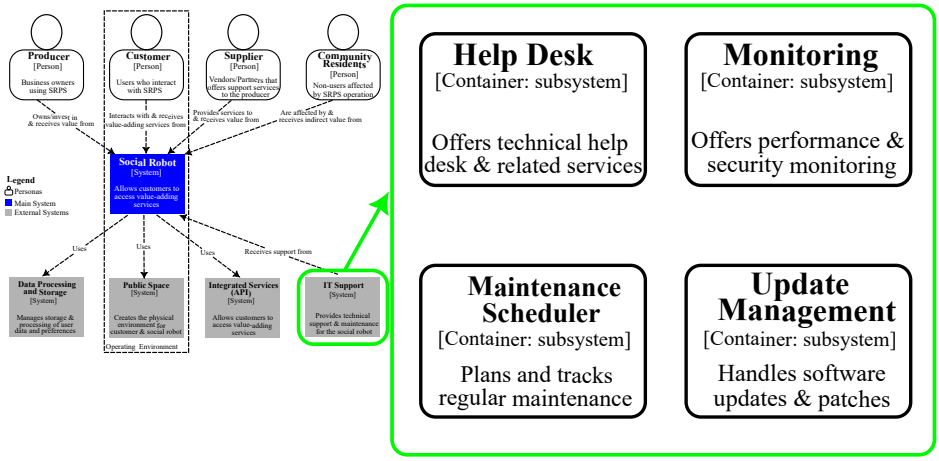


**Fig. 10** Level 2 System Context View of the IT Support System

- **Technical Help Desk:** Offers immediate assistance for operational issues, providing troubleshooting and user support.
- **Maintenance Scheduler:** Plans and tracks regular maintenance activities to prevent potential failures and ensure optimal performance.
- **Update Management:** Handles software updates and patches, ensuring that the robot's systems are up to date with the latest security patches and functional improvements.
- **Performance and Security Monitoring:** Continuously tracks system performance and security against operational parameters to quickly identify and resolve any deviations from expected performance or security breaches.

# 6 FUNCTIONAL ARCHITECTURE VIEW

The functional architectural view of a service-oriented social robot in public spaces showcases the system's operational capabilities and limitations [22]. Illustrated in Figure 11, this view details the main system (the social robot) and its interactions with internal subcomponents and external systems. Designed to engage directly with customers in public environments, the social robot delivers a range of services, from providing information and educational content to offering entertainment. These functions are enabled by an array of internal subcomponents that support the robot's operational capabilities.

## 6.1 Internal Structure of the Social Robot System

The internal structure of the social robot is intricately designed to ensure seamless integration and functionality. Each component within the robot is interconnected, with the Processing & Control Unit serving as the operational core that directs data flows and commands to other modules like sensors, actuators, and the user interface. The Network Interface bridges internal operations with external systems, supporting

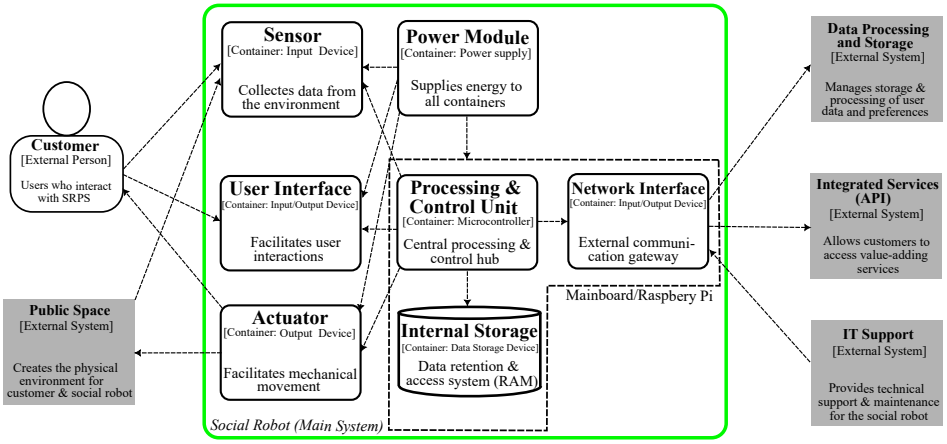


**Fig. 11** Functional Architectural View of the Social Robot System

continuous data exchange for real-time updates and synchronization. This structural design not only supports the robot's direct interactions with customers but also ensures adaptability to the varying demands of public space environments. Here's a breakdown of how each component and system functions within this architecture (See Section 5.2.1 for more details):

- **Sensors:** These are the robot's primary data collection tools, capturing a wide range of environmental inputs like visual, auditory, and tactile signals. The data from sensors is critical for the robot to perceive its surroundings and make informed decisions about how to interact with its environment and the people within it.
- **Actuators:** Actuators translate the robot's digital decisions into physical actions. This could include moving parts of the robot, such as wheels or arms, or other mechanisms like opening a compartment or adjusting an attachment. Actuators allow the robot to interact physically with its environment, performing tasks or enhancing the engagement with users.
- **User Interface:** This module serves as the interaction bridge between the robot and its human users. It typically includes devices for input (like touchscreens or keyboards) and output (like displays or speakers), enabling the robot to receive commands from users and provide responses or requested information.
- **Processing & Control Unit:** Often considered the "brain" of the robot, this unit processes all incoming data from the sensors and user inputs, runs it through programmed algorithms, and determines the appropriate outputs or actions. This unit controls all other internal components and ensures they work in harmony.
- **Internal Storage:** This component stores data that the robot collects or generates, such as user preferences, interaction logs, and operational data. This storage enables the robot to access historical data quickly, which is essential for functions like personalizing interactions based on past user engagements.
- **Network Interface:** This module provides connectivity options for the robot, allowing it to communicate with external systems and networks. It handles both

the intake of new information and the sending of data to external sources, crucial for updates, remote monitoring, or integration with broader service systems.
- **Power Module:** Supplies the necessary power to all components of the robot, ensuring they operate effectively throughout the robot's active periods. Efficient energy management within this module is critical to maintain the robot's functionality over extended periods without recharge.

## 6.2 External Systems Interacting with the Social Robot

The external systems interacting with the social robot system are described briefly below:

- **Public Space System:** Creates and manages the physical and social setting in which the robot operates. This system can influence operational parameters like navigation paths and interaction protocols, adapting to environmental and social norms. Refer to section 5.2.2 for more details on this external system.
- **Data Processing and Storage System:** Augments the robot's onboard processing capabilities, particularly for data-intensive operations or when data needs to be securely stored offsite. This system is essential for heavy computational tasks that are not feasible on the robot's own processing unit. For more details on this external system, refer to section 5.2.3.
- **Integrated Services (API) System:** Acts as a gateway for the robot to access additional functionalities and data from other service providers. This system enables the robot to offer a broader range of services by integrating external data sources and platforms through APIs. Refer to section 5.2.4 for more details on this external system.
- **IT Support System:** This system is responsible for the continuous technical support and maintenance of the social robot, ensuring all software and hardware components function optimally. It plays a pivotal role in security monitoring, maintaining data privacy, and efficiently troubleshooting and resolving technical issues that may occur during operations [67]. For more details on this external system, refer to section 5.2.5.

## 6.3 Handling Service Requests with the Social Robot System

In the scenario where a customer interacts with a service-oriented social robot in a challenging public space environment characterized by rain and noise, the flow of data through the system and its interaction with external systems play a crucial role in service delivery [7]. The brief description below outlines the sequential steps taken by the social robot system to handle a service request under such adverse conditions:

### Step 1. Service Request Initiation

**Customer Interaction:** The *customer* uses the *User Interface* module of the social robot, utilizing touch or voice commands. The interface is designed to efficiently process inputs despite ambient noise, incorporating advanced noise-cancellation technologies.

### Step 2. Data Collection and Initial Processing

**Sensory Input:** The robot's *Sensors* actively gather environmental data, including noise levels and precipitation, aiding the system in adapting its functionalities to these inputs.
**Data Processing:** The *Processing & Control Unit* receives inputs from both the user and environmental sensors, assessing the request and making necessary adjustments to ensure effective communication and response in noisy, wet conditions.

### Step 3. External Communication and Data Handling

**Network Interface Usage:** The processed data, along with any additional required inputs, is transmitted via the *Network Interface* to either the *Integrated Services (API) System* for external data (like weather updates) or the *Data Processing and Storage System* for retrieving stored user preferences or historical interaction data.
**Data Retrieval and Processing:** Necessary data is fetched and possibly further processed by the *Data Processing and Storage System* to tailor the response to the customer's needs.

### Step 4. Response Formulation and Delivery

**Response Sending:** The refined response or service confirmation is relayed back to the robot through the *Network Interface*. The *Processing & Control* Unit then formulates and sends the appropriate response to the *User Interface* for user interaction.

### Step 5. Actuation and User Feedback

**Actuator Engagement:** If the service involves physical action, such as moving to a covered area or handing out materials, the *Actuators* execute these tasks under the direction of the *Processing & Control Unit*.
**Final Interaction:** The customer receives the service via the *User Interface*, with adjustments like increased screen brightness or volume to counteract the rain and noise.

### Additional Considerations:

**Environmental Adaptations:** The robot's systems continually adjust to ongoing rain and noise, enhancing screen brightness or volume for clarity.
**Security and Privacy:** All personal data transmissions are securely handled, with encryption and secure network protocols managed by the *Network Interface*.

# 7 SECURITY PERSPECTIVE

The security architectural perspective encompasses a suite of architectural strategies, practices, and principles designed to equip a system with specific security-related attributes across multiple architectural views [82]. Often overlooked in the early stages of project development, security considerations are crucial but challenging due to their

complexity and the detailed analysis they require. This oversight may stem from a misconception that security is a concern to be handled by specialized teams rather than a responsibility of the organization as a whole [52].

For service-oriented social robots operating in public spaces, defining clear security objectives is essential. These objectives outline the system's capacity to manage, monitor, and audit access and actions performed on system resources, ensuring robust mechanisms are in place to detect and recover from security incidents [83]. The security architectural perspective addresses key concerns such as resources, principals (users and systems that interact with or manage the system) [84], policies (rules governing access and use), threats (potential sources of compromise), security objectives (goals for protecting the system), and security mechanisms (tools and protocols to enforce security).

We adopted the five-step security activity methodology proposed by Rozanski and Woods, [52] to frame the security architectural perspective of this study. This structured approach begins with identifying sensitive resources within the system, followed by defining the security policy tailored to protect these resources. Subsequently, it involves identifying potential threats to the system, designing the security implementation to mitigate these threats, and assessing the security risks involved. Each of these steps is detailed in the following subsections, providing an overview of our security strategy.

## 7.1 Identifying Security-Sensitive Resources (Assets) in the Social Robot System for Public Spaces

Before securing the system, it's crucial to pinpoint what needs protection. Across all architectural views, we've identified four key categories of sensitive resources (Assets) [73]: Hardware, Software [85], Principals [84], and Data, each with unique characteristics and vulnerabilities.

1. **Hardware:** This category includes all the physical components of the system, which are susceptible to both physical and cyber-attacks [86]. Examples include the social robot itself, external data storage devices, and network communication infrastructure. These components are critical as they are the tangible parts of the system exposed to direct interaction and external threats.
2. **Software:** Comprising operating systems, application software, and utility software, this category is vulnerable to a variety of software exploits and cyber-attacks [85]. For instance, the operating system Ubuntu, application software like ROS and its packages, and other utility software form the backbone of the robot's functionality and are prime targets for exploitation.
3. **Principals:** This category refers to entities the system must securely identify for security operations, including persons, roles, equipment, or other systems. These principals are often targets of impersonation, manipulation, and social engineering attacks, making reliable identification crucial for maintaining system integrity [84].

4. **Data:** Referring to all user or system data, whether at rest or in transit, this category is governed by strict privacy laws and is frequently targeted in cyberattacks [65]. Ensuring the security of data, especially sensitive user information, is paramount for compliance and user trust.

Table 4 summarizes the descriptions, examples, and potential threats associated with the security-sensitive resources of a service-oriented social robot operating in public spaces. It provides an overview of each resource category's relevance and vulnerabilities in the system's security architecture [73].

**Table 4** Summary of Security-Sensitive Resources: Descriptions, Examples, and Threats for the Social Robot System

| Resource | Description | Examples | Potential Threats |
|---|---|---|---|
| **Hardware** | Physical components of the system that are exposed to both physical tampering and cyber threats. | Social robots, external data storage devices, and network communication infrastructure. | Physical damage, theft, unauthorized access, cyberattacks. |
| **Software** | Programs and operating systems subject to software exploits and cyberattacks. | Operating system (Ubuntu), ROS, database management systems. | Malware, ransomware, software bugs, unauthorized modifications. |
| **Principals** | Entities requiring secure identification and access control to prevent unauthorized actions. | Users, administrators, service technicians, equipment, or other systems that interact with the social robot. | Impersonation, social engineering, unauthorized access. |
| **Data** | Sensitive information that must be protected both in transit and at rest, subject to privacy laws and susceptible to breaches. | User data, system logs, configuration settings | Data breaches, unauthorized disclosure, manipulation. |

## 7.2 Defining Security Policy for the Social Robot System

The security policy specifies the security requirements of the social robot system. It outlines the necessary controls to protect system resources and specifies access permissions for different principals or groups. The policy acts as a security framework, detailing constraints and access provisions that the system must enforce [83].

After identifying the sensitive resources and potential threats, formulating a security policy (or trust model) is critical. This policy underpins the security architecture, stipulating access rights for various principals to system resources, sometimes with conditions such as time or day restrictions. It also defines the integrity and accountability measures needed when accessing sensitive resources [87].

A well-defined security policy should classify resources and principals into groups based on roles and organizational units rather than individual specifics. This approach emphasizes policy over design, focusing on 'what' access is allowed rather than 'how' it is implemented [88].

Creating a security policy for the social robot system involves [89]:

1. **Principal Classes Identification:** Organize principals into classes based on their roles and access needs to various resource types. Principals can be categorized into Robot Operators, IT Support Staff, and End Users (Customers) [84]. Robot Operators may require access to operational controls and maintenance functionalities, IT Support Staff needs access to software updates and security configurations, and End Users interact mainly with the user interface for services [90].
2. **Resource Classes Identification:** Group sensitive resources into classes that can be uniformly managed for access control. Sensitive resources can be segmented into Physical Hardware (robot body, sensors, actuators), Software Systems (operating system, application software), and Data (user data, operational logs). This classification helps in applying uniform security policies across similar resource types [91].
3. **Access Control Sets Definition:** For each resource class, determine permissible operations and the principal classes authorized to perform these operations. For example, the Data resource class, define operations like Read, Write, and Delete. IT Support Staff may be granted Read and Write permissions to operational logs for troubleshooting, while End Users may only have Read access to their personal interaction history [92].
4. **Sensitive System Operations Identification:** Define access permissions for system-level operations that go beyond managed resources, like administrative functions. Identify critical system-level operations such as firmware updates, system restarts, or changes to security settings, which should be accessible only to IT Support Staff or designated Robot Operators. Administrative functions like these are crucial and should be restricted to authorized personnel only [69].
5. **Integrity Requirements Identification:** Specify integrity safeguards for operations that involve information modification or are particularly sensitive, such as audit trails or dual approval systems. Implement audit trails and require dual approval for actions such as accessing stored user data or modifying the robot's core settings. This might involve an IT administrator approving changes made by a Robot Operator, ensuring an extra layer of security and integrity for sensitive operations [93].

### 7.2.1 Security Objectives

Security objectives establish the overarching goals and desired outcomes of security measures within a system. For a service-oriented social robot in public spaces, these objectives are critical in guiding the development and implementation of security strategies. Essential security objectives include confidentiality, integrity, availability, accountability, auditability, detection and recovery, and data privacy [88]. Together, these objectives not only dictate the direction and priorities of security efforts but also define the key areas of focus for protecting the system and ensuring optimal security performance. These seven objectives are integral to maintaining a secure and reliable operation of social robots in dynamic public environments.

***Confidentiality***

Ensures that sensitive information, such as user data or operational specifics, is kept secret and only accessible to authorized individuals or systems. This objective demands encryption protocols for data at rest and in transit, user authentication mechanisms, and strict access controls.

***Integrity***

Protects data and system operations from unauthorized changes, ensuring that all data transmissions, operations, and processes are executed as intended, free from alterations or tampering. Requirements for integrity include secure, tamper-evident data storage, checksums, and hash validations to detect and prevent unauthorized modifications.

***Availability***

Ensures that the social robot and its services are accessible to users when needed, even under adverse conditions or attack scenarios. This involves implementing robust failover and redundancy systems, regular maintenance schedules, and performance monitoring to handle potential downtimes or disruptions efficiently.

***Accountability***

Holds users and systems accountable for their actions within the system. Implementing strong authentication and authorization protocols, logging of user activities, and traceable user sessions are essential requirements for ensuring that all actions can be attributed to a specific entity.

***Auditability***

Allows system activities to be audited through transparent and accessible logs. This requires maintaining detailed and immutable logs of all system and user activities, which can be reviewed to ensure compliance with policies and to trace suspicious activities retrospectively.

***Detection and Recovery***

Involves the capability to detect security incidents promptly and recover from them effectively, minimizing the impact on system operations and data integrity. Security requirements here include the implementation of intrusion detection systems, regular system and data backups, and incident response protocols to address and mitigate security breaches quickly.

***Data Privacy***

Protects personal and sensitive information from unauthorized access and misuse, aligning with legal standards such as GDPR. Data privacy measures involve ensuring that data collection, processing, storage, and sharing are performed in compliance with privacy laws and user consent, implementing data minimization principles, and providing users with access and control over their data.

### 7.2.2 Security Requirements

Security requirements are the specific conditions or capabilities that a system must meet to comply with the security policy and achieve the security objectives. These include technical specifications, procedural rules, and compliance needs that the system must fulfil to ensure it is secure [94]. Security requirements translate the broad directives of the security policy into detailed, actionable, and measurable tasks. They are essentially the implementation steps needed to achieve the security objectives and adhere to the security policy. These requirements cover all aspects of the system, including hardware, software, human interactions, and environmental factors.

The relationship dynamics among security objectives, policy, and requirements are integral to system security. Security objectives set the overarching goals that dictate the security policy's purpose and direction, serving as abstract guides for the security approach. The security policy, structured around these objectives, lays out specific guidelines and forms the governance structure necessary for maintaining security integrity. Stemming from this policy, security requirements detail the operational and technical actions needed to fulfil these objectives, specifying the responsibilities, tools, and processes required to ensure the system's security [88].

## 7.3 Identifying Threats to the Social Robot System

Identifying threats is crucial for defining the security needs of the social robot system, focusing on what must be protected and from whom. This stage culminates in the creation of a threat model (an analysis that includes an inventory of potential threats, their impacts, and likelihoods). The threat model is essential for understanding the vulnerabilities and preparing appropriate defensive measures [37].

To develop a robust threat model for the social robot security system, we posed several critical questions to understand the Tactics, Techniques, and Procedures (TTP) of potential threat actors [95]. These questions aimed to identify who might breach the security policy, their motivations, and the methods they might use to circumvent security measures. Additionally, we considered the characteristics of these potential attackers, such as their sophistication, resources, and commitment, as well as the consequences of potential security breaches. This structured inquiry helps in crafting detailed defensive strategies to protect the system effectively.

It's important to acknowledge that threats may originate from both external sources, such as cybercriminals or competitors, and internal sources, including current or former employees who may exploit their access and knowledge of the system [96]. Internal threats are particularly insidious as insiders can often bypass security controls more easily than external attackers [97]. Furthermore, the system's deployment environment (public space) can significantly influence the nature of threats.

### 7.3.1 Tactics, Techniques, and Procedures (TTP) of Threat Actors

Tactics, Techniques, and Procedures (TTPs) describe the behaviours, strategies, and methods employed by attackers to orchestrate cyberattacks on systems [95]. Tactics define the overarching goals or objectives behind an attack; techniques detail the

methods and strategies used to conduct the attack; and procedures outline the tools and processes employed to facilitate the attack.

**Table 5** Summary of Threat Actor Categories, TTPs, and Motivations for Attacks

| Threat Actor | Tactics | Techniques | Motivations |
|---|---|---|---|
| **Internal** | Infiltrate system internally | Use of authorized credentials | Financial gain, espionage, sabotage, revenge |
| **External** | Breach security system externally | Hacking, phishing, malware | Financial gain, competitive advantage, political / ideological reasons |
| **Supply Chain** | Compromise during fabrication / supply | Insertion of backdoors | Economic or political espionage, sabotage |
| **Public Space** | Exploit public space accessibility | Physical or remote disruption | Vandalism, theft, sabotage, natural disaster impacts |

For the social robot system, we have delineated four principal groups of threat actors: Internal, External, Supply Chain, and Public Space actors. Table 5 provides an overview of these categories, detailing their tactics, techniques, and motivations for engaging in malicious activities.

1. **Internal Threat Actors:** These include employees, authorized users, and organization staff who have internal system access. Insider threats can arise from intentional acts, as well as unintentional errors due to mistakes, recklessness, or inadequate training [97]. Examples also include users under duress, such as those compelled by external pressures to compromise the system [98].
2. **External Threat Actors:** Individuals or groups outside the organization who typically do not have authorized access. These may include hackers, cybercriminals, competitors, organized crime groups, and state actors, who may engage remotely or physically within public spaces [35].
3. **Supply Chain Threat Actors:** Those involved in the creation, distribution, or maintenance of the robot's components. They can introduce vulnerabilities into the robot's hardware, software, or communications infrastructure during any phase of its lifecycle [99].
4. **Public Space Threat Actors:** Includes both human actors like vandals, thieves, or saboteurs, and natural/man-made disasters such as fires, floods, or other catastrophic events. These actors capitalize on the robot's physical exposure in public environments [37].

Expanding on our foundational research into the threat landscape and attack surface of the social robot system [37], we have compiled a list of approximately 30 distinct threat actors that fall into these primary groups. This detailed classification, available in Table A6 of Appendix D, includes entities such as malicious users, privileged attackers, competitors, spies, state-level intelligence agents, and other potential adversaries. Furthermore, we have categorized the motivations for these actors into seven main objectives (ranging from information gathering and privilege escalation to data modification, unauthorized command execution, service disruption, and asset destruction)

summarized in Table A7 of Appendix D. Additionally, we have outlined 77 potential attack types classified under physical, cybersecurity, social, and environmental (public space) attacks, further enriching our understanding of the diverse threats faced by the system.

### 7.3.2 Threat Model for the Social Robot System

The threat model for the social robot system operating in public spaces is a structured representation of all the potential threats that could impact the system, helping to prioritize security measures based on the likelihood and potential impact of these threats. This model synthesizes data from previously identified security-sensitive resources and categorized threat actors, enhancing the understanding of the risks faced by the system [100].

To develop this threat model, we begin by outlining potential threat pathways, classifying them into scenarios such as unauthorized access, data breaches, physical damage, and system disruptions. Each scenario is evaluated for its probability and the severity of its impact, with a focus on vulnerabilities in the social robot's architecture that could be exploited by various threat actors. Drawing from our prior research [37], in which we used the ENISA template for AI cybersecurity in autonomous systems, we delineate four primary attack scenarios for the social robot system: user abuse of the social robot, system compromise, insider threats, and exploitation for social engineering purposes. For each scenario, we detail the attack's description, impact, detectability, risk of cascading effects, affected assets, involved stakeholders, attack steps, recovery time and effort, existing gaps and challenges, and potential countermeasures. This structured approach not only guides the development of the threat model but also provides a robust structured approach for understanding and mitigating risks associated with the social robot system.

## 7.4 Designing Security Implementations to Mitigate Threats

The integration of service-oriented social robots in public spaces introduces specific security challenges that, while unique in context, align with familiar principles in cybersecurity. To counteract these challenges, we've adopted a defence-in-depth approach, emphasizing layered security measures [27]. Our strategy encompasses seven key security mitigation approaches: physical security, endpoint security, identity and access management, application security, network security, data security, and cloud security, complemented by robust security operations which include monitoring, response, and recovery. These measures are interconnected, often overlapping in their functions and responsibilities, yet each is crucial in fortifying the robot's defence against potential threats.

### 7.4.1 Overview of Cybersecurity Approaches for Social Robots in Public Spaces

Here is a brief summary of the proposed cybersecurity strategies for social robots operating in public spaces.

***Physical Security***

Ensures the protection of the robot's hardware and associated infrastructure from physical threats such as theft, vandalism, or natural disasters. Measures include secure enclosures, surveillance systems (CCTV), and controlled access environments to safeguard the robot and its operational context [49].

***Endpoint Security***

Focuses on protecting the endpoints of the robot system, including any user interfaces or connection points. This approach employs anti-malware software, intrusion detection systems, and regular security patches to prevent unauthorized access and attacks [101].

***Identity and Access Management (IAM)***

Involves managing the digital identities and access rights of all users and systems interacting with the robot. Techniques include the use of strong authentication methods, role-based access control, and auditing and logging to ensure that only authorized entities can access sensitive functions and data [102].

***Application Security***

Addresses the security considerations needed to protect the robot's applications from exploits. This includes the development of secure code, regular application testing (such as penetration testing and vulnerability assessments) [103], and the implementation of application firewalls and encryption [104].

***Network Security***

This involves protecting the data being transmitted across networks to and from the robot. Methods include using VPNs, firewalls, secure Wi-Fi protocols, and intrusion prevention systems to shield data from interception or manipulation [105].

***Data Security***

Ensures that all data collected, processed, or stored by the robot is protected against unauthorized access and leaks [65]. Data security measures include encryption, data masking, and stringent access controls, coupled with secure backup and data loss prevention strategies.

***Cloud Security***

This pertains to protecting any cloud-based resources utilized by the robot for processing or storage. This includes employing cloud-specific security policies, secure access credentials, and encrypted communication channels [75].

***Security Operations and Control***

Comprises continuous monitoring, threat detection, incident response, and recovery procedures to quickly address any security breaches [69]. It incorporates the use of security information and event management (SIEM) systems, regular security audits,

and a well-defined incident response plan to maintain ongoing system resilience and integrity.

### 7.4.2 Security Perspective Architectural View

We have developed a security perspective architectural view for the service-oriented social robot system, incorporating all components previously discussed [82], including the introduction of 'Principals'—entities requiring identification and authentication, which could be individuals or systems [84]. Figure 12 visually demonstrates the security implementations designated for each system element and container, applying a suite of security strategies to safeguard the social robot system in public environments.

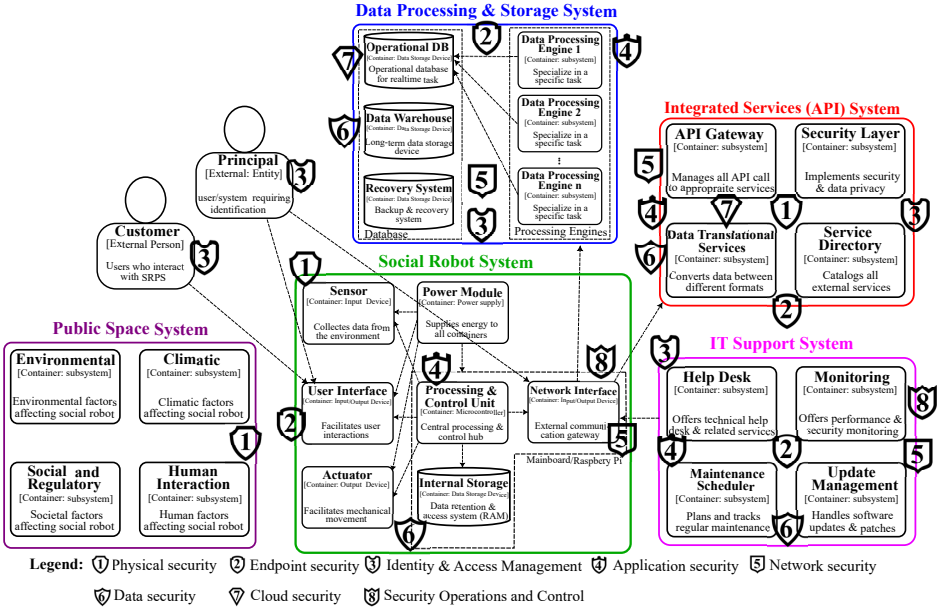


**Fig. 12** Security Perspective Architectural View of the Social Robot System

The delineation of specific security control mechanisms to particular elements or containers is challenging due to the interconnected nature of the system's operations. Nevertheless, we have endeavoured to assign certain security controls to specific elements and containers, recognizing that the impact of these controls might extend beyond the designated boundaries. Table 6 summarizes the security control approaches employed across each element and subsystem. For example:

- *Physical Security* is relevant to the social robot, public space, and Integrated Services (API) System [49].
- *Endpoint Security* covers all endpoints and devices such as the social robot, Data Processing and Storage System, Integrated Services (API) System, and IT Support System [101].

**Table 6** Applicability of Security Measures Across System Components of the Social Robot System

| Element | Physical security | Endpoint security | Identity & Access Management | Application security | Network security | Data security | Cloud security | Security Operations & Control |
|---|---|---|---|---|---|---|---|---|
| Social Robot System | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ |
| Public Space System | ✓ | | | | | | | |
| Data Processing & Storage System | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Integrated Services (API) System | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Customer | | | ✓ | | | | | |
| Principals | | | ✓ | | | | | |
| IT Support System | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |

- *Identity and Access Management (IAM)* is crucial for Customers, Principals, IT Support Systems, Data Processing and Storage Systems, and the Integrated Services (API) System [23].
- *Application Security* is necessary wherever software applications are operational, including the social robot, Data Processing and Storage System, Integrated Services (API) System, and IT Support System [85].
- *Network Security* is implemented across all network-connected components like the social robot, Data Storage and Processing System, Integrated Services (API) System, and IT Support System [105].
- *Data Security* is enforced on the social robot, Data Processing and Storage System, Integrated Services (API) System, and IT Support System [65, 67].
- *Cloud Security* measures are applied to the Data Processing and Storage System and the Integrated Services (API) System [75].
- *Security Operations* primarily involve the IT Support System and the social robot [69].

In the subsequent subsection, we will explore specific security threats that these measures are designed to mitigate within the context of a service-oriented social robot operating in public spaces.

### 7.4.3 Physical Security

Physical security involves implementing various measures to protect the social robots and their supporting infrastructure from physical threats, such as damage, theft, and unauthorised access [49]. Given that social robots are designed to interact with humans in public areas, their physical integrity is paramount for both the protection of the technology and the safety of individuals in its vicinity [37].

The physical security of these robots is multifaceted. It begins with robust design, utilising durable materials that can withstand physical interaction and resist potential vandalism [96, 106]. Tamper-proofing is also essential, ensuring that the robot's internal components are secured against unauthorised access with measures like sealed compartments and specialised screws. Alarm systems are incorporated to alert when the robot is being moved or tampered with improperly [107]. Geo-fencing utilises GPS to create virtual boundaries, triggering alerts if the robot strays outside designated zones [108].

For immediate safety, robots are equipped with an emergency stop mechanism that anyone can activate to halt operations instantly. High visibility through distinctive branding helps deter theft and makes it easier for the public to identify and report the robot if it's out of place [109]. Including various sensors, like cameras and proximity sensors, enables the robot to avoid collisions and detect tampering or unsuitable environments. Tethering the robot to a specific location can prevent theft and limit movement in certain contexts.

Remote monitoring capabilities allow security personnel to oversee the robot's status from afar, intervening as necessary [110]. Ensuring that staff and security teams are well-trained on the robot's functionality and potential security threats is another layer of protection. Additionally, public awareness campaigns can play a significant role in discouraging tampering and promoting community vigilance.

Finally, secure storage protocols for when the robots are not in active use protect them from theft and vandalism, completing the circle of physical security measures. Collectively, these strategies form an extensive framework to ensure social robots' physical safety, data, and people around them, enabling them to perform their designated functions effectively and securely [86].

### 7.4.4 Endpoint Security

Endpoint security protects devices like workstations, servers, mobile devices, and social robots from cyber threats [24]. These devices, known as endpoints, are vulnerable when connected to corporate networks and can be exploited by cybercriminals. Effective endpoint security solutions detect, analyze, block, and mitigate attacks in real time, preserving network integrity by ensuring that all devices adhere to stringent security protocols, thus safeguarding against data breaches and cyber threats [101].

Endpoint Protection Platforms (EPP) are specialized software deployed on endpoints, linked to centralized security analytics and management interfaces to ensure robust protection. Popular EPPs include Cortex XDR[5], Crowdstrike Falcon[6], SentinelOne Singularity Platform[7], Harmony Endpoint[8], and Microsoft Defender Endpoint[9]. These platforms often extend beyond basic endpoint security, providing monitoring, threat discovery, and response across network, endpoint, and cloud environments. Subscription to these services, especially for service-oriented social robots

[5] https://www.paloaltonetworks.com/cortex/cortex-xdr
[6] https://www.crowdstrike.com/platform/
[7] https://www.sentinelone.com/platform/
[8] https://www.checkpoint.com/harmony/endpoint/
[9] https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint

in public spaces, offers the additional advantage of advanced security protection and access to threat intelligence, ensuring cyber defence.

### 7.4.5 Identity and Access Management (IAM)

Identity and Access Management (IAM) is a framework of business processes, policies, and technologies that facilitates the management of electronic or digital identities. By managing roles and access privileges for individual network users and the conditions in which access privileges are granted or denied, IAM systems ensure that the right individuals access the right resources at the right times for the right reasons [23]. It includes *Administration* for creating and managing user accounts, ensuring up-to-date permissions; *Authentication*, which verifies user identities through various methods like passwords and biometrics; *Authorization*, which grants access to resources post-authentication; and *Auditing*, which monitors the integrity of the entire IAM process [111]. These components work cohesively to ensure that system interactions are secure, traceable, and conform to established security protocols, thereby safeguarding against unauthorized access and maintaining operational integrity within the SRPS system.

Figure 13 presents a nuanced multi-tiered architecture crucial for managing access and identity within social robots' security infrastructure in city ferry operations with insights from ISO/IEC 24760-2:2015 [112]. Building upon the security perspective depicted in Figure 12, this architecture is meticulously designed to ensure that every interaction within the system is secure, from the user level to the cloud [113].

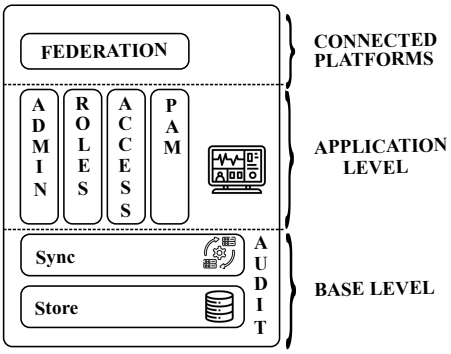


**Fig. 13** Multi-tiered architecture for SRPS Identity and Access Management

The architecture lays the groundwork for robust data storage and management at the base level, integral to the system's integrity. This foundation is strengthened by synchronization mechanisms that harmonize data across single or multiple storage solutions, including virtual and meta-databases. These synchronization platforms ensure that data is consistently accurate and readily available, forming the backbone of the robot's memory and knowledge base.

Above this, at the application level, lies the operational core of the system, where various components work in tandem to safeguard the robot's interactions with its users and the environment. The ADMIN function meticulously creates, modifies, and

removes user profiles, roles, and permissions, ensuring only authorized users have system access. Diverse user roles are managed here, each being meticulously defined and assigned specific permissions. The ACCESS control segment [114] takes charge of both authentication, verifying the identity of users and applications, and authorization, granting them specific access rights based on their roles. Privileged Access Management (PAM) [115] is another cornerstone at this level, managing heightened access rights and ensuring that elevated permissions are carefully allocated and monitored. Lastly, the AUDIT function [116] performs monitoring, tracking user behaviours, access patterns, and potential security breaches, thereby upholding accountability and creating an audit trail for actions within the system.

At the topmost tier, the architecture encompasses Connected Platforms, highlighting the system's integration with external cloud services and other platforms. The FEDERATION component [117] is pivotal at this level, facilitating cloud services' seamless and secure connection into the core system, ensuring that the entire architecture functions as a cohesive unit. Federation capabilities allow the system to maintain a unified control and management perspective overall integrated platforms, bolstering interoperability and security simultaneously.

This architecture delineates clear responsibilities across its three levels, ensuring robust and scalable Identity and Access Management for social robots operating in public spaces. It seamlessly integrates with external platforms, providing a security structure designed to protect against various threats without compromising system functionality or user accessibility.

### 7.4.6 Application Security

Application security refers to the practices and policies that are implemented to protect software applications from external threats such as cyberattacks, data breaches, and other forms of unauthorized access [85, 104]. This field of security focuses on securing an application at every phase of its development and deployment lifecycle to prevent vulnerabilities that malicious actors could exploit. The goal is to thwart unauthorised access, code or data tampering and to prevent service disruptions, ensuring applications operate securely and as intended [118]. Implementing secure coding practices is fundamental [119], which means developers are tasked with writing code that anticipates and mitigates security risks by adhering to established coding principles, utilising trusted libraries, leveraging standardised architectures, understanding common coding pitfalls as outlined by resources like the OWASP Top 10 [120], and maintaining a detailed software bill of materials for transparency [121].

Security testing is another pillar of application security [122], comprising techniques like Static Application Security Testing (SAST) [123], which scrutinises code to find vulnerabilities; Dynamic Application Security Testing (DAST) [124], which tests the running application for real-time vulnerabilities; and Interactive Application Security Testing (IAST) [125], which integrates aspects of both SAST and DAST for thorough vulnerability detection. Additionally, runtime application protection mechanisms such as Web Application Firewalls (WAF) and Runtime Application Self-Protection (RASP) [126] are deployed to identify and mitigate threats during an application's

operation. With modern applications often dependent on numerous third-party components, dependency scanning [127] becomes crucial to determine any embedded vulnerabilities. Lastly, a diligent patch management process is vital to ensure that applications are routinely updated and patched [128], addressing known vulnerabilities promptly to maintain the security integrity of the city ferry's social robot.

Moreover, adopting the "shift-left" approach, as exemplified in DevSecOps practices [129] and frameworks such as the Microsoft Security Development Lifecycle [130], OWASP Software Assurance Maturity Model (SAMM) [131], NIST's Secure Software Development Framework (SSDF) [132], McGraw's Touchpoints [133], Building Security In Maturity Model (BSIMM) [134], and Software Assurance Forum for Excellence in Code (SAFECode) [135], emphasizes the integration of security at early stages and throughout the software development process. This proactive strategy not only bolsters security but also mitigates costs and delays that typically arise from addressing security issues after development. Additionally, diligent patch management is crucial, ensuring that applications are consistently updated and patched to address known vulnerabilities swiftly. This ongoing maintenance is vital for preserving the operational and security integrity of the city ferry's social robot.

### 7.4.7 Network Security

Network security encompasses the practices and policies aimed at protecting the integrity, confidentiality, and accessibility of the social robot's network infrastructure and data, utilizing a combination of hardware and software technologies [25]. Central to these efforts are firewalls [136], which serve as vigilant gatekeepers, monitoring and controlling network traffic based on established security policies to differentiate between trusted and untrusted networks. Distributed firewalls extend this protective measure across multiple network segments, improving scalability and fault tolerance. However, these systems introduce challenges such as the complexity of managing consistent policies across a distributed landscape and potential performance impacts due to the processing overhead [137]. Complementing these are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) [138], which detect and alert suspicious network activities and can actively intervene to block potential threats. Virtual Private Networks (VPN) [139] are essential for providing secure, encrypted connections for remote access to the private network, a feature increasingly utilised by mobile or remote employees.

Network Access Control (NAC) [140] permits only verified and compliant devices network access, controlling the scope of data accessible to each device. This is bolstered by antivirus and antimalware software, which is crucial in identifying and preventing malicious software from compromising the network. Behavioural analytics [141] tools play a vital role by establishing a baseline of normal network behaviour and identifying deviations, signalling possible security incidents. Securing Wi-Fi networks [142] through encryption is critical to prevent eavesdropping and unauthorised access. At the same time, Data Loss Prevention (DLP) technologies and strategies [143] are essential to safeguard sensitive data from loss, misuse, or unauthorised access. Together, these components form a network security strategy necessary for protecting the interconnected systems within the city ferry's digital infrastructure.

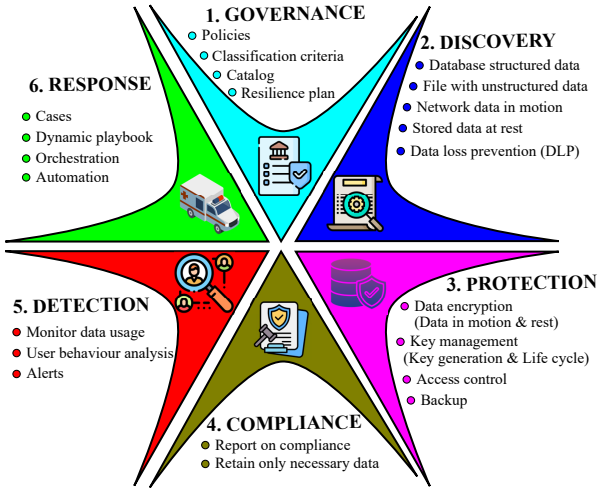


**Fig. 14** Data security Ecosystem for Social Robots in Public Spaces

### 7.4.8 Data Security

Data Security refers to the protective measures, strategies, and techniques used to safeguard data from unauthorized access, corruption, loss, or breaches. It encompasses both digital data (on computers, servers, databases) and physical data (paper records) [26]. Figure 14 delineates the multifaceted approach to data security for the city ferry's social robot, encompassing a spectrum of strategies designed to protect data integrity and prevent unauthorised access. Governance [144] sets the stage with policies defining secure data practices, classification criteria to distinguish data sensitivity, catalogues for asset organisation, and resilience plans to maintain data availability amidst disruptions. Discovery [145] focuses on understanding data storage and movement, highlighting structured data within databases, unstructured data in files, the flow of network data, and stored data at rest, all under the watchful eye of Data Loss Prevention (DLP) mechanisms.

Data protection [146], both in transit and at rest, is ensured through encryption and the careful management of cryptographic keys, strict access controls, and regular data backups. Compliance [147] is about adhering to legal standards, with rigorous reporting on compliance and a policy to retain only essential data. Detection strategies include the ongoing monitoring of data usage, analysis of user behaviour to spot irregularities, and alerts to flag unauthorised activities [148]. Finally, the response component outlines the swift and coordinated actions taken post-detection, from managing specific cases to deploying dynamic playbooks, orchestrating a unified security response, and utilising automation to resolve security incidents efficiently without manual intervention [149]. This data security ecosystem ensures that every aspect, from policy to practice, is geared towards maintaining the utmost security for the social robot's operations within the public space.

### 7.4.9 Cloud Security

Cloud Security is a term encompassing the suite of strategies, controls, technologies, and procedures that collectively protect the cloud's vast array of intellectual properties, data, applications, services, and the infrastructure they reside on [75]. As a subset of broader security disciplines like computer and network security, cloud security represents a specialised focus within the information security domain.

When compared with on-premises security [80], the cloud security landscape presents both contrasts and challenges stemming from the fundamental differences between cloud-based and traditional IT environments. Organisations exert complete control over their physical servers and infrastructure in conventional settings, tailoring security measures to precise specifications. In contrast, cloud security often requires entrusting certain aspects of security to cloud service providers, particularly in IaaS and PaaS models, while ensuring these providers adhere to stringent security protocols.

Scalability and flexibility are further points of divergence; where on-premises solutions demand substantial time and resources to scale, cloud services boast almost instantaneous scalability with security mechanisms that adapt and maintain protection in tandem [150]. Access points in cloud security also differ, with the cloud offering ubiquitous access instead of the geographically limited or VPN-dependent access of on-premises solutions.

The shared responsibility model is intrinsic to cloud security, where duties are split between the cloud provider and the customer, unlike the sole responsibility borne by organisations in conventional setups [151]. This model delineates clear boundaries for instance, the cloud provider may secure the infrastructure while the customer safeguards their hosted data and applications.

Patch management is another area where cloud services often have the edge, with SaaS models offering automatic software updates and patches, reducing the risk of vulnerabilities arising from unpatched systems [152]. This responsibility rests solely on the organisation in an on-premises scenario.

Data storage location also marks a significant difference; on-premises data is typically centralised within a physical location, while cloud-stored data may span multiple data centres and regions, introducing variables related to data residency and regulatory compliance. The cost structure of cloud security typically follows an OpEx model, which contrasts with the CapEx-intensive nature of on-premises security, requiring upfront investment in hardware and software.

Lastly, visibility and complexity in cloud security present unique challenges due to cloud services' dynamic and distributed nature, which can complicate asset monitoring and management compared to the more contained environments of on-premises systems.

In summary, while the primary aim of safeguarding assets remains consistent across both cloud and conventional security, the approach and execution in cloud environments necessitate a nuanced understanding and strategic adaptations tailored to meet the distinctive demands of cloud computing.

### 7.4.10 Security Operations and Control

Security operations and control for information systems encompass the deployment and management of protective measures to safeguard the confidentiality, integrity, and availability of information and systems. This critical function is designed to detect security threats and provide timely alerts, facilitating swift and efficient response actions [153]. It involves leveraging security information and event management (SIEM) systems [154], conducting regular security audits, and maintaining a robust incident response plan to ensure continuous system resilience and integrity. Typically, these services are available as part of an endpoint security platform, offering an approach to security management and threat mitigation.

#### *Security Information and Event Management (SIEM)*

SIEM systems act as the nerve centre for security monitoring, providing real-time analysis of security alerts from various hardware and software sources. They aggregate and analyse log data, offering real-time alerting, data storage for forensic analysis, and data correlation to discern patterns indicative of cyber attacks [154]. SIEM dashboards provide a comprehensive view of an organisation's security posture. At the same time, its threat detection capabilities are enhanced by predefined rules and threat intelligence integrations, facilitating swift investigative responses and aiding in compliance reporting.

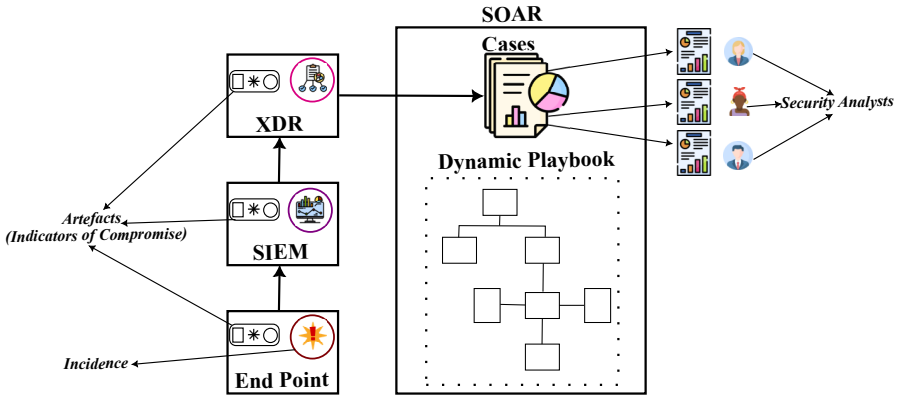


**Fig. 15** Incidence response ecosystem for city ferry social robot

#### *Extended Detection and Response (XDR)*

XDR expands upon traditional EDR systems by assimilating data across multiple security layers, including endpoints, networks, servers, and cloud services [155]. This enriched data perspective enables federated searches across diverse data points, enhancing visibility and threat detection accuracy. XDR's unified platform allows for automated threat detection using advanced analytics and machine learning, improving incident response capabilities. It integrates threat intelligence, streamlines incident

response with direct containment actions, and supports in-depth investigations for comprehensive incident impact understanding [156]. The integration and orchestration with other security tools foster efficient security workflows, and its cloud integration ensures that security monitoring encompasses both on-premises and cloud environments. XDR's ability to correlate data effectively reduces alert fatigue, focusing security teams on legitimate threats.

SIEM and XDR are critical components of the city ferry social robot's security architecture, offering layered security monitoring and detection capabilities [156]. These systems provide a security overview, automate threat detection, and enhance the organisation's incident response, ensuring robust defence against cybersecurity threats.

#### *Incidence Response*

Figure 15 illustrates an incident response ecosystem for the social robots system based on insights from endpoint security, SIEM and XDR. This system's core is a multi-tiered strategy identifying a security incident at the social robot endpoint. As potential threats are detected, they generate 'artefacts,' also known as Indicators of Compromise (IoCs) [157], which serve as early warnings of malicious activity. These IoCs are then escalated to the SIEM system, which aggregates and correlates the data to provide a view of the security event. The refined incident details are subsequently passed to the XDR system for an in-depth analysis, resulting in the creation of detailed 'cases' that contextualise the nature and potential impact of the incident [158].

Parallel to XDR's analytical process is the SOAR (Security, Orchestration, Automation and Response) platform, which receives these cases and applies a Dynamic Playbook (structured workflows with predefined actions) to automate the incident response, ensuring swift and precise mitigation efforts [159]. This automation is crucial for rapid containment and resolution of security incidents.

Running alongside the automated processes are human security analysts who receive the same cases from the XDR [155]. These experts bring their critical thinking and experience to bear on the incidents, providing nuanced analysis, decision-making, and, when necessary, manual intervention to complement the automated responses offered by the SOAR system.

This integrated approach, combining both automated and manual responses, encapsulates the incident response's complexity, ensuring that each security threat is met with both the rapidity of automation and the discernment of human expertise. This dual-layered response is critical to maintaining the robustness of the security posture for social robots within the dynamic public space of city ferries.

#### *Backups and Recovery*

Backups and disaster recovery are critical components of the social robot security framework, with backups as the safeguard for data preservation and disaster recovery, providing a strategic plan for business continuity in the aftermath of a crisis [160]. Regular data copies are created and stored in multiple, often off-site, locations to protect against loss or corruption due to various threats. The frequency and retention

of these backups and their type (full, incremental, or differential) form the backbone of a robust backup strategy [161].

On the other hand, disaster recovery is an expansive concept that includes data retrieval and the resumption of IT operations and services with minimal delay. Key to disaster recovery is establishing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), which set the maximum allowable downtime and data loss duration. This involves failover processes to secondary systems, regular DR testing to validate the plan's effectiveness, and a comprehensive approach to maintaining business operations during and after a disaster[160].

A well-documented Disaster Recovery Plan (DRP) outlines structured procedures for responding to unplanned events such as natural disasters, cyber-attacks, or hardware failures [162]. It encompasses a risk assessment to identify and prioritise threats, a communication plan for stakeholder engagement during a crisis, clearly defined roles and responsibilities, and detailed action steps for recovery. This plan also includes a complete inventory of IT assets, a backup and restoration strategy, provisions for an alternate operational site, and essential vendor contact information. Regular training and awareness programs ensure staff readiness, while continual testing and updates keep the DRP current and effective. Thus, a DRP is a dynamic and essential document within an organisation's broader risk management and IT strategies, ensuring operations' resilience and rapid recovery during a disaster.

## 7.5 Assessing Security Risks in the Social Robot System

The final step in the security design process for the social robot system involves an assessment of security risks [82]. This crucial phase ensures that the security infrastructure is effectively calibrated to balance potential risks against the costs of mitigation and the consequences of security breaches. By carefully evaluating each identified risk in relation to the designed security measures, this assessment determines whether the implemented security measures have achieved an acceptable balance between cost and risk.

The process begins by revisiting the threat model [100] to re-evaluate the likelihood and potential impact of each identified threat, considering the newly implemented security measures. Each risk is analyzed to ascertain its expected frequency of occurrence and the estimated severity of its impact should it materialize. This reassessment helps in understanding whether the security infrastructure sufficiently mitigates the risks or if further refinement is necessary.

Risk assessment [51] is typically documented in a tabular format, listing each risk alongside its likelihood, potential impact, and the notional cost, calculated as the product of impact and adjusted probability. This format helps stakeholders quickly identify and prioritize risks based on their notional cost, focusing on those with the highest potential for loss and likelihood of occurrence. We provided four potential attack scenarios in our previous work on the threat landscape and attack surface of social robots in public space [37].

Key activities in this phase include:

- **Risk Reevaluation:** For each risk, its likelihood and impact are reassessed in the context of the current security measures.
- **Cost/Risk Analysis:** Evaluate whether the potential costs of a risk occurring are acceptably mitigated by the proposed security measures.
- **Decision Making:** Determine if the current level of risk is acceptable. If not, the process may require looping back to refine the threat model and security implementations.

The goal is to ensure that the social robot operates within a security threshold that is both economically and operationally viable. This assessment not only confirms the adequacy of security measures but also underscores the need for ongoing security management to adapt to evolving threats and vulnerabilities.

# 8 IMPLEMENTING ARCHITECTURAL VIEWS IN A CITY FERRY SOCIAL ROBOT

This section introduces the practical application of various architectural frameworks to a service-oriented social robot operating in a city ferry context. We focus on the ARI robot [163], a humanoid designed by PAL Robotics in Spain, tailored for natural human-robot interactions. This use case is set within Fredrikstad Kommune, where the municipality owns the ARI robot, and the SecuRoPS team handles its software operations and security [85]. The robot is employed to inform, educate, and entertain tourists and local ferry users about events, cultural heritage, and activities happening within the municipality. This engagement not only promotes local businesses such as hotels, restaurants, museums, and libraries but also leverages the social robot's capabilities to enhance visitor experiences.

**Table 7** Technical Specifications of the ARI Social Robot System

| **Feature** | **Specifics** |
|---|---|
| Vision & Sensory Systems | RGB-D cameras, LIDAR, thermal sensors to interact and navigate. |
| Audio & Communication | 4X microphone array, 2X 30W speakers, wireless and Ethernet connectivity |
| Interactive Components | 2X LCD screen eyes, touchscreen, 4 DoF arm |
| Processing & Control Units | On-board PC (Intel i9, SSD 1TB, 32GB RAM), GPU Nvidia Xavier NX/Orin |
| Network Features | Wireless 802.11ax, Ethernet 1000 BaseT |
| Physical Interfaces | USB ports, HDMI, Audio In/Out, power buttons, Emergency Stop button |
| Power & Autonomy | 24V/60Ah battery providing 8-12 hours of autonomy |

The robot's technical specifications[10], ranging from sensory and connectivity features to its hardware configurations, play critical roles in realizing these architectural views. Table 7 summarizes the social robot's features, illustrating how each component contributes to the robot's functional and security profiles within this complex urban environment. These technical capabilities, managed by the SecuRoPS team,

[10]https://docs.pal-robotics.com/ari/sdk/23.1.11/hardware/hardware_overview.html

support the robot's integration into the city ferry environment, aligning with the architectural view strategies developed to enhance user interaction while maintaining security and operations. The role of external service providers like OpenAI[11] and Nvidia[12] in enhancing data processing capabilities also underscores the collaborative effort required to maintain and optimize such advanced service-oriented systems in dynamic public settings.

## 8.1 Business Context Architecture View

Figure 16 presents the business context architecture view tailored for the city ferry use case involving the ARI Social Robot. This representation highlights the interplay among various personas and systems within the municipality of Fredrikstad, showcasing how each entity interacts with the ARI Robot to fulfill distinct roles and leverage its services.

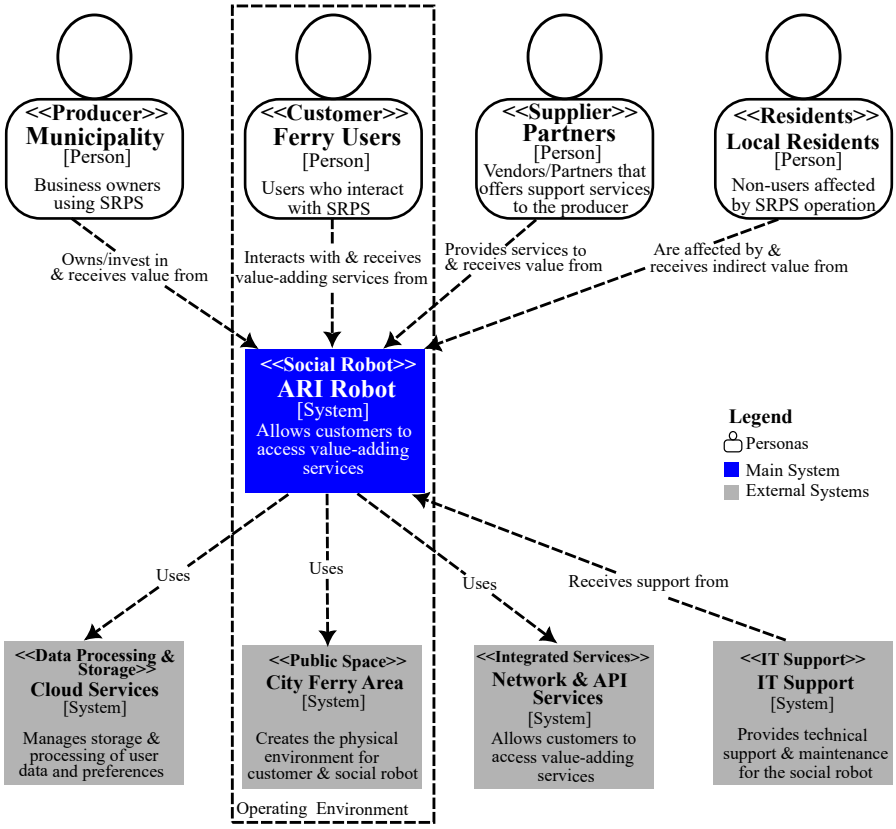


**Fig. 16** Business Context Architecture View of City Ferry Use Case

[11] https://openai.com/
[12] https://www.nvidia.com/en-us/

1. **Producer (Municipality):** The municipality, as the business owner, invests in and derives value from the ARI Robot, utilizing it to enhance public services and cultural engagement.
2. **Customers (Ferry Users):** Ferry users interact with the ARI Robot to receive informational, educational, and entertainment services during their ferry rides.
3. **Suppliers (Partners):** Various partners, including technology providers and local businesses, support the robot's functions and benefit through service provision and business referrals.
4. **Community Residents (Local Residents):** While not direct users of the robot, local residents are impacted by its operations and indirectly benefit from improved public services and insights generated by the robot's data.

Table 8 illustrates the correspondence between the original business context elements and their specific roles in the city ferry use case, providing a detailed description for each.

**Table 8** Mapping of Original Elements to Use Case Elements

| Elements | Use Case Elements | Description |
|---|---|---|
| Producer | Municipality | Owns the ARI Robot and integrates it into public services |
| Customer | Ferry Users | Users interacting directly with the robot for services |
| Supplier | Partners | Include technology providers and local businesses supporting the robot |
| Community Resident | Local Residents | Community members indirectly impacted by the robot's operations |
| Social Robot System | ARI Robot | Main system providing interactive services |
| Data Processing & Storage | Cloud Services | Handles extensive data processing and storage requirements |
| Public Space System | City Ferry Area | The operating environment for the robot on the ferry |
| Integrated Services | Network Infrastructure & API services | Manages integration and interaction with external services |
| IT Support | SecuRoPS Team | Provides technical support, security services and maintenance |

Table 9 outlines the business value propositions offered to each persona within the city ferry use case.

## 8.2 System Context Architecture View

In the system context architectural view, we delve deeper into the roles and interactions of each element within the city ferry use case as presented in Figure 16, utilizing the C4 model Container view (Level 2). This detailed examination is presented in the following subsections:

**Table 9** Business Value Propositions for City Ferry Use Case Personas

| Personas | Business Value Proposition |
|---|---|
| Municipality | Enhances public service delivery gains insights for city planning, increases cultural engagement |
| Ferry Users | Provides real-time information, education, and entertainment during ferry rides |
| Partners | Receives referrals, promotes their services/products through the robot, collaborates on technology |
| Local Residents | Benefits from enhanced city services and projects informed by data from the robot |

### 8.2.1 The Municipality (Producer)

Fredrikstad Municipality[13], serving as the producer, orchestrates several departments including Operations, Legal, and IT, similar to the structure detailed in Section 5.1.1. The Project Management Team acts as the primary interface between the municipality and external partners, channelling the concerns and requirements of internal stakeholders[58, 60]. Key concerns from the municipality include data security and privacy [65], compliance with GDPR and local data protection regulations, enhancing the social robot's ability to interact in Norwegian, and deriving tangible business value from the robot's operation in the city ferry area. Additionally, considerations are made for the physical security of the expensive robot assets [86] and incorporating local branding elements. The municipality provides critical resources such as network infrastructure, service data, and data storage facilities to support the project.

### 8.2.2 City Ferry Users (Customers)

This group includes city ferry users who interact with or are affected by the social robot. Users' needs, requirements, and concerns [60] were captured through two phases of research conducted by the SecuRoPS team, involving online surveys and in-depth interviews to capture users' experiences, trust levels, and data-sharing preferences. Initial findings highlighted a strong preference for travel assistance and local tourism information over functions easily performed by smartphones. Following this feedback, the project team focused on developing unique and complementary services for future deployment. Engagement strategies included media outreach through radio and TV, social media campaigns on platforms like LinkedIn and Instagram, and community events such as workshops and expos, to gather extensive user feedback and refine service offerings.

### 8.2.3 Partner (Suppliers)

The suppliers for the city ferry use case encompass a diverse group of entities, including Hardware Vendors, Software Vendors, Technology Suppliers like AI specialists, User Experience (UX) Designers [74], Public Space Managers/Administrators, Robot Operators, Third-party Service Providers, Insurance Companies, and Infrastructure & Facility Managers. These partners provide essential components ranging from physical

[13] https://www.fredrikstad.kommune.no/

hardware to software solutions, contributing significantly to the functionality, integration, and compliance of the social robot with existing standards. Their responsibilities extend to ongoing support, updates, integration with public space infrastructure, and maintaining stringent security and operational standards.

Key partners for this project include the SecuRoPS team, PAL Robotics, and various Municipality-owned entities like museums and libraries, alongside local businesses and external service providers like OpenAI and Nvidia [58]. The SecuRoPS team, led by the Institute for Energy Technology (IFE)[14], spearheads significant work packages focused on cybersecurity, robotics integration, and user experience design, collaborating with entities such as Høgskolen i Østfold (HIØ)[15] and SNØ Designstudio[16]. These teams are pivotal in refining the social robot's design to meet user preferences and ensure seamless integration into the public space.

Municipality-owned partners provide crucial support services and content from various cultural and administrative platforms. Local businesses engage with the social robot system to enhance visibility and attract tourists. External technology service providers like OpenAI and Nvidia enhance the robot's capabilities through advanced AI technologies and computing platforms. OpenAI enhances natural language processing and machine learning models, making the social robot more interactive and intelligent. Nvidia contributes with its robotics simulation tools and AI computing platforms, crucial for developing and testing the robot's functionalities in simulated environments. This partnership framework ensures the social robot is not only technologically advanced but also well-integrated within the community and capable of delivering meaningful interactions.

### 8.2.4 Local Residents (Community Residents)

In the city ferry use case, community residents encompass a diverse group of stakeholders who are affected by the presence of the ARI social robot within the public ferry spaces. This category includes Bystanders, Passers-by, Regulators, Privacy/Digital Rights Advocates, Ethicists and Social Scientists, Law Enforcement or Security Agencies, and the Media [58]. Each subgroup has distinct requirements and concerns regarding the social robot's presence and operations.

Key among these are the Regulators, specifically Sikt[17] – Norwegian Agency for Shared Services in Education and Research. This agency is responsible for approving all use cases and pilot studies before they commence, ensuring that the deployment and operation of the ARI social robot adhere to all applicable laws and regulations, including data protection laws such as GDPR and local Norwegian data protection guidelines. They scrutinize the robot's compliance with safety and privacy standards, ensuring that it operates within the legal framework designed to protect public interests.

The media[18] also plays a pivotal role in this setup. It acts as a critical conduit between the project and the public, shaping the perception of the social robot's utility

[14] https://ife.no/en/front-page/
[15] https://www.hiof.no/
[16] https://snodesignstudio.com/
[17] https://sikt.no/
[18] https://ife.no/menneskelignende-robot-testet-i-offentligheten/

and impact within the community. Through proactive media outreach involving radio and TV segments, and social media campaigns on platforms like LinkedIn and Instagram, the project garners visibility and engages with the community. These efforts are supplemented by direct community engagement strategies such as workshops, expos, and conferences, which provide platforms for firsthand interaction with the robot and feedback collection.

This approach ensures that the social robot not only serves its functional purpose of informing, educating, and entertaining ferry users but also respects and integrates into the social fabric of Fredrikstad Municipality, fostering a positive relationship with all community residents and aligning with societal values and norms.

### 8.2.5 ARI Robot (Social Robot System)

The ARI robot [163], a humanoid robot developed by PAL Robotics[19] in Spain, serves as the focal point of the city ferry use case within Fredrikstad Municipality. Designed for natural human-robot interactions, ARI engages with ferry users (tourists and locals alike) to inform, educate, and entertain them about local events, cultural heritage, and activities. This use case emphasizes the integration of the robot into the municipal landscape to enhance community engagement and support local businesses like hotels, restaurants, museums, and libraries.

In this context, ARI's subsystems[20] are tailored to operate efficiently in the dynamic environment of a city ferry. The robot is equipped with advanced sensors and actuators that enable it to interact effectively with its environment and users. These include RGB-D cameras for depth sensing and navigation, a multi-microphone array for clear audio reception, and robust actuators for physical interactions. The user interface module, featuring a touchscreen and animated LCD screen eyes, makes the robot approachable and interactive, facilitating user engagement directly.

The onboard processing and control unit, powered by high-performance components like an Intel i9 PC and Nvidia's Xavier NX or Orin GPUs, handles complex computations for real-time interaction and response. This unit ensures seamless integration of sensory inputs and user commands, coordinating all robotic actions and interactions. Network connectivity through advanced wireless and Ethernet interfaces enables ARI to connect with external data processing services provided by entities like OpenAI and Nvidia, enhancing its operational capabilities with AI-driven functionalities such as natural language processing and machine learning models.

Additionally, ARI's design includes an internal storage module to retain essential data and a robust power module to ensure prolonged autonomous operation, crucial for continuous service throughout its daily activities in public spaces.

Table 7, as referenced earlier, encapsulates these technical specifications, highlighting the sophisticated design and capabilities of the ARI robot that support the architectural views intended to enhance the user experience while ensuring operational security and functionality in the complex urban environment of the Fredrikstad Municipality's city ferry area.

---

[19] https://pal-robotics.com/
[20] https://docs.pal-robotics.com/ari/sdk/23.1.11/hardware/hardware_overview.html

### 8.2.6 City Ferry Area (Public Space System)

The City Ferry area, as a dynamic public space within Fredrikstad Kommune, presents unique challenges and opportunities for the deployment of the ARI robot [70]. This setting demands an understanding of the environmental, climatic, social, regulatory, and human interaction factors that influence the robot's functionality and integration into the community [164].

#### *Environmental Factors*

In the City Ferry area, the environmental factors include not only the physical layout and infrastructural elements such as docking stations, seating arrangements, and sheltered areas that facilitate user interaction with the robot but also the technological infrastructure necessary for robust network connectivity. These elements ensure that the robot can navigate and function effectively in this highly trafficked public space [165].

#### *Climatic Factors*

Given the open-air nature of the city ferry environment, the robot must be capable of operating under various weather conditions. This includes adaptations for rain, changes in temperature, and handling the salty sea air, all of which could potentially impact mechanical components and sensor functionality [166].

#### *Social and Regulatory Factors*

These play a critical role in the city ferry area, where the robot interacts with a diverse cross-section of the community. Regulatory compliance, particularly with Sikt (the Norwegian Agency for Shared Services in Education and Research), ensures all operational protocols meet strict standards before deployment. Additionally, the robot must adhere to societal norms and expectations, engaging users in a manner that respects local cultural and social values [167].

#### *Human Interaction Factors*

In the bustling environment of the city ferry area, human interaction factors are particularly salient. The robot is designed to handle interactions with a diverse public, managing disturbances such as noise from ferry operations and crowded conditions. Security considerations are paramount to protect the robot against potential vandalism or theft, especially in such an accessible public space [168].

In preparation for future deployments at event centres, similar considerations are being evaluated to ensure the ARI robot can adapt to different public settings effectively. This includes enhancing the robot's capabilities to manage larger crowds and more complex interaction scenarios, ensuring it remains a beneficial and secure feature in various public environments. The emphasis in these areas on human interaction and regulatory compliance highlights the adaptability and robustness required for the ARI robot to function optimally within the multifaceted public settings of Fredrikstad Municipality [48].

### 8.2.7 Cloud Services (Data Processing and Storage)

In the context of the city ferry use case, cloud services play a pivotal role in expanding the data processing and storage capabilities of the ARI robot beyond its onboard facilities [80]. The ARI robot, while equipped with an on-board PC featuring an Intel i9 processor, 1TB SSD, and 32GB RAM, is designed for basic data processing tasks and temporary data storage. For extensive data management and long-term storage needs, the system leverages external cloud services.

#### *Microsoft OneDrive*

OneDrive[21] is utilized for secure cloud storage, providing a reliable solution for storing large volumes of data generated from daily interactions and operational logs. This integration ensures data redundancy and enhances data accessibility for the SecuRoPS team, enabling efficient data management and backup solutions.

#### *PAL Robotics GitLab Platform*

Gitlab[22] serves as the central hub for code collaboration and version control. This platform facilitates seamless updates and maintenance of the robot's software, allowing multiple developers to collaborate in real time. During the preliminary testing phases, an institution-issued PC was also used for additional data and code storage, providing a flexible testing environment for rapid prototyping and adjustments.

The hybrid data management approach, combining robust onboard processing capabilities with cloud services, ensures the ARI robot can perform optimally in real-time while also benefiting from the expansive storage and advanced processing power of cloud solutions. This strategy not only enhances the robot's performance in delivering information and entertainment to ferry users but also supports complex data analysis tasks that feed into continuous improvements and service personalization for ferry users and residents within the municipality.

### 8.2.8 Network and API Services (Integrated Services)

In the city ferry use case, the ARI robot is equipped with state-of-the-art Network and API Services that are pivotal for its efficient operation within the dynamic public space of the ferry area [66]. These integrated services ensure that ARI can communicate seamlessly with both internal and external systems, providing real-time, contextually relevant information to users.

The ARI robot utilizes advanced wireless technology, specifically 802.11ax Wi-Fi, to maintain a robust and high-speed connection within the local network. For connections to the external internet, the robot employs VPN Cisco Anyconnect Secure Mobility[23], which ensures a secure and reliable link to online resources and external APIs. This setup is crucial for protecting data transfers, especially when handling sensitive information related to ferry users and local events.

API Services are central to the operational efficacy of the ARI robot, facilitating essential interactions with a multitude of external platforms and services. Through

[21] https://onedrive.live.com/login/
[22] https://about.gitlab.com/
[23] https://www.cisco.com/site/us/en/products/security/secure-client/index.html

these APIs, the robot accesses real-time data from local business databases, cultural event schedules, and municipal systems, allowing it to deliver a rich array of services such as navigation assistance, event notifications, and updates on local regulations. The integration extends to leveraging APIs from technology partners like OpenAI and Nvidia, enhancing the robot's artificial intelligence capabilities for improved user interactions and decision-making.

These Network and API Services not only empower the ARI robot to function as an informational conduit within the city ferry environment but also ensure it operates within a secure, controlled, and efficient network framework, enhancing both user experience and system reliability.

### 8.2.9 IT Support System

In the city ferry use case, the IT Support System plays a crucial role in ensuring that the ARI social robot operates smoothly and efficiently. This system provides technical support and maintenance, crucial for the ongoing functionality and security of the robot within the dynamic public space environment [67].

The IT Support System for ARI is managed by the SecuRoPS team, which includes IT professionals specialized in robotics, cybersecurity, and software maintenance [85]. This team is responsible for regular software updates, hardware checks, troubleshooting issues, and optimizing the robot's performance to handle the interactive demands of ferry users and the complexities of operating in a public space.

To facilitate these operations, the IT support infrastructure includes remote monitoring tools that allow for real-time diagnostics and intervention, reducing system downtimes and ensuring ARI is always ready to assist users [67]. The support system also includes disaster recovery plans and backup solutions to protect data and functionality in case of hardware failure or other disruptions.

Additionally, the IT Support System works closely with external partners such as PAL Robotics, OpenAI, and Nvidia to ensure that the latest software patches, security updates, and technological enhancements are integrated seamlessly into ARI's operational framework [69]. This collaboration ensures that the ARI robot not only meets the current technological standards but also adapts to new advancements and security protocols to provide reliable service to city ferry users and partners.

## 8.3 Functional Architecture View

In the city ferry use case, the ARI robot acts as the central functional unit within a complex system designed to serve ferry users with informational, educational, and entertainment services about local events, cultural heritage, and activities. This functional architecture view [22], depicted in Figure 17, illustrates how the ARI robot interacts with both users and various external systems to perform its tasks effectively.

At the core of this system is the ARI robot, equipped with sensors to perceive environmental and user inputs, and actuators to respond dynamically within the public space of the city ferry area. The user interface, consisting of touchscreens and microphones, allows ferry users to interact with the robot, asking for recommendations on hotels, restaurants, or city events. Depending on user preferences, which they

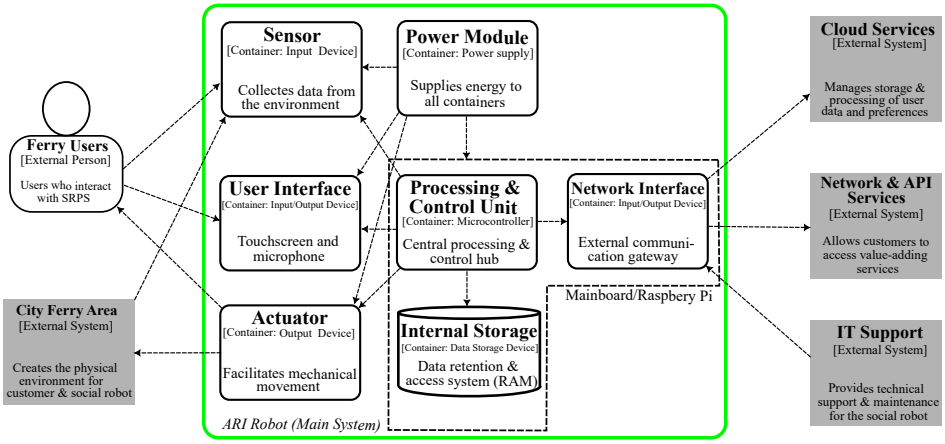


**Fig. 17** Functional Architecture View of City Ferry Use Case

can choose to save for future interactions, the robot offers personalized suggestions. This data can be stored securely in cloud services like Microsoft OneDrive or on local devices provided by the municipality or the SecuRoPS institution, ensuring user data privacy and transparency [169].

Network and API Services play a critical role in this architecture, facilitating robust communication links through Wi-Fi, with secure internet access provided via VPN (Cisco AnyConnect Secure Mobility) [170]. This setup ensures that the ARI robot can access external databases and services necessary for providing up-to-date information and services to users. IT support ensures continuous operational efficiency and security of the robot through regular updates and maintenance.

### 8.3.1 Handling Service Requests with the ARI Robot System

Service request handling by the ARI robot in the city ferry area involves a series of coordinated steps aimed at delivering personalized and responsive service to ferry users. The process begins when a user interacts with the robot's user interface. Advanced noise-cancellation technologies and responsive touchscreens ensure effective communication even in the bustling, noisy ferry environment.

1. **Service Request Initiation:** Ferry users interact with ARI using the touchscreen or voice commands, initiating service requests ranging from local information to entertainment options.
2. **Data Collection and Initial Processing:** ARI's sensors collect real-time environmental data, while the user interface captures user inputs. This data is processed by the ARI's central Processing & Control Unit, which adjusts the interaction dynamically based on current environmental conditions and user input.
3. **External Communication and Data Handling:** If the service request requires additional information, such as weather updates or external data, the Network Interface facilitates communication with Integrated Services (API) System or the Data Processing and Storage System to fetch necessary details.

4. **Response Formulation and Delivery:** Once the required information is retrieved and processed, the Processing & Control Unit formulates a response, which is then communicated back to the user through the User Interface.
5. **Actuation and User Feedback:** For requests requiring physical action, such as guiding the user to a specific location within the ferry area, ARI's actuators are engaged to perform the task. The user receives the requested service or information through visual displays or auditory outputs tailored to be effective despite ambient noise.
6. **Data Storage and Privacy:** Upon conclusion of the interaction, users are prompted to save their preferences for future visits. A transparent display of the information to be saved is shown, and upon user confirmation, data is securely stored as per the user's granularity preferences either in the cloud or on local devices.
7. **Additional Considerations:** Throughout the interaction, ARI adapts its functionalities to handle ongoing environmental variables like noise and crowd dynamics, ensuring optimal service delivery.

This structured approach in the functional architecture not only enhances the user experience but also ensures that each interaction with the ARI robot is secure, personalized, and contextually aware, aligning perfectly with the dynamic and interactive nature of the city ferry setting.

## 8.4 Security Perspective

The security architecture of the ARI social robot, operating within the city ferry environment of Fredrikstad Municipality, is designed based on the security perspective architectural view [82] depicted in Figure 12. This architecture adheres to the 5-step security activity methodology outlined by Nick Rozanski and Eoin Woods in Section 7, covering everything from identifying security-sensitive resources to assessing risks. This systematic approach ensures security measures are in place to protect the robot and its public interactions, aligning with established security practices to effectively mitigate potential threats.

### 8.4.1 Identifying Security-Sensitive Resources

In this step, the ARI robot's critical resources have been identified, which include its hardware components such as sensors and actuators, software systems including the operating system and applications, data both in transit and at rest, and the principals involved, particularly the users and system administrators [73]. This categorization helps in pinpointing what needs protection and forms the foundation for further security measures.

### 8.4.2 Defining the Security Policy

The security policy for the ARI robot is, specifying the protective measures and protocols necessary to shield the identified sensitive resources. It defines who (which principals) can access what resources under what conditions, emphasizing the need

for stringent access controls, data integrity, and confidentiality measures. This policy serves as the backbone of the security framework, ensuring that all operations align with the municipality's legal and regulatory standards [91].

### 8.4.3 Identifying Threats to the ARI Robot

Threat modeling has been conducted to understand the potential security challenges faced by the ARI robot in the city ferry context [96]. This involves analyzing threats from various sources including cyber-attacks, physical tampering, insider threats [98], and environmental hazards. Each identified threat is evaluated based on its likelihood and potential impact, with special consideration given to the unique public space setting of the city ferry.

### 8.4.4 Designing Security Implementations for the ARI Robot

With a clear understanding of the threats, a layered security strategy has been designed to mitigate these risks. This includes physical security measures to protect the robot's hardware [86], cybersecurity solutions such as firewalls and antivirus for network and endpoint protection, and advanced encryption methods for securing data communications. Additionally, robust authentication and access control mechanisms have been put in place to manage the interactions between the robot and users, as well as between the robot and other integrated systems. A brief summary of the security approaches for the city ferry use case is presented Table 10

**Table 10** Summary of Security Approaches for the City Ferry Use Case

| **Security Approach** | **Description** |
|---|---|
| Physical Security | Protects hardware from physical threats using locks and surveillance. |
| Endpoint Security | Guards against malware and monitors endpoints for suspicious activities. |
| Identity & Access Management | Manages user access through authentication & access controls. |
| Application Security | Secures software from exploits via audits and secure coding practices. |
| Network Security | Protects data in transit with VPNs and secure network connections. |
| Data Security | Ensures the integrity and confidentiality of stored data. |
| Cloud Security | Protects cloud-stored data with encryption and secure access controls. |
| Security Operations & Control | Manages overall security posture with SIEM systems and regular audits. |

#### *Security Approaches for the City Ferry Use Case*

In the city ferry use case involving the ARI robot, a set of security measures is deployed to protect against potential threats and ensure the integrity, availability, confidentiality and data privacy of the system. Each security approach is tailored to address specific aspects of the system's operation in the public environment:

1. **Physical Security:** Physical security measures are implemented to protect the ARI robot's hardware components from physical threats such as theft, vandalism,

and environmental damage. This includes securing the robot in a locked enclosure when not in use and employing surveillance systems within the ferry area to monitor and deter unauthorized physical interactions [86, 108].

2. **Endpoint Security:** Endpoint security is essential for protecting the ARI robot and associated devices from cyber threats such as malware and ransomware [101, 171]. For optimal protection in environments like the city ferry, we recommend subscribing to Crowdstrike Falcon Pro, tailored for small businesses. This solution provides next-generation antivirus capabilities and incorporates advanced threat intelligence, offering deeper insights into potential vulnerabilities. Its automated threat investigation features significantly speeds up the alert, triage, and response processes, enhancing the overall security posture and response efficiency.
3. **Identity and Access Management (IAM):** IAM systems ensure that only authorized users can access the ARI robot and its data. This involves the use of multi-factor authentication, role-based access controls, and continuous monitoring of access logs to prevent unauthorized access and detect potential security breaches [111].
4. **Application Security:** Application security is vital for protecting the software operating on the ARI robot against various cyber threats [85]. The primary application software, ROS 1, utilized by ARI is susceptible to a range of security vulnerabilities, including clear text communications, weak authentication procedures, unauthorized access, and source code manipulation by external nodes. Additionally, the inherent lack of robust security features in the ROS framework exposes it to risks of data tampering and denial-of-service attacks [172]. To mitigate these issues, we have implemented Secure ROS (SROS), which is specifically designed to bolster the security of ROS 1 environments by addressing these vulnerabilities [173]. Furthermore, additional application security measures are integrated through our endpoint security subscription package, which offers end-to-end security solutions with monitoring functionality, ensuring a comprehensive security approach that covers all aspects of application integrity and safety.
5. **Network Security:** Network security protocols are critical for protecting the transmission of data between the ARI robot and external systems, including cloud services and integrated APIs [170]. To enhance security measures, we utilize Cisco AnyConnect Secure Mobility for VPN services, which ensures secure and reliable connections. Additionally, the network is protected through secure Wi-Fi protocols and robust firewall configurations to prevent unauthorized access and maintain data integrity during its transit. Furthermore, our comprehensive security solution from Crowdstrike extends additional network security capabilities, integrating advanced threat detection and response mechanisms that fortify the network against potential cyber threats [171].
6. **Data Security:** Data security focuses on protecting the data collected and stored by the ARI robot, both on-device and within cloud storage solutions like Microsoft OneDrive. To safeguard this information, we employ robust encryption techniques, data anonymization practices, and regular backups to ensure data integrity and availability in case of system failure or security breaches [65]. Additionally, data security measures are complemented by other security strategies, including endpoint

security, application security, cloud security, and comprehensive security operations, each contributing layers of protection to secure data across all storage and processing points.

7. **Cloud Security:** Cloud security is vital for protecting all data hosted on cloud platforms such as OpenAI and Nvidia. It includes employing encrypted storage solutions, secure access credentials, and adherence to industry-standard security protocols to prevent unauthorized access and data leaks [174, 175]. Furthermore, additional layers of security are provided directly by cloud service providers, enhancing overall data protection through their own advanced security measures.
8. **Security Operations and Control:** Security operations entail the continuous monitoring and management of the security posture of the ARI robot system. This includes leveraging Security Information and Event Management (SIEM) systems [154] for the detection and response to security incidents, conducting regular security audits, and continuously updating the threat model and security measures in response to new and evolving threats. Additionally, our Crowdstrike Security package enhances these efforts by offering real-time monitoring and threat detection, further bolstering our security operations.

### 8.4.5 Assessing Security Risks for the ARI

The final step involves a thorough assessment of the residual risks after the proposed security measures are implemented. This risk assessment reviews the adequacy of the security infrastructure in mitigating identified risks and determines if the balance between risk severity and mitigation cost is acceptable [51]. If necessary, adjustments are made to enhance security measures or to refine the threat model and security policies, ensuring that the ARI robot operates securely within the highly interactive and exposed city ferry environment.

This security perspective that cuts across all architectural views, not only protects the ARI robot and its data but also ensures the safety and privacy of the ferry users interacting with the robot, thereby maintaining their trust and the integrity of the service provided.

# 9 DISCUSSION

This paper has articulated three primary architectural views (business context, system context, and functional) as well as an overarching security perspective, all tailored to the deployment of service-oriented social robots in public spaces like city ferries. Each view caters to specific stakeholders' needs, supporting the effective design, deployment, and security of these robots to ensure they operate efficiently and safely, providing significant value to all involved parties.

The **business context architecture** maps the interrelations and engagements among various stakeholders, such as customers, producers, suppliers, and community residents. This view lays out the foundational business model, clarifying each stakeholder's contributions and benefits. It is essential for grasping the strategic alignments and value propositions crucial for the robots' successful deployment.

The **system context architecture** penetrates deeper into the technical and operational interactions between the social robot and its environment. This includes interactions with both internal subsystems and external entities, detailing the technical roles of various producer departments and the robot's integration with other systems. This detailed scrutiny is vital for pinpointing technical prerequisites and maintaining the system's coherence and functional integrity.

The **functional view** sheds light on the operational capabilities of the social robot within its operational environment. It describes how the robot processes sensory inputs, interacts with users through its interfaces, and connects with external systems for additional data processing and cloud-based services. This view highlights the robot's roles in delivering information, facilitating user interaction, and managing data, underscoring its practical utility in public spaces.

Lastly, the **security perspective** addresses the critical need for robust protection measures across multiple layers—physical, endpoint, identity and access management, application, network, data, and cloud security. Each security layer tackles specific vulnerabilities, from safeguarding the robot's physical components to securing sensitive data flows, thus fortifying the system against a range of potential threats.

Together, these architectural views and security strategies illustrate an approach to managing the complexities of deploying service-oriented social robots in public settings, ensuring they deliver expected functionalities securely and efficiently.

## 9.1 Justification of Security Decisions

### Utilization of Established Security Approaches

Opting for Secure ROS (SROS) for application security reflects a preference for proven reliability and extensive community backing over novel, untested methods. SROS is recognized for its robust security features tailored to the ROS environment, offering clear advantages in terms of compatibility and community support. This choice mitigates potential risks associated with pioneering new security technologies and ensures that the social robot benefits from established best practices and resources.

### Incorporation of Professional Security Services

Integrating professional services like Crowdstrike Falcon Pro aligns with the strategy of outsourcing complex security management to experts. This approach extends beyond merely enhancing security measures—it shifts the responsibility of maintaining cutting-edge security defences to specialized providers. This is particularly vital for protecting data privacy and adhering to stringent regulatory standards, offering a layer of security that supplements internal efforts and safeguards against evolving cyber threats.

### Cost-Benefit Analysis of Security Investments

The decision to scale security investments based on actual threat levels addresses efficient resource allocation. Given the current low risk of targeted attacks against social

robots, extensive investment in high-end security solutions may not yield proportional benefits. However, the use of scalable and professional security services ensures readiness for potential threats at a justifiable cost, balancing preparedness with fiscal prudence.

## 9.2 Limitations

While the strategic security strategy presented in this work is robust, it presents several limitations:

1. **Adaptability to Emerging Threats:** Heavy reliance on established security protocols may slow adaptation to novel cyber threats. Security systems must remain flexible to swiftly address emerging vulnerabilities.
2. **Dependence on External Providers:** Outsourcing critical security operations creates dependencies that could introduce risks if service providers face disruptions.
3. **Privacy and Data Security Risks:** Despite external security measures, the ultimate responsibility for data privacy remains with the system operators, maintaining a residual risk of potential data breaches.

In the context of a city ferry, the practical implementation of these architectural views highlights real-world challenges and considerations. The paper illustrates how each architectural facet (from business justification to security) is not a standalone element but part of an integrated system that must function cohesively to ensure the successful operation of SRPS. It demonstrates that deploying social robots in public domains such as city ferries requires an approach, balancing business goals with technical feasibility and stringent security protocols.

This research contributes to the field by providing architectural views that can guide practitioners and researchers alike. It offers a foundational structure from which SRPS can be analysed, developed, and securely integrated into public spaces. It has a potential blueprint for similar applications in various public domains beyond city ferries. As SRPS continue to evolve, the frameworks presented here will require adaptation and refinement to keep pace with technological advancements and emerging security threats, ensuring that SRPS can deliver on their promise of enhancing public spaces in a secure and economically viable manner.

# 10 CONCLUSION

This paper tackled the complex challenge of integrating social robots into public spaces by elaborating on three distinct architectural views (business context, system context, and functional view) and a security perspective. These views and perspectives were designed to cater to the unique demands and interactions required for social robots operating within dynamic and often unpredictable public environments. The security perspective detailed eight interrelated security approaches: physical security, endpoint security, identity and access management (IAM), application security, network security, data security, cloud security, and security operations and control. These approaches are interrelated and sometimes challenging to separate, demonstrating the complexity of securing social robots in public spaces effectively. Applying these

frameworks in the context of a city ferry social robot showcases the practical considerations and the intricate planning required to bring SRPS to life. From ensuring robust business processes to maintaining security, the successful implementation of SRPS demands attention to detail and commitment.

Our investigation yielded several key findings. Firstly, the **business context architecture view** highlighted how social robots could significantly enhance service delivery and stakeholder engagement by acting as intermediaries in various public settings. The **system context architecture view** not only provided a detailed blueprint for the interactions between social robots and their operational ecosystems but also offered a detailed structure of each element within the system. This detailed structuring is invaluable for software architects in gathering requirements, addressing concerns, and assigning responsibilities to identified stakeholders, enhancing the overall design and implementation process. Additionally, the **functional view** delineated the operational capabilities and limitations of the social robots, emphasizing their practical applications within public environments. Finally, the **security perspective** developed herein underscored the critical need for comprehensive, interrelated security measures to protect both the robots and the data they handle from a variety of potential threats. These strategies emphasized the importance of incorporating security early in the design process of social robot software and applications, ensuring robust protection from the outset.

The implications of this research are profound, extending beyond mere academic interest to practical applications in urban planning, hospitality, and entertainment industries, among others. By outlining a structured approach to deploying social robots, this study contributes significantly to the ongoing discourse on smart city technologies and automation's role in enhancing public space utility and safety.

However, several avenues remain open for future research. The integration of advanced artificial intelligence in social robots, managing complex data privacy issues, and developing more resilient robotic systems that can adapt to diverse environmental conditions are critical areas that require further exploration. Future research should also refine the deployment and integration of SRPS, focusing on developing advanced business models to enhance economic and social value, establishing standards for interoperability, and designing user experiences that improve human-robot interaction. Additionally, longitudinal studies assessing the long-term impacts of social robots on public behaviour, space utilization, and community well-being would provide deeper insights into their effectiveness and societal acceptance. Further exploration in security to address emerging threats and ensure privacy and safety, as well as ethical and regulatory considerations to navigate the socio-economic implications of social robotics, is encouraged. Cross-disciplinary research is also suggested to develop comprehensive strategies that address the multifaceted needs of communities, contributing to the effective and ethical use of social robots in enhancing urban life and public services.

In conclusion, the architectural views and security strategies proposed in this paper are not just academic exercises; they are foundational components that will significantly influence the future landscapes of public spaces and robotics. As we stand on the brink of a new era in public service delivery and urban experience facilitated by advanced robotics, the findings of this study not only provide a roadmap for future

developments but also highlight the transformative potential of social robots in shaping the future of public interactions and services.

**Funding.** This research was funded by the Norwegian Research Council under the SecuRoPS project "User-centered Security Framework for Social Robots in Public Spaces" with project code 321324.

**Conflict of Interest/Competing Interest.** Vasileios Gkioulos, one of the authors of this paper, serves as a member of the editorial board for the journal to which this paper is being submitted. While every effort has been made to ensure the integrity and impartiality of the research presented in this paper, Vasileios Gkioulos acknowledges the potential for a conflict of interest due to his editorial role. All decisions regarding the review and publication process of this paper will be handled by other members of the editorial board to maintain objectivity and fairness.

# References

[1] Fortunati, L., Cavallo, F., Sarrica, M.: The Role of Social Robots in Public Space. In: Casiddu, N., Porfirione, C., Monteriù, A., Cavallo, F. (eds.) Ambient Assisted Living. Lecture Notes in Electrical Engineering, pp. 171–186. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-04672-9_11

[2] Mintrom, M., Sumartojo, S., Kulić, D., Tian, L., Carreno-Medrano, P., Allen, A.: Robots in public spaces: Implications for policy design **5**(2), 123–139 (2022) https://doi.org/10.1080/25741292.2021.1905342

[3] Woods, E., Rozanski, N.: The system context architectural viewpoint. In: 2009 Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture, pp. 333–336 (2009). https://doi.org/10.1109/WICSA.2009.5290673

[4] Kotusev, S., Kurnia, S., Dilnutt, R.: Enterprise architecture artifacts as boundary objects: An empirical analysis **155**, 107108 (2023) https://doi.org/10.1016/j.infsof.2022.107108

[5] Weilkiens, T., Lamm, G.J., Roth, S., Walker, M.: Model-Based System Architecture, pp. 1–603. John Wiley & Sons, Ltd, ??? (2022). https://doi.org/10.1002/9781119051930

[6] Ciambra, F., Nardini, M., Protano, A., Tocci, A.: Complex Systems Advanced Modelling **22**(1), 1829–1845 (2012) https://doi.org/10.1002/j.2334-5837.2012.tb01440.x

[7] Vishwakarma, L.P., Singh, R.K., Mishra, R., Demirkol, D., Daim, T.: The adoption of social robots in service operations: A comprehensive review **76**, 102441 (2024) https://doi.org/10.1016/j.techsoc.2023.102441

[8] Yang, J., Chew, E.: A Systematic Review for Service Humanoid Robotics Model in Hospitality **13**(6), 1397–1410 (2021) https://doi.org/10.1007/s12369-020-00724-y

[9] Song, B., Zhang, M., Wu, P.: Driven by technology or sociality? Use intention of service robots in hospitality from the human–robot interaction perspective **106**, 103278 (2022) https://doi.org/10.1016/j.ijhm.2022.103278

[10] Ivanov, S., Seyitoğlu, F., Markova, M.: Hotel managers' perceptions towards the use of robots: A mixed-methods approach **22**(4), 505–535 (2020) https://doi.org/10.1007/s40558-020-00187-x

[11] Čaić, M., Odekerken-Schröder, G., Mahr, D.: Service robots: Value co-creation and co-destruction in elderly care networks **29**(2), 178–205 (2018) https://doi.org/10.1108/JOSM-07-2017-0179

[12] Čaić, M., Mahr, D., Oderkerken-Schröder, G.: Value of social robots in services: Social cognition perspective **33**(4), 463–478 (2019) https://doi.org/10.1108/JSM-02-2018-0080

[13] Scianca, N., Ferrari, P., De Simone, D., Lanari, L., Oriolo, G.: A behavior-based framework for safe deployment of humanoid robots **45**(4), 435–456 (2021) https://doi.org/10.1007/s10514-021-09978-5

[14] Infantino, I., Augello, A., Maniscalto, U., Pilato, G., Vella, F.: A Cognitive Architecture for Social Robots. In: 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), pp. 1–5 (2018). https://doi.org/10.1109/RTSI.2018.8548520

[15] Heredia, J., Lopes-Silva, E., Cardinale, Y., Diaz-Amado, J., Dongo, I., Graterol, W., Aguilera, A.: Adaptive Multimodal Emotion Detection Architecture for Social Robots **10**, 20727–20744 (2022) https://doi.org/10.1109/ACCESS.2022.3149214

[16] Tanevska, A., Rea, F., Sandini, G., Cañamero, L., Sciutti, A.: A Socially Adaptable Framework for Human-Robot Interaction **7**, 121 (2020) https://doi.org/10.3389/frobt.2020.00121

[17] Foggia, P., Greco, A., Roberto, A., Saggese, A., Vento, M.: A Social Robot Architecture for Personalized Real-Time Human–Robot Interaction **10**(24), 22427–22439 (2023) https://doi.org/10.1109/JIOT.2023.3303196

[18] Botta, A., Rotbei, S., Zinno, S., Ventre, G.: Cyber security of robots: A comprehensive survey **18**, 200237 (2023) https://doi.org/10.1016/j.iswa.2023.200237

[19] Oruma, S.O., Ayele, Y.Z., Sechi, F., Rødsethol, H.: Security Aspects of Social

Robots in Public Spaces: A Systematic Mapping Study **23**(19), 8056 (2023) https://doi.org/10.3390/s23198056

[20] Kirca, Y.S., Degirmenci, E., Demirci, Z., Yazici, A., Ozkan, M., Ergun, S., Kanak, A.: Runtime Verification for Anomaly Detection of Robotic Systems Security **11**(2), 166 (2023) https://doi.org/10.3390/machines11020166

[21] Rozanski, N., Woods, E.: The Context Viewpoint. In: Software Systems Architecture: Working with Stakeholders Using Viewpoints and Perspectives, 2nd ed., 3rd print edn. Addison-Wesley, Upper Saddle River, NJ (2013)

[22] Rozanski, N., Woods, E.: The Functional Viewpoint. In: Software Systems Architecture: Working with Stakeholders Using Viewpoints and Perspectives, 2nd ed., 3rd print edn. Addison-Wesley, Upper Saddle River, NJ (2013)

[23] Indu, I., Anand, P.M.R., Bhaskar, V.: Identity and access management in cloud environment: Mechanisms and challenges **21**(4), 574–588 (2018) https://doi.org/10.1016/j.jestch.2018.05.010

[24] Kamruzzaman, A., Ismat, S., Brickley, J.C., Liu, A., Thakur, K.: A Comprehensive Review of Endpoint Security: Threats and Defenses. In: 2022 International Conference on Cyber Warfare and Security (ICCWS), pp. 1–7 (2022). https://doi.org/10.1109/ICCWS56285.2022.9998470

[25] Fuentes-García, M., Camacho, J., Maciá-Fernández, G.: Present and Future of Network Security Monitoring **9**, 112744–112760 (2021) https://doi.org/10.1109/ACCESS.2021.3067106

[26] Thuraisngham, B., Kantarcioglu, M., Khan, L.: Secure Data Science: Integrating Cyber Security and Data Science, 1st edn. CRC Press, Boca Raton (2022). https://doi.org/10.1201/9781003081845

[27] Oruma, S.O.: Towards a User-centred Security Framework for Social Robots in Public Spaces. In: Proceedings of the 27th International Conference on Evaluation and Assessment in Software Engineering. EASE '23, pp. 292–297. Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3593434.3593446

[28] Ding, B., Li, Y., Miah, S., Liu, W.: Customer acceptance of frontline social robots—Human-robot interaction as boundary condition **199**, 123035 (2024) https://doi.org/10.1016/j.techfore.2023.123035

[29] Nakanishi, J., Kuramoto, I., Baba, J., Ogawa, K., Yoshikawa, Y., Ishiguro, H.: Continuous Hospitality with Social Robots at a hotel **2**(3), 452 (2020) https://doi.org/10.1007/s42452-020-2192-7

[30] Liu, X., Ge, S.S., Zhao, F., Mei, X.: A dynamic behavior control framework

for physical human-robot interaction **101**(14) (2021) https://doi.org/10.1007/s10846-020-01286-x

[31] Asprino, L., Ciancarini, P., Nuzzolese, A.G., Presutti, V., Russo, A.: A reference architecture for social robots **72**, 100683 (2022) https://doi.org/10.1016/j.websem.2021.100683

[32] Martínez-Rojas, A., Sánchez-Oliva, J., López-Carnicer, J.M., Jiménez-Ramírez, A.: AIRPA: An Architecture to Support the Execution and Maintenance of AI-Powered RPA Robots. In: González Enríquez, J., Debois, S., Fettke, P., Plebani, P., Weerd, v.d. Inge, Weber, I. (eds.) Business Process Management: Blockchain and Robotic Process Automation Forum. Lecture Notes in Business Information Processing, pp. 38–48. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-85867-4_4

[33] Pramila, P.V., Amudha, S., Saravanan, T.R., Sankar, S.R., Poongothai, E., Boopathi, S.: Design and Development of Robots for Medical Assistance: An Architectural Approach. In: Contemporary Applications of Data Fusion for Advanced Healthcare Informatics, pp. 260–282. IGI Global, 701 East Chocolate Avenue, Hershey, PA 17033, USA (2023). https://doi.org/10.4018/978-1-6684-8913-0.ch011

[34] Stange, S., Hassan, T., Schröder, F., Konkol, J., Kopp, S.: Self-Explaining Social Robots: An Explainable Behavior Generation Architecture for Human-Robot Interaction **5** (2022). Accessed 2024

[35] Oruma, S.O., Petrovic, S.: Security Threats to 5G Networks for Social Robots in Public Spaces: A Survey **11**, 63205–63237 (2023) https://doi.org/10.1109/ACCESS.2023.3288338

[36] Yaacoub, J.-P.A., Noura, H.N., Salman, O., Chehab, A.: Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations **21**(1), 115–158 (2022) https://doi.org/10.1007/s10207-021-00545-8

[37] Oruma, S.O., Sánchez-Gordón, M., Colomo-Palacios, R., Gkioulos, V., Hansen, J.K.: A Systematic Review on Social Robots in Public Spaces: Threat Landscape and Attack Surface **11**(12), 181 (2022) https://doi.org/10.3390/computers11120181

[38] Hristozov, A.D., Matson, E.T., Gallagher, J.C., Rogers, M., Dietz, E.: Resilient Architecture Framework for Robotic Systems. In: 2022 International Conference Automatics and Informatics (ICAI), pp. 18–23 (2022). https://doi.org/10.1109/ICAI55857.2022.9960094

[39] Malavolta, I., Lewis, G., Schmerl, B., Lago, P., Garlan, D.: How do you architect your robots? state of the practice and guidelines for ROS-based systems. In: Proceedings of the ACM/IEEE 42nd International Conference on

Software Engineering: Software Engineering in Practice. ICSE-SEIP '20, pp. 31–40. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3377813.3381358

[40] Dieber, B., White, R., Taurer, S., Breiling, B., Caiazza, G., Christensen, H., Cortesi, A.: Penetration Testing ROS. In: Koubaa, A. (ed.) Robot Operating System (ROS) vol. 831, pp. 183–225. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-20190-6_8

[41] DeMarinis, N., Tellex, S., Kemerlis, V.P., Konidaris, G., Fonseca, R.: Scanning the Internet for ROS: A View of Security in Robotics Research. In: 2019 International Conference on Robotics and Automation (ICRA), pp. 8514–8521 (2019). https://doi.org/10.1109/ICRA.2019.8794451

[42] Afanasyev, I., Mazzara, M., Chakraborty, S., Zhuchkov, N., Maksatbek, A., Yesildirek, A., Kassab, M., Distefano, S.: Towards the Internet of Robotic Things: Analysis, Architecture, Components and Challenges. In: 2019 12th International Conference on Developments in eSystems Engineering (DeSE), pp. 3–8 (2019). https://doi.org/10.1109/DeSE.2019.00011

[43] Khalid, A., Kirisci, P., Khan, Z.H., Ghrairi, Z., Thoben, K.-D., Pannek, J.: Security framework for industrial collaborative robotic cyber-physical systems **97**, 132–145 (2018) https://doi.org/10.1016/j.compind.2018.02.009

[44] DiLuoffo, V., Michalson, W.R., Sunar, B.: Robot Operating System 2: The need for a holistic security approach to robotic architectures **15**(3), 1729881418770011 (2018) https://doi.org/10.1177/1729881418770011

[45] Batth, R.S., Nayyar, A., Nagpal, A.: Internet of Robotic Things: Driving Intelligent Robotics of Future - Concept, Architecture, Applications and Technologies. In: 2018 4th International Conference on Computing Sciences (ICCS), pp. 151–160 (2018). https://doi.org/10.1109/ICCS.2018.00033

[46] Lawrence, M.G., Williams, S., Nanz, P., Renn, O.: Characteristics, potentials, and challenges of transdisciplinary research. One Earth **5**(1), 44–61 (2022) https://doi.org/10.1016/j.oneear.2021.12.010

[47] The Research Council of Norway: User-Centred Security Framework for Social Robots in Public Space (SecuRoPS) - Prosjektbanken. https://prosjektbanken.forskningsradet.no/project/FORISS/321324 (2021)

[48] Carmona, M.: Public Places Urban Spaces: The Dimensions of Urban Design, Third edition edn. Routledge, Taylor & Francis Group, New York London (2021)

[49] Stallings, W., Brown, L.: Physical and Infrastructure Security. In: Computer Security: Principles and Practice, Fourth edition edn. Pearson, New York, NY (2018)

[50] Lindblom, J., Alenljung, B., Billing, E.: Evaluating the User Experience of Human–Robot Interaction. In: Jost, C., Le Pévédic, B., Belpaeme, T., Bethel, C., Chrysostomou, D., Crook, N., Grandgeorge, M., Mirnig, N. (eds.) Human-Robot Interaction: Evaluation Methods and Their Standardization. Springer Series on Bio- and Neurosystems, pp. 231–256. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-42307-0_9

[51] Reid, P.E.: Risk Assessment. In: Facility Manager's Guide to Security: Protecting Your Assets. River Publishers, New York (2005). https://doi.org/10.1201/9781003151067

[52] Rozanski, N., Woods, E.: Software Systems Architecture: Working with Stakeholders Using Viewpoints and Perspectives, 2nd ed., 3rd print edn. Addison-Wesley, Upper Saddle River, NJ (2013)

[53] Brown, S.: The C4 Model for Visualising Software Architecture. Lean Publishing, Ruboss Technology Corporation 1321 Blanshard Street, Suite 301 Victoria, British Columbia, Canada V8W 0B6 (2022)

[54] Gonzalez-Lopez, F., Bustos, G.: Business process architecture design methodologies – a literature review **25**(6), 1317–1334 (2019) https://doi.org/10.1108/BPMJ-09-2017-0258

[55] Marklund, M.L. Johan: Introduction to Business Process Design. In: Business Process Modeling, Simulation And Design, 3rd edn. Chapman and Hall/CRC, New York (2018). https://doi.org/10.1201/9781315162119

[56] OMG: Unified Modeling Language, v2.5.1 (2017)

[57] Burdett, J.O.: A Model for Customer-Supplier Alliances **29**(5) (1991) https://doi.org/10.1108/00251749110136136

[58] Rozanski, N., Woods, E.: Identifying and Engaging Stakeholders. In: Software Systems Architecture: Working with Stakeholders Using Viewpoints and Perspectives, 2nd ed., 3rd print edn. Addison-Wesley, Upper Saddle River, NJ (2013)

[59] König, M., Bein, L., Nikaj, A., Weske, M.: Integrating Robotic Process Automation into Business Process Management. In: Asatiani, A., García, J.M., Helander, N., Jiménez-Ramírez, A., Koschmider, A., Mendling, J., Meroni, G., Reijers, H.A. (eds.) Business Process Management: Blockchain and Robotic Process Automation Forum vol. 393, pp. 132–146. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-58779-6_9

[60] Rozanski, N., Woods, E.: Concerns, Principles and Decisions. In: Software Systems Architecture: Working with Stakeholders Using Viewpoints and Perspectives, 2nd ed., 3rd print edn. Addison-Wesley, Upper Saddle River, NJ

(2013)

[61] Radley-Gardner, O., Beale, H., Zimmermann, R. (eds.): General Data Protection Regulation (GDPR), p. 88. Hart Publishing, Kemp House, Chawley Park, Cumnor Hill, Oxford, OX2 9PH, United Kingdom (2016). https://doi.org/10.5040/9781782258674

[62] Marchang, J., Di Nuovo, A.: Assistive multimodal robotic system (AMRSys): Security and privacy issues, challenges, and possible solutions. APPLIED SCIENCES-BASEL **12**(2174) (2022) https://doi.org/10.3390/app12042174

[63] Matthews, P., Greenspan, S.: Robots in Society. In: Matthews, P., Greenspan, S. (eds.) Automation and Collaborative Robotics: A Guide to the Future of Work, pp. 211–248. Apress, Berkeley, CA (2020). https://doi.org/10.1007/978-1-4842-5964-1_7

[64] Belanche, D., Casaló, L.V., Flavián, C., Schepers, J.: Service robot implementation: A theoretical framework and research agenda. The Service Industries Journal **40**(3-4), 203–225 (2020) https://doi.org/10.1080/02642069.2019.1672666

[65] Thuraisngham, B., Kantarcioglu, M., Khan, L.: Data Security and Privacy. In: Secure Data Science: Integrating Cyber Security and Data Science, 1st edn., pp. 15–28. CRC Press, Boca Raton (2022). https://doi.org/10.1201/9781003081845

[66] Lamothe, M., Guéhéneuc, Y.-G., Shang, W.: A Systematic Review of API Evolution Literature. ACM Comput. Surv. **54**(8), 171–117136 (2021) https://doi.org/10.1145/3470133

[67] McQuate, C.: Security Officers and Equipment Monitoring. In: Fennelly, L.J. (ed.) Effective Physical Security, Fifth edition edn., pp. 343–346. Elsevier, Cambridge, MA (2017)

[68] Garg, R.K., Garg, R.: Decision Support System for Evaluation and Ranking of Robots Using Hybrid Approach. IEEE Transactions on Engineering Management **70**(9), 3283–3296 (2023) https://doi.org/10.1109/TEM.2021.3079704

[69] Stallings, W., Brown, L.: IT Security Control, Plans and Procedures. In: Computer Security: Principles and Practice, Fourth edition edn. Pearson, New York, NY (2018)

[70] Altman, I., Zube, E.H.: Public Places and Spaces. Springer, New York (2012)

[71] Brandão, A., Brandão, P.: Public Space, Infrastructure, Landscape: An Interdisciplinary Matrix for Urban Spatial Continuity. In: Public Space Reader. Routledge, New York (2021)

[72] Hosseini, M., Shabani, M.: New approach to customer segmentation based on changes in customer value. Journal of Marketing Analytics **3**(3), 110–121 (2015) https://doi.org/10.1057/jma.2015.10

[73] Reid, P.E.: Facility Manager's Guide to Security: Protecting Your Assets. River Publishers, New York (2005). https://doi.org/10.1201/9781003151067

[74] de Saille, S., Kipnis, E., Potter, S., Cameron, D., Webb, C.J.R., Winter, P., O'Neill, P., Gold, R., Halliwell, K., Alboul, L., Bell, A.J., Stratton, A., McNamara, J.: Improving Inclusivity in Robotics Design: An Exploration of Methods for Upstream Co-Creation. Frontiers in Robotics and AI **9** (2022)

[75] Dotson, C.: Practical Cloud Security. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, USA (2019)

[76] Bertolini, A., Salvini, P., Pagliai, T., Morachioli, A., Acerbi, G., Trieste, L., Cavallo, F., Turchetti, G., Dario, P.: On Robots and Insurance. International Journal of Social Robotics **8**(3), 381–391 (2016) https://doi.org/10.1007/s12369-016-0345-z

[77] Wilson, C.: Public engagement and AI: A values analysis of national strategies. Government Information Quarterly **39**(1), 101652 (2022) https://doi.org/10.1016/j.giq.2021.101652

[78] Choi, J.: Range Sensors: Ultrasonic Sensors, Kinect, and LiDAR. In: Goswami, A., Vadakkepat, P. (eds.) Humanoid Robotics: A Reference, pp. 2521–2538. Springer, Dordrecht (2019). https://doi.org/10.1007/978-94-007-6046-2_108

[79] Dario, P., Laschi, C., Guglielmelli, E.: Sensors and actuators for 'humanoid' robots. Advanced Robotics **11**(6), 567–584 (1996) https://doi.org/10.1163/156855397X00083

[80] Zhang, Z., Nan, G., Tan, Y.: Cloud Services vs. On-Premises Software: Competition Under Security Risk and Product Customization **31**(3), 848–864 (2020) https://doi.org/10.1287/isre.2019.0919

[81] Elfaki, A.O., Abduljabbar, M., Ali, L., Alnajjar, F., Mehiar, D., Marei, A.M., Alhmiedat, T., Al-Jumaily, A.: Revolutionizing Social Robotics: A Cloud-Based Framework for Enhancing the Intelligence and Autonomy of Social Robots. Robotics **12**(2), 48 (2023) https://doi.org/10.3390/robotics12020048

[82] Rozanski, N., Woods, E.: The Security Perspective. In: Software Systems Architecture: Working with Stakeholders Using Viewpoints and Perspectives, 2nd ed., 3rd print edn. Addison-Wesley, Upper Saddle River, NJ (2013)

[83] Paananen, H., Lapke, M., Siponen, M.: State of the art in information security policy development. Computers & Security **88**, 101608 (2020) https://doi.org/

10.1016/j.cose.2019.101608

[84] Stallings, W., Brown, L.: Human Resources Security. In: Computer Security: Principles and Practice, Fourth edition edn. Pearson, New York, NY (2018)

[85] Stallings, W., Brown, L.: Software Security. In: Computer Security: Principles and Practice, Fourth edition edn., pp. 379–418. Pearson, New York, NY (2018)

[86] Reid, P.E.: Access Hardware; Mechanical Locks, Latches, Keys. In: Facility Manager's Guide to Security: Protecting Your Assets. River Publishers, New York (2005). https://doi.org/10.1201/9781003151067

[87] Srinivas, J., Das, A.K., Kumar, N.: Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems **92**, 178–188 (2019) https://doi.org/10.1016/j.future.2018.09.063

[88] Landoll, d.J.: Information Security Policies, Procedures, and Standards: A Practitioner's Reference. CRC Press, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742 (2016)

[89] Landoll, d.J.: Information Security Policy Framework. In: Information Security Policies, Procedures, and Standards: A Practitioner's Reference. CRC Press, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742 (2016)

[90] Landoll, d.J.: Information Security Policy Basics. In: Information Security Policies, Procedures, and Standards: A Practitioner's Reference. CRC Press, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742 (2016)

[91] Landoll, d.J.: Information Security Policy Details. In: Information Security Policies, Procedures, and Standards: A Practitioner's Reference. CRC Press, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742 (2016)

[92] Stallings, W., Brown, L.: Access Control. In: Computer Security: Principles and Practice, Fourth edition edn., pp. 127–168. Pearson, New York, NY (2018)

[93] Deogun, D., Johnsson, D.B., Sawano, D.: Ensuring Integrity of State. In: Secure by Design. Manning Publications, Shelter Island (2019)

[94] Mellado, D., Blanco, C., Sánchez, L.E., Fernández-Medina, E.: A systematic review of security requirements engineering. Computer Standards & Interfaces **32**(4), 153–165 (2010) https://doi.org/10.1016/j.csi.2010.01.006

[95] Yu, Z., Wang, J., Tang, B., Lu, L.: Tactics And Techniques Classification In Cyber Threat Intelligence. The Computer Journal, 048 (2022) https://doi.org/

10.1093/comjnl/bxac048

[96] Reid, P.E.: Threats to Facilities. In: Facility Manager's Guide to Security: Protecting Your Assets. River Publishers, New York (2005). https://doi.org/10.1201/9781003151067

[97] Tsiostas, D., Kittes, G., Chouliaras, N., Kantzavelou, I., Maglaras, L., Douligeris, C., Vlachos, V.: The Insider Threat: Reasons, Effects and Mitigation Techniques. In: 24th Pan-Hellenic Conference on Informatics. PCI 2020, pp. 340–345. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3437120.3437336

[98] Thuraisngham, B., Kantarcioglu, M., Khan, L.: Stream Analytics for Insider Threat Detection. In: Secure Data Science: Integrating Cyber Security and Data Science, 1st edn., pp. 145–168. CRC Press, Boca Raton (2022). https://doi.org/10.1201/9781003081845

[99] ENISA: Threat Landscape for Supply Chain Attacks. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (2021)

[100] Xiong, W., Lagerström, R.: Threat modeling – A systematic literature review. Computers & Security **84**, 53–69 (2019) https://doi.org/10.1016/j.cose.2019.03.010

[101] Kadrich, M.: Endpoint Security, p. 377. Addison-Wesley Professional, 75 Arlington Street, Suite 300 Boston, MA 02116 (2007)

[102] Dotson, C.: Identity and Access Management. In: Practical Cloud Security. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, USA (2019)

[103] Garcia, M.L.: Introduction to Vulnerability Assessment. In: Fennelly, L.J. (ed.) Effective Physical Security, Fifth edition edn., pp. 23–44. Elsevier, Cambridge, MA (2017)

[104] Bell, L., Brunton-Spall, M., Smith, R., Bird, J.: Agile Application Security. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, USA (2017)

[105] Bejtlich, R.: The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, Inc., 38 Ringold Street, San Francisco, CA 94103 (2013)

[106] Soleimanzadeh, H., Rolfe, B., Bodaghi, M., Jamalabadi, M., Zhang, X., Zolfagharian, A.: Sustainable Robots 4D Printing **7**(12), 2300289 (2023) https://doi.org/10.1002/adsu.202300289

[107] Black, I.S.: Alarms Intrusion Detection System. In: Fennelly, L.J. (ed.) Effective Physical Security, Fifth edition edn., pp. 391–400. Elsevier, Cambridge, MA (2017)

[108] Reid, P.E.: Physical Separation: Fences, Barriers, Gates, Distance, Lighting. In: Facility Manager's Guide to Security: Protecting Your Assets. River Publishers, New York (2005). https://doi.org/10.1201/9781003151067

[109] Aymerich-Franch, L., Ferrer, I.: Social robots as a brand strategy. In: Innovation in Advertising and Branding Communication, pp. 86–102. Routledge, New York (2020)

[110] Kumari, M., Kumar, A., Singhal, R.: Design and Analysis of IoT-Based Intelligent Robot for Real-Time Monitoring and Control. In: 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and Its Control (PARC), pp. 549–552 (2020). https://doi.org/10.1109/PARC49193.2020.236673

[111] Haber, M.J., Rolls, D.: The Five As of Enterprise IAM. In: Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution. Apress, Berkeley, CA (2020). https://doi.org/10.1007/978-1-4842-5165-2

[112] ISO/IEC: Information Technology — Security Techniques — A Framework for Identity Management — Part 2: Reference Architecture and Requirements, Case postale 56, CH-1211 Geneva 20 (2015). https://www.iso.org/standard/57915.html

[113] Bertino, E., Takahashi, K.: Identity Management: Concepts, Technologies, and Systems. Artech House Information Security and Privacy Series, p. 196. Artech House, Boston, Mass. (2011)

[114] Mohammad, Z.N., Farha, F., Abuassba, A.O.M., Yang, S., Zhou, F.: Access control and authorization in smart homes: A survey **26**(6), 906–917 (2021) https://doi.org/10.26599/TST.2021.9010001

[115] Garbis, J., Chapman, J.W.: Privileged Access Management. In: Garbis, J., Chapman, J.W. (eds.) Zero Trust Security: An Enterprise Guide, pp. 155–161. Apress, Berkeley, CA (2021). https://doi.org/10.1007/978-1-4842-6702-8_12

[116] Podugu, S., Rayapureddi, V.K., Gupta, M.: Auditing Customer Identity and Access Management. In: Modernizing Enterprise IT Audit Governance and Management Practices, pp. 181–210. IGI Global, 701 East Chocolate Avenue, Hershey, PA 17033, USA (2023). https://doi.org/10.4018/978-1-6684-8766-2.ch007

[117] Hardjono, T.: Federated Authorization over Access to Personal Data for Decentralized Identity Management **3**(4), 32–38 (2019) https://doi.org/10.1109/

MCOMSTD.001.1900019

[118] Balapour, A., Nikkhah, H.R., Sabherwal, R.: Mobile application security: Role of perceived privacy as the predictor of security perceptions **52**, 102063 (2020) https://doi.org/10.1016/j.ijinfomgt.2019.102063

[119] Meng, N., Nagy, S., Yao, D.D., Zhuang, W., Argoty, G.A.: Secure coding practices in Java: Challenges and vulnerabilities. In: Proceedings of the 40th International Conference on Software Engineering. ICSE '18, pp. 372–383. Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3180155.3180201

[120] Marchand-Melsom, A., Nguyen Mai, D.B.: Automatic repair of OWASP Top 10 security vulnerabilities: A survey. In: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops. ICSEW'20, pp. 23–30. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3387940.3392200

[121] Stoddard, J.T., Cutshaw, M.A., Williams, T., Friedman, A., Murphy, J.: Software Bill of Materials (SBOM) Sharing Lifecycle Report (2023). https://doi.org/10.2172/1969133

[122] Felderer, M., Büchler, M., Johns, M., Brucker, A.D., Breu, R., Pretschner, A.: Chapter One - Security Testing: A Survey. In: Memon, A. (ed.) Advances in Computers vol. 101, pp. 1–51. Elsevier, 230 Park Avenue, 7th Floor, New York, NY 10169, USA (2016). https://doi.org/10.1016/bs.adcom.2015.11.003

[123] Yang, J., Tan, L., Peyton, J., A Duer, K.: Towards Better Utilizing Static Application Security Testing. In: 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering In Practice (ICSE-SEIP), pp. 51–60 (2019). https://doi.org/10.1109/ICSE-SEIP.2019.00014

[124] Millar, S., Podgurskii, D., Kuykendall, D., Rincón, J., Miller, P.: Optimising Vulnerability Triage in DAST with Deep Learning. In: Proceedings of the 15th ACM Workshop on Artificial Intelligence And Security. AISec'22, pp. 137–147. Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3560830.3563724

[125] Pan, Y.: Interactive Application Security Testing. In: 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA), pp. 558–561 (2019). https://doi.org/10.1109/ICSGEA.2019.00131

[126] Le-Thanh, P., Le-Anh, T., Le-Trung, Q.: Research and Development of a Smart Solution for Runtime Web Application Self-Protection. In: Proceedings of the 12th International Symposium on Information and Communication Technology. SOICT '23, pp. 304–311. Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3628797.3628901

[127] Wang, W., Dumont, F., Niu, N., Horton, G.: Detecting Software Security Vulnerabilities Via Requirements Dependency Analysis **48**(5), 1665–1675 (2022) https://doi.org/10.1109/TSE.2020.3030745

[128] Dissanayake, N., Jayatilaka, A., Zahedi, M., Babar, M.A.: Software security patch management - A systematic literature review of challenges, approaches, tools and practices **144**, 106771 (2022) https://doi.org/10.1016/j.infsof.2021.106771

[129] Mayoral-Vilches, V., García-Maestro, N., Towers, M., Gil-Uriarte, E.: DevSecOps in Robotics. arXiv (2021). https://doi.org/10.48550/arXiv.2003.10402

[130] Howard, M., Lipner, S.: Security Development Lifecycle. Microsoft Secure Software Development Series. Microsoft Press, One Microsoft Way, Redmond, WA 98052-6399, USA (2006)

[131] SAMM, O.: OWASP SAMM: The Model. https://owaspsamm.org/model/ (2023)

[132] Souppaya, M., Scarfone, K., Dodson, D.: Secure Software Development Framework (SSDF) Version 1.1 :: Recommendations for Mitigating the Risk of Software Vulnerabilities, Gaithersburg, MD (2022). https://doi.org/10.6028/NIST.SP.800-218

[133] McGraw, G.: Software Security: Building Security In. In: 2006 17th International Symposium on Software Reliability Engineering, pp. 6–6 (2006). https://doi.org/10.1109/ISSRE.2006.43

[134] McGraw, G.: Software security and the building security in maturity model (BSIMM). Journal of Computing Sciences in Colleges **30**(3), 7–8 (2015)

[135] SAFECode: Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Lifecycle Program (2018)

[136] Liang, J., Kim, Y.: Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall. In: 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0752–0759 (2022). https://doi.org/10.1109/CCWC54503.2022.9720435

[137] Ioannidis, S., Keromytis, A.D., Bellovin, S.M., Smith, J.M.: Implementing a distributed firewall. In: Proceedings of the 7th ACM Conference on Computer and Communications Security, pp. 190–199. ACM, Athens Greece (2000). https://doi.org/10.1145/352600.353052

[138] Kizza, J.M.: System Intrusion Detection and Prevention. In: Kizza, J.M. (ed.) Guide to Computer Network Security. Texts in Computer Science, pp. 295–323. Springer International Publishing, Cham (2024). https://doi.org/10.1007/

978-3-031-47549-8_13

[139] Ezra, P.J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., Damasevicius, R.: Secured Communication Using Virtual Private Network (VPN). In: Khanna, K., Estrela, V.V., Rodrigues, J.J.P.C. (eds.) Cyber Security and Digital Forensics. Lecture Notes on Data Engineering and Communications Technologies, pp. 309–319. Springer, Singapore (2022). https://doi.org/10.1007/978-981-16-3961-6_27

[140] Khan, A., Tahir, S., Khan, F., Tahir, H., Zulkifl, Z.: Enhancing Security of Cloud-based IoT Systems through Network Access Control (NAC). In: 2021 International Conference on Communication Technologies (ComTech), pp. 103–108 (2021). https://doi.org/10.1109/ComTech52583.2021.9616855

[141] Sharma, B., Pokharel, P., Joshi, B.: User Behavior Analytics for Anomaly Detection Using LSTM Autoencoder - Insider Threat Detection. In: Proceedings of the 11th International Conference on Advances in Information Technology. IAIT '20, pp. 1–9. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3406601.3406610

[142] Lamers, E., Dijksman, R., Vegt, p.d. Arjan, Sarode, M., Laat, d. Cees: Securing Home Wi-Fi with WPA3 Personal. In: 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), pp. 1–8 (2021). https://doi.org/10.1109/CCNC49032.2021.9369629

[143] Daubner, L., Považanec, A.: Data Loss Prevention Solution for Linux Endpoint Devices. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. ARES '23, pp. 1–10. Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3600160.3605036

[144] Benfeldt, O., Persson, J.S., Madsen, S.: Data Governance as a Collective Action Problem **22**(2), 299–313 (2020) https://doi.org/10.1007/s10796-019-09923-z

[145] Staheli, D., Mancuso, V., Harnasch, R., Fulcher, C., Chmielinski, M., Kearns, A., Kelly, S., Vuksani, E.: Collaborative Data Analysis and Discovery for Cyber Security. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) (2016). https://www.usenix.org/conference/soups2016/workshop-program/wsiw16/presentation/staheli Accessed 2024

[146] Carey, P., Carey, P.: Data Protection: A Practical Guide to UK and EU Law, Fifth edition edn., p. 369. Oxford University Press, Oxford, United Kingdom (2018)

[147] Horstmann, B., Diekmann, N., Buschmeier, H., Hassan, T.: Towards Designing Privacy-Compliant Social Robots for Use in Private Households: A Use

Case Based Identification of Privacy Implications and Potential Technical Measures for Mitigation. In: 2020 29th IEEE International Conference on Robot and Human Interactive Communication (RO-MAN), pp. 869–876 (2020). https://doi.org/10.1109/RO-MAN47096.2020.9223556

[148] Huda, S., Alinka: Next Level Cybersecurity: Detect the Signals, Stop the Hack. Leaders Press, VIA TRENTO E TRIESTE 49, 19015 - Levanto, Italy (2019)

[149] Gerard, J.: Digital Forensics and Incident Response, Third edition edn. Packt, Livery Place, 35 Livery Street, Birmingham, B3 2PB, United Kingdom (2022)

[150] Kayes, A.S.M., Rahayu, W., Watters, P., Alazab, M., Dillon, T., Chang, E.: Achieving security scalability and flexibility using Fog-Based Context-Aware Access Control **107**, 307–323 (2020) https://doi.org/10.1016/j.future.2020.02.001

[151] Demissie, B.F., Ranise, S.: Assessing the Effectiveness of the Shared Responsibility Model for Cloud Databases: The Case of Google's Firebase. In: 2021 IEEE International Conference on Smart Data Services (SMDS), pp. 121–131 (2021). https://doi.org/10.1109/SMDS53860.2021.00026

[152] Souppaya, M., Scarfone, K.: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology (2021). https://doi.org/10.6028/NIST.SP.800-40r4-draft

[153] Muniz, J.: The Modern Security Operations Center: The People, Processes and Technology for Operating SOC Services, 1st edn. Pearson Education, Inc, Hoboken (2021)

[154] González-Granadillo, G., González-Zarzosa, S., Diaz, R.: Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures **21**(14), 4759 (2021) https://doi.org/10.3390/s21144759

[155] Sullivan, J.: Extended Detection and Response (XDR) For Dummies, Cisco Special Edition, Cisco special edition edn. John Wiley & Sons, Inc, 111 River St. Hoboken, NJ 07030-5774 (2022)

[156] George, A.S., Sagayarajan, S., Baskar, D.T., George, A.S.H.: Extending Detection and Response: How MXDR Evolves Cybersecurity **1**(4), 268–285 (2023) https://doi.org/10.5281/zenodo.8284342

[157] Haber, M.J., Rolls, D.: Indicators of Compromise. In: Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution. Apress, Berkeley, CA (2020). https://doi.org/10.1007/978-1-4842-5165-2

[158] Stevens, R., Votipka, D., Dykstra, J., Tomlinson, F., Quartararo, E., Ahern, C., Mazurek, M.L.: How Ready is Your Ready? Assessing the Usability of Incident

Response Playbook Frameworks. In: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. CHI '22, pp. 1–18. Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3491102.3517559

[159] Bartwal, U., Mukhopadhyay, S., Negi, R., Shukla, S.: Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots. In: 2022 IEEE Conference on Dependable and Secure Computing (DSC), pp. 1–8 (2022). https://doi.org/10.1109/DSC54232.2022.9888808

[160] Mendonça, J., Andrade, E., Endo, P.T., Lima, R.: Disaster recovery solutions for IT systems: A Systematic mapping study **149**, 511–530 (2019) https://doi.org/10.1016/j.jss.2018.12.023

[161] Brennan, S.: Making Data Sustainable: Backup Culture and Risk Perception. In: Sustainable Media, p. 21. Routledge, New York (2016)

[162] Sawalha, I.H.: Views on business continuity and disaster recovery **10**(3), 351–365 (2021) https://doi.org/10.1108/IJES-12-2020-0074

[163] Cooper, S., Di Fava, A., Vivas, C., Marchionni, L., Ferro, F.: ARI: The Social Assistive Robot and Companion. In: 2020 29th IEEE International Conference on Robot and Human Interactive Communication (RO-MAN), pp. 745–751 (2020). https://doi.org/10.1109/RO-MAN47096.2020.9223470

[164] Errante, L.: Public Space: Mapping the Physical, Social and Cultural Accessibility for the Creation of Urban Commons. In: Macrì, E., Morea, V., Trimarchi, M. (eds.) Cultural Commons and Urban Dynamics: A Multidisciplinary Perspective, pp. 113–140. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-54418-8_8

[165] Carmona, M.: The Visual Dimension. In: Public Places Urban Spaces: The Dimensions of Urban Design, Third edition edn., pp. 252–314. Routledge, Taylor & Francis Group, New York London (2021)

[166] Carmona, M.: The Perceptual Dimension. In: Public Places Urban Spaces: The Dimensions of Urban Design, Third edition edn., pp. 152–195. Routledge, Taylor & Francis Group, New York London (2021)

[167] Carmona, M.: The Social Dimension. In: Public Places Urban Spaces: The Dimensions of Urban Design, Third edition edn., pp. 315–382. Routledge, Taylor & Francis Group, New York London (2021)

[168] Carmona, M.: The Functional Dimension. In: Public Places Urban Spaces: The Dimensions of Urban Design, Third edition edn., pp. 384–470. Routledge, Taylor & Francis Group, New York London (2021)

[169] Vitale, J., Tonkin, M., Herse, S., Ojha, S., Clark, J., Williams, M.-A., Wang, X., Judge, W.: Be More Transparent and Users Will Like You: A Robot Privacy and User Experience Design Experiment. In: 2018 13th ACM/IEEE International Conference on Human-Robot Interaction (HRI), pp. 379–387 (2018)

[170] Stallings, W., Brown, L.: Wireless Network Security. In: Computer Security: Principles and Practice, Fourth edition edn., pp. 722–753. Pearson, New York, NY (2018)

[171] Arfeen, A., Ahmed, S., Khan, M.A., Jafri, S.F.A.: Endpoint Detection & Response: A Malware Identification Solution. In: 2021 International Conference on Cyber Warfare and Security (ICCWS), pp. 1–8 (2021). https://doi.org/10.1109/ICCWS53234.2021.9703010

[172] Stallings, W., Brown, L.: Denial-of-Service Attacks. In: Computer Security: Principles and Practice, Fourth edition edn., pp. 246–272. Pearson, New York, NY (2018)

[173] White, R., Caiazza, G., Christensen, H., Cortesi, A.: SROS1: Using and Developing Secure ROS1 Systems. In: Koubaa, A. (ed.) Robot Operating System (ROS): The Complete Reference (Volume 3). Studies in Computational Intelligence, pp. 373–405. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-91590-6_11

[174] Stallings, W., Brown, L.: Cloud and IoT Security. In: Computer Security: Principles and Practice, Fourth edition edn., pp. 445–479. Pearson, New York, NY (2018)

[175] Ahmad, S., Mehfuz, S., Beg, J.: Enhancing Security of Cloud Platform with Cloud Access Security Broker. In: Kaiser, M.S., Xie, J., Rathore, V.S. (eds.) Information and Communication Technology for Competitive Strategies (ICTCS 2020). Lecture Notes in Networks and Systems, pp. 325–335. Springer Nature, Singapore (2021). https://doi.org/10.1007/978-981-16-0882-7_27