AI-Powered Self-Service Physical Security for Data Centers

Nareddy Abhireddy
Independent Researcher
nareddy.abhireddy.researcher@gmail.com

Abstract

Physical security management in data center environments is becoming increasingly customer-centric, with providers offering self-service capabilities to reduce wait times and improve customer experience. However, this shift creates a dichotomy: greater autonomy for customers can also open the door to misuse, and distrust in the underlying technology may lead customers to deliberately circumvent security controls, undermining their effectiveness. This mismatch between customer trust and security assurance remains an underexplored area of research.

Artificial intelligence offers a path forward through personalized self-service and decision-support models, which have been shown to improve user experience while increasing trust and reliance on associated technologies elsewhere in the AI domain. This paper proposes extending that approach to physical security management in data centers by designing personalized self-service frameworks tailored to individual customer profiles. We first identify key personalization factors — such as age and technology experience level — and map them into a customized service framework. A user needs assessment, conducted through focus groups, then informs UI customizations that support self-service capabilities. The goal is a personalized approach to physical security self-service that enhances customer experience without compromising security.

Keywords: AI-Driven Self-Service, Physical Security Management, Data Center Security, Personalized Security Models, Customer Experience Optimization, Security Usability Design, Trust in AI Systems, Security Control Effectiveness, Self-Service Security Systems, Decision Support Systems, User-Centric Security Design, Security Personalization Factors, Human-Centered AI, Secure Customer Interfaces, Access Control Systems, Behavioral Security Analytics, Customer Trust Modeling, Security Risk Mitigation, Adaptive Security Frameworks, Intelligent Security Services.

1. Introduction

Prior research shows the potential to employ AI for low-risk physical security service support in data-center environments, allowing organizations to focus on critical aspects while relying on machines to handle their routine work. However, such efforts still rely on traditional interaction approaches and functionalities, where an organization's user needs and discomforts are not considered. In new-age systems where user-centricity is the kingpin for adoption, focusing on user discomfort toward the existing technologies is the way forward. To harness the full benefits of AI support, organizations need to move not only from user-driven systems to self-service but also to personalized self-service, where the existing tastes and experience of individuals are considered for effective usage.

The presence of online security self-service systems has considerably improved incident response times. But not all information can be handled via these systems, prompting users to reach human support. Dedicated AI support for these high-volume, low-complexity human tasks with actual or perceived user discomfort in using such systems, therefore, appears to be one of the best solutions. For physical-security management in such environments, where the internal admission regulation is stricter than at an airport, continuous user need analysis plays a vital role in service effectiveness. Users, mainly employees, have specific tastes and customizable requirements for signing in-out, requesting permission for external visitors, managing their visitors, and other physical-security-check-related activities. An analysis of their requirements and discomfort while using existing systems can lead to an effective personalized security self-service design.

2. Foundations of AI-Driven Physical Security in Data Centers

One or both of the following aspects shape personalized AI-driven self-service customer interfaces for physical security management in Data Center Services. A Data Center's employees are usually young people or skilled Data Center's services providers managers who interact with the Data Center Security System through the Security Interface. These individuals may prefer some degree of self-service in resolving security incidents without the involvement of Security or Facilities Management personnel. Such a self-service model usually increases user satisfaction. However, as any service system, it requires a design that meets the users' needs, tastes, and preferences to be efficient in terms of user satisfaction. Several youths in various regions of the world, including India, South Korea, and Singapore, participated in an investigation of the interactions of customers aged 15 to 25 years with physical security services and service providers. The investigation revealed a need to introduce personalized self-services or at least the possibility of customization of customer interactions.

While the Data Center Security System's customer segments interact through a similar security interface, decision-support AI models support these transactions behind the scenes. The models vary in complexity and sophistication depending on the segment of customers to which the security incident corresponds. The reason for this disparity is that an AI model (or a set of AI models) supporting a customer segment is usually customized using a training dataset that corresponds specifically to the customer segment. The main sources of these training datasets are the past incidents and accidents that the Data Center Service has experienced. However, many Data Center Services or Service Providers do not keep records of minor incidents even when these incidents cause security problems with relatively high frequency.

2.1. Definitions and scope

Personalization, self-service and physical security in data centers are defined and their domain delineated.

In the context of self-service, personalization refers to making information, applications and services relevant and tailored to the user's needs and preferences. It supports self-service adoption, improves overall user experience and makes it easier for users to find what they are looking for and complete their goals. For data centers and cloud computing providers, the user customer is an organization—often an enterprise with thousands of employees, putting pressure on services to offer self-service solutions that can assist the organization in solving common issues by themselves, especially those who do not require human oversight. Yet these organizations have their own users—often being youngsters or inexperienced people. Personalized security interfaces provide data-center customers and their users improved experience when using self-service security applications.

Data centers house multi-tenant cloud computing services. Customers rent out part of the data center to host their own servers. They in turn offer services, often to many end-users. It is common for these end-users to be youngsters—young university students, teenagers, disloyal clients, hackers testing their skills and challenging the organization. Attackers can subvert an organization's security by using easily obtainable information to bypass the organization's security policies. Personalizing security services—emails to be received when user accounts are hacked or websites presenting maintenance alerts, dashboards, even the data stolen in attacks—improves user experience and builds user trust in security solutions. Improving this user experience in the self-service components of security in large multi-tenant cloud computing

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 04 Issue: 02
RECEIVED: APRIL 07
REVISED: APRIL 26
ACCEPTED: MAY 08
PUBLISHED: MAY 17

services, while keeping the solution's effectiveness or performance, is decisive for an organization.

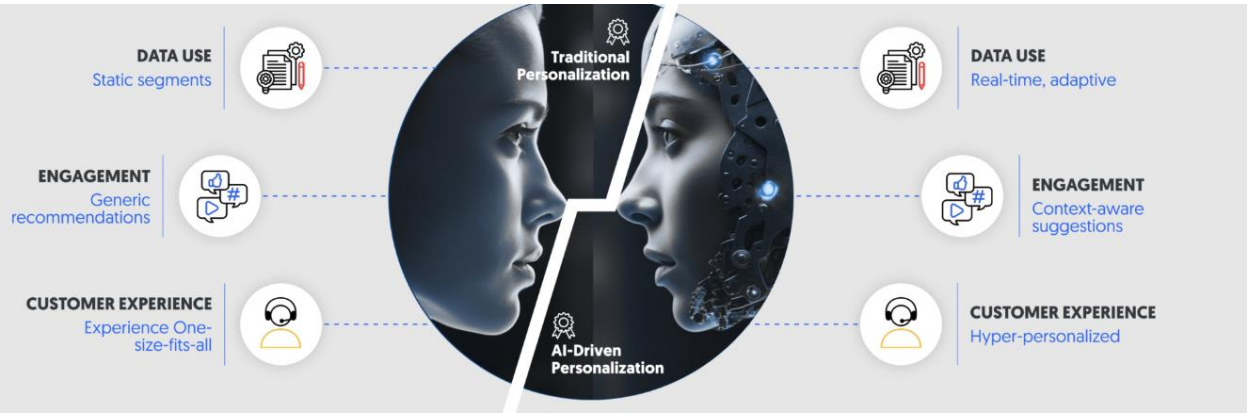


Fig 1: The AI-Powered Customer Experience

2.2. Key technological enablers

Personalized AI-enabled self-service solutions for managing physical security at data centres require a range of supporting technologies, especially in the areas of personalized customer self-service models, the AI models and data infrastructures that enable security decision support, and the data and services used for integrated management of security-related functions.

2.2.a. Personalized customer self-service models

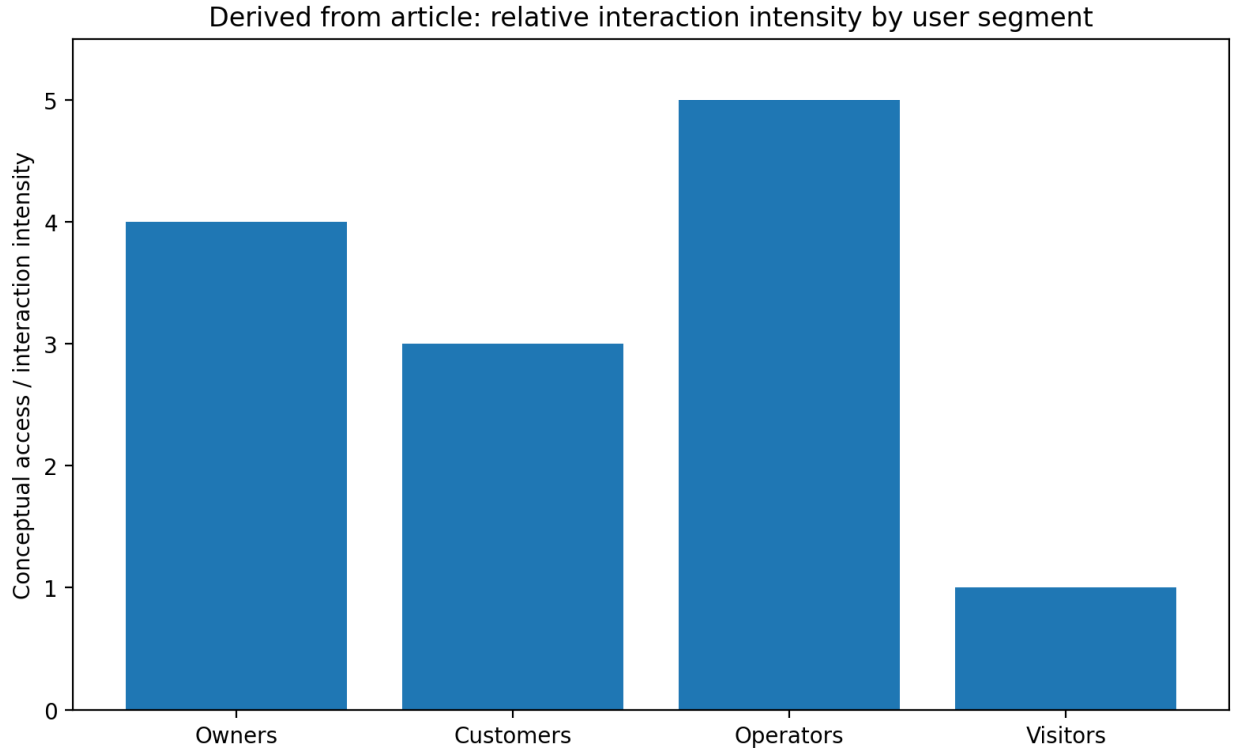
The handling of security issues, and particularly incidents, has been recognized for many years as a challenging area for self-service. Generally, security incidents need immediate attention—usually by highly skilled personnel—and they are often complex, sensitive, and demand considerable resources. This makes effective immediate and long-term management of security incidents vital for security governance. Despite these difficulties, it is possible to identify classes of users for whom personalized security self-service interfaces are appropriate. Such personalized self-service interfaces should improve the experience and satisfaction of both internal and external users of security services and make those users more willing to contemplate

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 04 Issue: 02
RECEIVED: APRIL 07 REVISED: APRIL 26 ACCEPTED: MAY 08 PUBLISHED: MAY 17

a greater degree of involvement in more effective management of security incidents (for example, acting as human sensors, aides, or even investigators).

2.2.b. Data-centre user population

Data-centre users are typically segmented into four groups: owners, customers, operators, and visitors. All except visitors often have multimodal access to the data centre either continuously (for example, operators) or at least at predetermined intervals (as is often the case for customers). Consequently, personalised security self-service interfaces suitable for these different groups can be defined.



Equation 1. Detection Accuracy

The states that security effectiveness includes **detection accuracy**, and it also names **TP, TN, FP, FN**.

Let:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

Step 1: Total number of classified security events is

$$N = TP + TN + FP + FN$$

Step 2: Correct decisions are the sum of true positives and true negatives:

$$\text{Correct Decisions} = TP + TN$$

Step 3: Detection accuracy is the fraction of correct decisions over all decisions:

$$\text{Detection Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Step 4: In percentage form,

$$\text{Detection Accuracy (\%)} = \frac{TP + TN}{TP + TN + FP + FN} \times 100$$

3. Methodology

The study draws upon a combination of empirical sources and modeling techniques for adaptation of AI-based decision support and self-service security management in data centers, with the security interface tailored to specific user profiles. Considered as a functional unit, the user profile consists of a segment marker and a user conduct model: the former is a categorical variable identifying the user group they belong to (e.g., contractor, data center employee, visiting technician, guest), whereas the latter determines the system-response customization, relying on data-collection methods (e.g., interview, control system logs, AI-driven activity detection) suitable for each group. The appropriation mechanism is built upon the input–output

expectations of the self-service interaction, focusing on clarity and accuracy of preconditions, which can differ between user profiles.

The proposed adaptation for profile-based tailoring of the service interface addresses a two-stage lifecycle: the first considers usage of the security self-service as a potential information gathering channel for users within a security process overseen by human operators; the second focuses on the system being wholly entrusted to the users for no-disturbance low-risk operations. Data collection, feature-engineering techniques, and evaluation plans for these stages are summarized. In addition to service-lifecycle phases, security self-service adoption demands assessment not only of security effectiveness, but also of usability and user acceptance.

Table 1. Core article structure and technical meaning

Section	Main idea	Technical interpretation
Introduction	AI can support low-risk physical security work in data centers	Move from generic support to personalized self-service
Foundations	Personalization improves satisfaction and trust	User-specific interface logic is required
Methodology	User profile = segment + conduct model	Personalization can be modeled as feature-driven adaptation
Objective	Tailored interfaces improve UX, confidence, and security efficiency	Main causal hypothesis of the study
Personalization	Different users need different interface depth and guidance	Adaptive UI/UX is central
AI Models	Rules-based, ML, and hybrid decision support	Hybrid model is most appropriate
Operationalization	Self-service must integrate access control, audit, and orchestration	Security services need governance and workflow discipline
Risk/Ethics	Fairness, accountability, transparency, retention	Responsible AI constraints

Section	Main idea	Technical interpretation
Evaluation	Security, usability, and adoption metrics	Performance must be measured multi-dimensionally

3.1. Tailoring Security Interfaces to User Profiles

This section explains the steps taken to customize self-service physical security management interfaces to match user profiles. User profile questionnaires identify the interests, trust levels, and knowledge of specific service areas of potential users. Features for quantitative assessment of user profiles and profile groups are then engineered. Finally, these user profiles serve as a roadmap for selecting optimal design parameters for self-service interfaces, as well as evaluating the interfaces' usability and effectiveness.

To ensure the best possible service experience, physical security management systems increasingly adopt self-service interfaces that allow clients to rapidly address their own inquiries regarding office premises. However, the ease of self-service also places greater responsibility on client users, who must feel comfortable submitting requests so that they are not ignored. To encourage confidence in submitting self-service requests, interfaces can be tailored to fit user profiles, thereby making information presentation clearer and helping users navigate the interface with greater speed and ease. Consequently, clients' perceived user experience of self-service systems is fundamental, as augmenting user experience promotes a sense of control, which in turn tends to build trust, encourage usage, and improve overall service satisfaction.

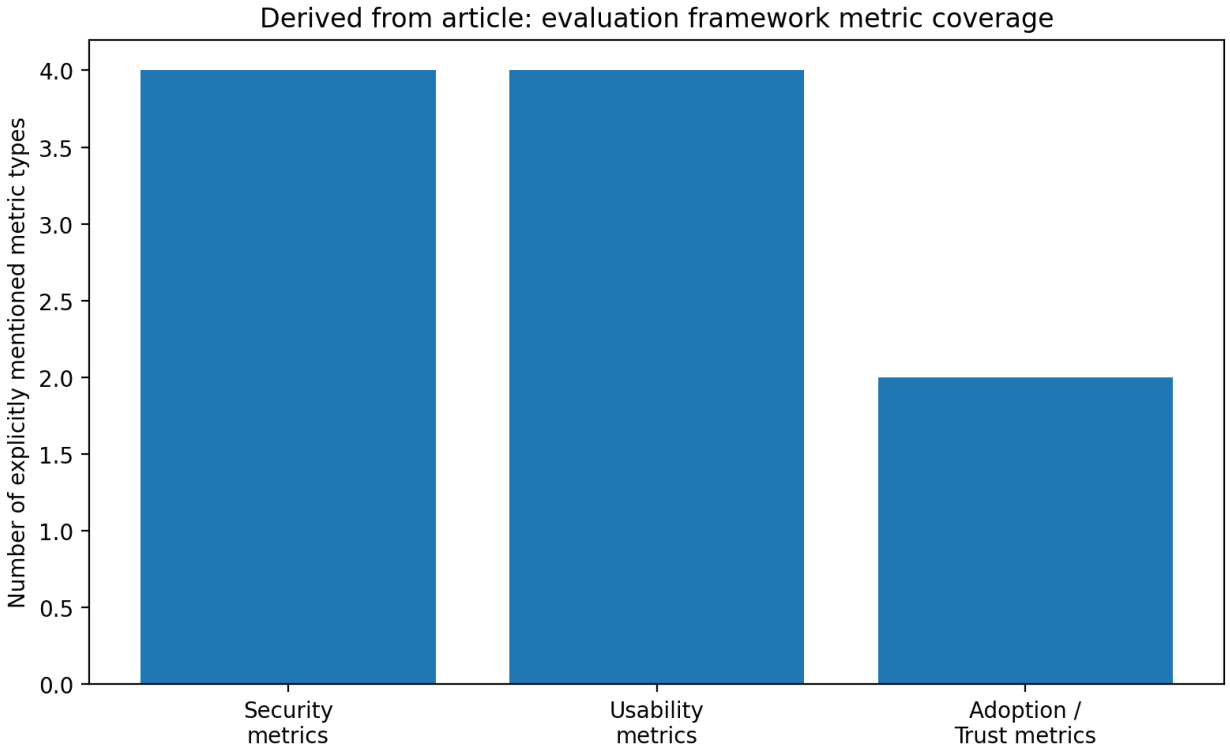
4. Objective of the Study

The objective of this study is the design of personalized self-service interfaces, powered by artificial intelligence (AI), for individual security management in data-center environments. The aim is to offer these interfaces to data-center administrators and any authorized individual or entity requiring access to these environments, such as service users, partners providing support and maintenance services, clients involved in the supply of equipment, or government agencies.

A primary objective of the research is to design service interfaces, personalized according to user profiles, with a direct impact on the quality and usability of each user's interaction with the physical-security services supporting the management of data centers. The quality of the user experience is expected to positively influence user confidence in the security services, creating an environment in which users are more willing to participate and use the services when

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 04 Issue: 02
RECEIVED: APRIL 07 REVISED: APRIL 26 ACCEPTED: MAY 08 PUBLISHED: MAY 17

appropriate. In turn, this should contribute to improving the overall security level of data-center environments. The assessment of the proposed objective is based on the following hypothesis: the customization of security-management interfaces, according to user profiles, improves user experience and confidence in the services offered and, consequently, the efficiency of physical security in data-center environments. Success is measured through careful comparison of the tailored interfaces and the results of usability-tests executing the services, and also through the analysis of users' perspectives regarding the quality of these services.



4.1. Research Purpose and Goals

The purpose of this study is to define personalized customer self-service models, using artificial intelligence (AI), for physical security management in data-center environments. Personalized interfaces will be customized for the two main user segments—public auditors and system administrators—identified in previous research. The main goal is to determine how

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 04 Issue: 02
RECEIVED: APRIL 07 REVISED: APRIL 26 ACCEPTED: MAY 08 PUBLISHED: MAY 17

interactions between users and security interfaces can be tailored to their specific characteristics, including preferences, trust in self-service security, technical knowledge, and past experience with self-service security systems. Based on the interface customization, a service design framework will also be proposed to ensure the secure operation of physical security management systems.

The anticipated contributions can be organized into three main categories: a methodology for preparing personalized customer self-service models for physical security management; an improvement in user experience with customer self-service models for physical security management; and an increase in the security effectiveness of physical security management systems through the accessible use of AI. Two hypotheses will be tested: Interface characteristics can be tailored to the profiles of their users, and such tailoring improves the user experience of the interface. Success will be demonstrated if the positive impact of user-profile tailoring on user experience can be shown with statistical confidence.

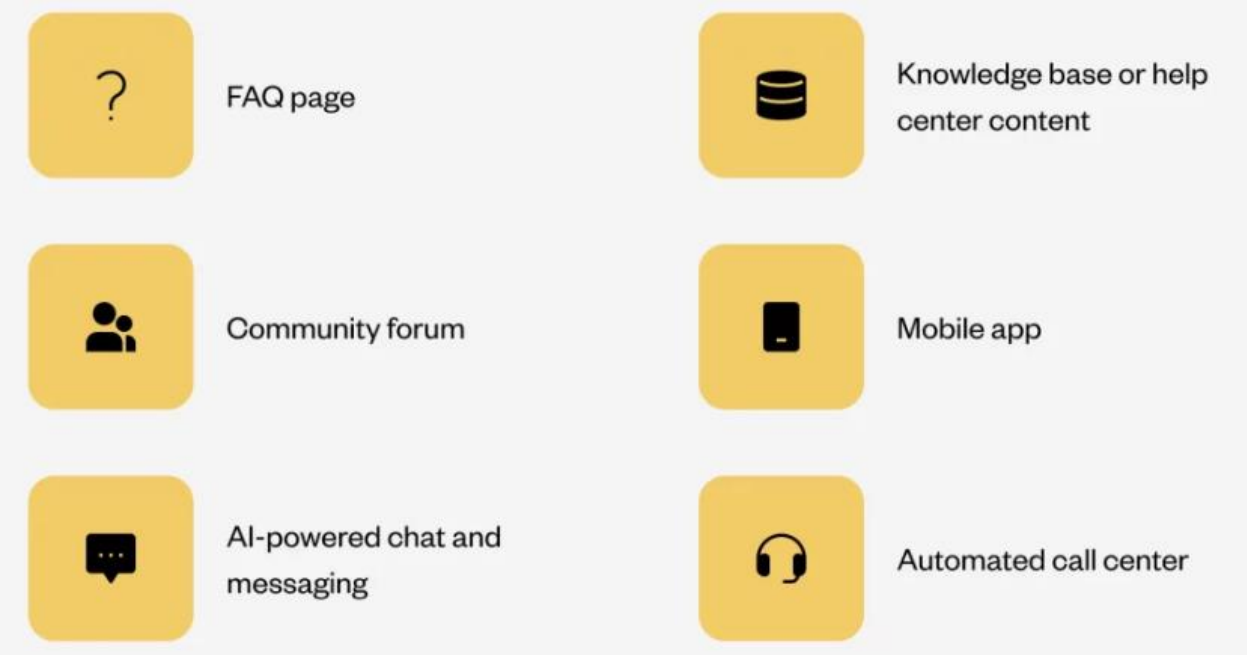


Fig 2: Examples of customer self-service

5. Research Summary

Aligning data centers' operational information and communication technology environment with a strategy based on AI-assisted personalized customer self-service modes applied to physical-security management is assisted by AI supported personalized customer services. Responding to frequent business interruptions and user frustration with service desk delays and inability to assist after-hours incidents by implementing AI-assisted personalized self-service modes would enhance users' experience and increase user availability. Three aspects of the investigation are the analysis of personalized-user profiles and their appearance towards adopting self-service modes, the potential of personalized self-service interface as an improvement in human behaviour for both end users and the operation team, and the adoption of AI models to assist the security management and security event prioritization in accordance with the defined modes. AI-assisted personalized customer self-service modes improve the user experience and raise the security level of the data-centre environment.

Delving into the pros and cons of a personalized approach in security disciplines by analysing two areas of concern of security-management operations is at the core of the investigation. The first concerns end users' willingness and necessity to become involved in security operations; from a security-management operations perspective, the service desk is often a bottleneck when assisting security events out of office work hours and weekends. The second area entails incorporating AI capabilities into security-management processes. AI models can assist in the pre-selection and filtering of security alerts, according to personalized criteria, thus providing an additional level of prioritization. The importance of personalizing self-service interfaces and a comprehensive usability evaluation remain relevant.

5.1. Customizing Security Interfaces for Enhanced User Experience

Security interfaces supporting self-service operation of physical data-center security are typically designed to provide a consistent overall experience to all user types. Such a strategy is therefore not user-centered and represents a simplified, one-size-fits-all approach. Individual users can be very different in terms of their experience with security interfaces and their level of knowledge about possible security risks and mitigation actions. Adopting such differences into the user experience design would help deliver a more tailored solution, potentially addressing specific issues of one type of user group while improving overall user experience.

A research goal is to explore how these individual user differences can be taken into account in the interface design. To achieve this goal, various user types are identified and specific methodologies are used to assess the level of knowledge of each user type about potential security risks and possible mitigation actions. The outcome of these assessments is then proposed as a means to customize the security interfaces for each user type with the aim of enhancing the overall experience and trust in the physical security of the data center while at the same time not introducing new security risks associated with a poorer knowledge of security measures.

Equation 2. False Positive Rate

The emphasizes that a high number of false positives wastes responder time.

Step 1: The false positive rate compares false alarms to all actually negative cases.

Actual negatives are:

$$TN + FP$$

Step 2: Therefore,

$$\text{False Positive Rate} = \frac{FP}{FP + TN}$$

Step 3: Percentage form:

$$\text{FPR (\%)} = \frac{FP}{FP + TN} \times 100$$

6. Personalization in Self-Service Security Interfaces

Self-service security interfaces can benefit from situationally-aware adaptation to match evolving user characteristics and skills over time. Data centers typically employ young, tech-savvy resources, yet some tasks may still introduce a burden. Users' backgrounds must therefore be assessed to ascertain the degree of personalization required. Younger, technology-oriented users may prefer finer granularity, while a broader approach may be warranted for less-expert resources. An assessment of their acceptance of such interfaces is essential. Additionally, flows originating from camera feeds can be enabled or disabled according to users' capabilities,

seamlessly integrating power and usability aspects, and reducing burdens for less-skilled profiles.

In data centers, resources involved in physical security are usually on the younger side of the experience curve, as younger components provide higher levels of reliability. Nevertheless, a portion of the work executed concerning facilities should receive extra effort. Users should therefore receive a careful assessment of their particular characteristics, defining the adoption of an area-specific self-service security interface. In this segmentation, user experience plays a significant role, being associated with user trust and leading to reduced costs for the organization. Moreover, an implicit cooperation factor exists among the involved stakeholders. Addressing the interface's acceptance across the user bases is a second major aspect associated with the proposed adaptation. Students of technology-oriented majors are expected to positively receive the adoption of finer levels of granularity in the self-service capabilities, while users belonging to traditional administration-oriented faculties tend to receive such capabilities with more reserve.

Table 2. User segments mentioned or implied

User segment	Role in data center security	Typical need	Interface implication
Owners	High-level stakeholders	Oversight, compliance, visibility	Dashboard-oriented interface
Customers	External or tenant users	Access requests, logs, temporary actions	Guided self-service with stricter controls
Operators	Internal experts	Operations optimization, event handling	Faster workflow, more advanced controls
Visitors	Limited-access external individuals	Temporary and constrained access	Minimal, high-clarity interface
Public auditors	Review and verification	Traceability, evidence, compliance checking	Read-heavy, audit-friendly workflow
System administrators	Technically experienced internal users	Fine-grained control, rapid action	Dense interface with expert shortcuts

6.1. User segmentation and needs assessment

Data-center physical security presents an ideal candidate for personalized customer self-service, as these facilities are generally closed to end users and are not accessible to casual users. Even though the technology used by these data-center operators has progressed over the years, the interface for consuming these services has lacked personalization. As a result, users from different domains consume these services based on a common interface. The difference between a corporate user seeking access to only the data center inside the facility and a cloud-user-of-the-facility seeking access for a few hours to perform maintenance should be captured and made available in the service interface.

Segmentation is a noteworthy method to measure user needs. In the case of data-center-integrated physical security management for multiple customers, the major segments are media and entertainment companies, cloud solution providers, enterprise companies, and other small users. The user-groups can be evaluated individually or collectively to understand possible needs. Some user-groups have direct access to the Data-center facility and require a single point of contact for these services. Media companies consume the data-center services only once a year for a few days, as they enjoy a high scale of production. The physical security service of the service provider and the physical security of the data-center owner should provide support for access control. The need for effective need-assessment strategies is paramount for offering a set of security services to users of the data-center facility. Need-assessment strategies help in identifying the key areas on which to focus in order to make the physical-security service more user-centric in nature. The user-groups implementing the digital-twin technology for providing services in the data-center market can be adopted as a baseline for service customization.

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 04 Issue: 02
RECEIVED: APRIL 07 REVISED: APRIL 26 ACCEPTED: MAY 08 PUBLISHED: MAY 17

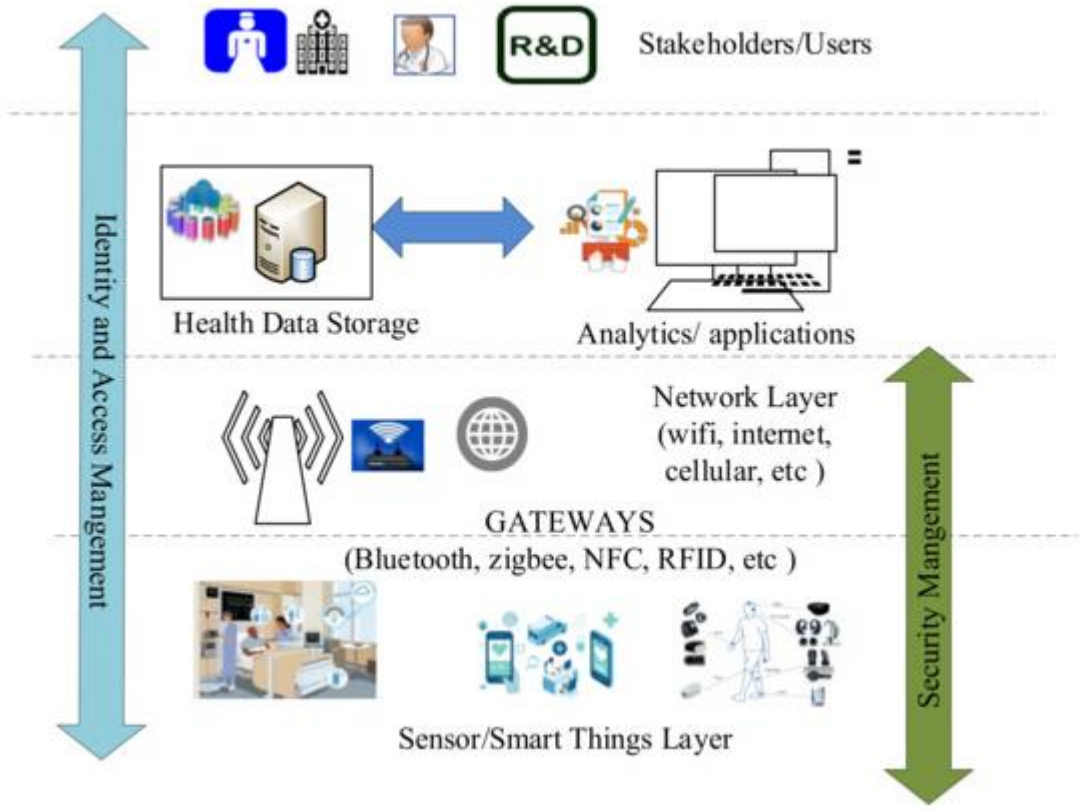


Fig 3: Self-Sovereignty Identity Management Model for Smart Healthcare System

6.2. Personalization strategies and UX implications

For the identified users, several strategies are proposed to enhance the experience and support security management. Customers and internal employees, the key users, could benefit from numerous enhancements and custom features; ML-powered product recommender engines supplied by real-time usage data and customer profiling could ease the shopping experience. Business divisions, users with heavy communication with Data Centre Operations and Data Centre Services, could have a central dashboard for support tickets and reports.

Such systems generally support normal operations, enabling the company and customers to maintain day-to-day operations with the Data Centre more efficiently. Crisis situations are

more complex; without the intervention of Security Operators, these interfaces are untrusted by the customer. Information and training are extremely important to build trust, and different motives are present. Generation Z and younger age groups require more content and engagement than Baby Boomers, who seek comfort and reduced incoming calls, whereas internal employees wish for better communication channels. During crisis situations, the security measures should remain firm to reduce false positives and contact volume, but testing with pure users is also important to detect interfaces' strength while building trust.

These aspects are common for many organizations, and products could fill different niches. The lack of use may be related to the perception of low engagement of firms with customers instead of victims of serious incidents. Keeping the user engaged improves experience and increases trust; in pure security situations or without an emotional connection to the Data Centre, the DMADUX process remains unchanged.

7. AI Models and Data Architectures for Security Management

A comprehensive, integrated system architecture supports physical security management, supplying the necessary user data and decision-support models. Security management, an essential component of physical security, encompasses actions taken to ensure both comprehensive data-center protection and the fulfillment of relevant compliance requirements. Physical security interfaces provide the bridge between users and support systems, allowing user-inputted information to be processed by underlying data sources and modelling architecture before being returned to attendees, operators, and management teams in a user-friendly manner.

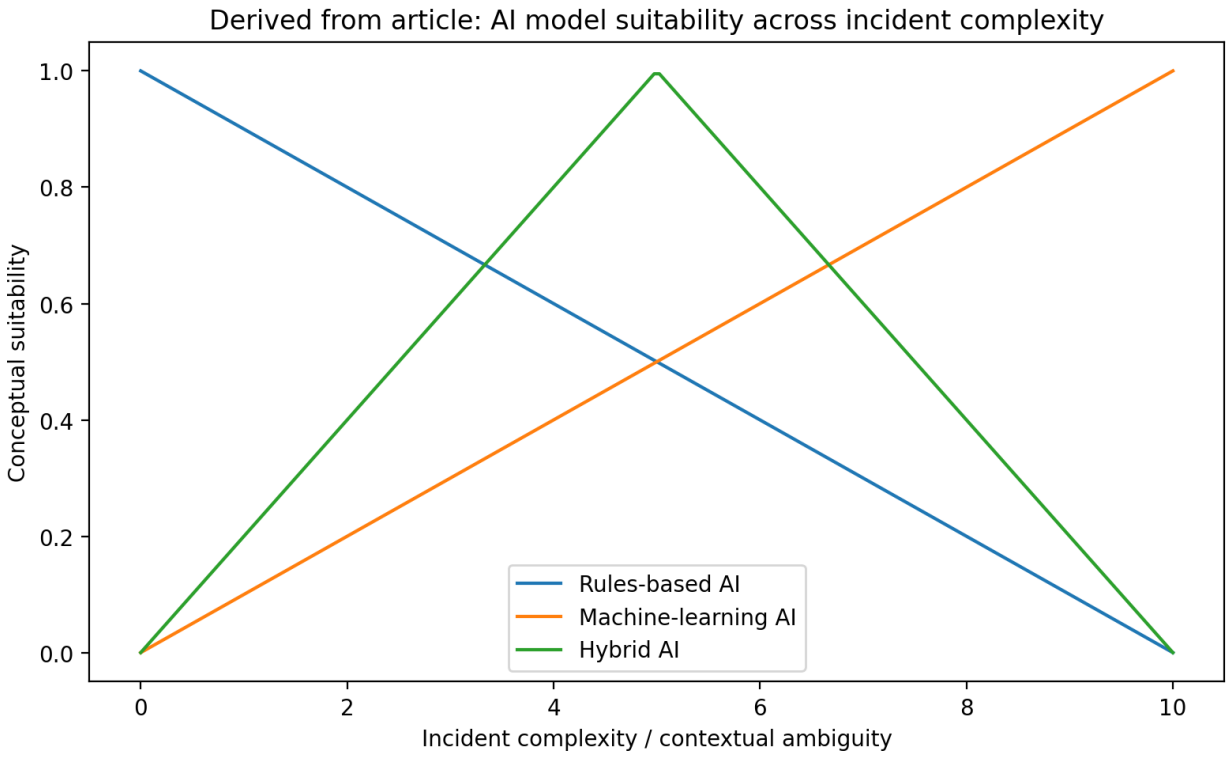
Management data flows in the context of physical security and user-provided information are illustrated in Figure 7.2. The data architecture, service layers, pipeline integration, and considerations for data privacy and quality are detailed in the following sections. Elements used to help users make physical security decisions are also described, focussing on the different types of automated decision-support systems being employed (rules-based, machine-learning, and hybrid). The ultimate aim is to match the capabilities of the employed decision-support architecture to the different classes of user activity being supported; data archiving and user-content auditing considerations are then highlighted. User inputs are essential for effective incident-response execution, enabling additional context and data to be leveraged for incident investigation and security-compliance maintenance.

7.1. Data sources and integration

Data integration for personalized self-service interfaces relies on the following sources: Security Information and Event Management (SIEM) systems aggregate logs from security components (e.g., firewall, VPN, IDS/IPS, DLP) and provide alerts for security incidents. IP telephony systems and ticketing platforms (e.g., ServiceNow) offer contextual data on user activities (e.g., work vacations), as well as onboarding/offboarding information. Physical access control systems (PACS) provide user access profiles, while video surveillance systems deliver images and footage of security incidents. Integration also encompasses weather and vulnerability data.

User privacy controls during personalization are paramount. The decision-support models leverage a mix of anonymized and non-anonymized data; hence, risk scoring supports data sharing with subject-matter experts for evaluation. Moreover, all models undergo a commitment phase to ensure quality before deployment. Anonymized logs from the self-service framework are aggregated and monitored to verify generalization and robustness. In particular, these metrics verify excessive false positives, negative false rates, and outlier long times for success and response.

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 04 Issue: 02
RECEIVED: APRIL 07
REVISED: APRIL 26
ACCEPTED: MAY 08
PUBLISHED: MAY 17



7.2. Model types for security decision support

A variety of model types can support security decision-making. Rules-based AI offers clear operational insights and enables fast response times. However, for more contextually complex incidents, machine-learning AI can help align responses with stakeholders' needs, ethics, and laws. Moreover, precise AI use can enhance user satisfaction and trust, improving the overall service experience. A successful combination of both solutions therefore satisfies the required decision-support capabilities.

Guided mainly by the defined user segments, a hybrid decision-support AI emerges as the most appropriate solution. While a rules-based engine will cover the majority of relevant incidents, machine-learning AI can support the remaining cases, alerting security operations to truly remarkable situations, particularly when the end-user service is not available.

8. Operationalizing Self-Service in Data Center Environments

To demonstrate the practical applicability of personalized customer self-service solutions in physical security management using AI, five data centers operated by a telecommunications provider in Portugal were considered. These data centers provide services for private companies, public administration, and other telecommunications operators. The service design for self-service in these environments adhered to the principles of Service-Dominant Logic (S-D Logic). S-D Logic emphasizes the co-creation value within service relationships, the design of a service ecosystem, service lifecycle and development, orchestration and governance mechanisms, service interfaces, and dynamically adjusting the service offering with service-dominant business models.

The service lifecycle covers all the elements of the service process from service design to delivery, and the service interface between the customer and provider becomes the main focus of the research. This approach allowed the analysis of self-service in security management to go beyond usability to the concepts of trust and sense-making. Indeed, the design of the interface is only one of the elements that need to be considered to improve the experience of self-service. These elements also determine the effectiveness of the self-service model in terms of security. The creation of customer segments in self-service is a way to go beyond usability and make the customers feel more comfortable and secure using the service. Customer interviews focused on understanding what makes them feel more secure and comfortable when interacting with security interfaces.

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 04 Issue: 02
RECEIVED: APRIL 07
REVISED: APRIL 26
ACCEPTED: MAY 08
PUBLISHED: MAY 17

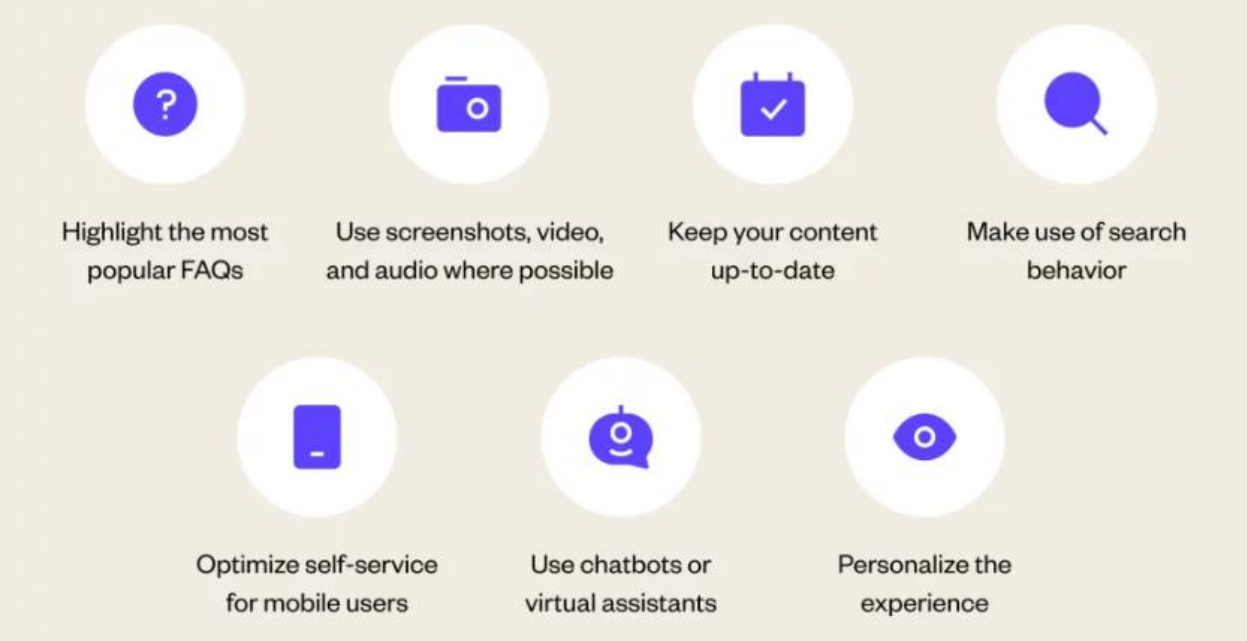


Fig 4: 7 Tips for Customer Self-Service

8.1. Service design and workflow orchestration

Structured self-service speaks to users' needs, shielding them from complex underlying technologies while anticipating and managing incidents. Security services weave into users' business lines and activities; service lifecycles often mirror business demand patterns.

For data centers, lifecycles match predictive analytics for data center demand; security responses typically align with incident-response procedures. Orchestration reflects the security PPD-IO model. Security-as-a-Service enables real-time monitoring of security incidents—user initiated or encountered—by monitoring systems, forwarding logs and alerts to AI-intensive decision-support engines, which may propose alternative responses.

Access, authentication, and authorization mechanisms assure that only authenticated users gain access to authorized resources and services; the principle of least privilege governs access assignments, and audit trails support assessment of risk and compliance.

Equation 3. False Negative Rate

The also names false negatives as a core security metric.

Step 1: Actual positive cases are

$$TP + FN$$

Step 2: False negative rate is the fraction of missed positives among all actual positives:

$$\text{False Negative Rate} = \frac{FN}{TP + FN}$$

Step 3: Percentage form:

$$\text{FNR (\%)} = \frac{FN}{TP + FN} \times 100$$

8.2. Access control and authentication mechanisms

Operationalization requires implementing support for access control, authentication, and authorization, including managing user roles and entitlements within an incident-management context. Mechanisms for mitigating the risk of unauthorized access must apply the principle of least-privilege while ensuring that accurate records are kept of which individuals have handled specific security events and their steps during the investigation. Based on empirical evidence, such an approach encourages accountability and fortifies trust in the AI-based required actions.

Self-service security interfaces are intended for internal users—primarily staff who are familiar with the facilities, processes, and procedures. For these individuals, the scaffolding associated with such interfaces should allow self-service while recording a clear audit trail to support subsequent external scrutiny, if required. Challenges arise because such users' roles may not be supported by established administrative procedures or the specialization of support functions in smaller organizations. Therefore, the identity and roles of individuals interacting with AI-based security management services, such as control and decision support, need to be dynamically matched with the required security service levels.

9. Risk, Ethics, and Compliance in AI-Enhanced Security

Risk, fairness, accountability, and transparency of AI-enabled personalized self-service models for physical security management are examined and structured within established frameworks promoting responsible, ethical AI. Bias analysis, accountability in model design and deployment, appropriate levels of disclosure, and privacy protection within data retention and regulatory compliance are addressed.

Risk analysis reviews the impact of biased training data on AI model decision making, discusses measures for promoting fairness and user trust, explores how ethical considerations are integrated into AI systems, and reviews the degree of transparency needed to promote user trust. Distinctions are drawn between training data bias and use-case awareness risk, together with model life cycle influences on bias mitigation. Relevant frameworks for algorithmic fairness and accountability are summarized. Methods for promoting user trust through risk and transparency disclosure, and their implications for service usage, are assessed.

Analysis of biased training data and its consequences for AI model-supported decision-making identifies measures for promoting fairness and user trust in digital security areas supported by AI technologies. Awareness of the risk of bias being present in training data is an important consideration when developing AI-supported systems since their performance depends largely on the quality and representativeness of the training data set. For personalized self-service systems provided for users with different skills, awareness of bias risk is also a factor in the level of transparency required to establish and maintain user trust.

9.1. Fairness, accountability, and transparency

Risks arising from security management support, and generalized decision support with minimal human intervention, require consideration of fairness, accountability, and transparency. The following analyses focus on bias considerations, disclosure of possible failures, and mechanisms of operational accountability.

Security guarantees should not favor particular user demographics. Security algorithms can discriminate if the underlying data has significant relevance to a user's protected characteristics, such as race, gender, or sexual orientation. An AI model classifier can be treated as unfair if its decision depends on protected characteristics inappropriately at test time. Moreover, multiple protected characteristics can be involved in discrimination even if decisions are invariant to each of the classifiers acting on these characteristics. Methods based on statistical

parity, equal opportunity, and how similar users are treated are useful for analyzing discrimination. Such issues are more critical when RA decision support is designed.

Fairness mitigation mechanisms are crucial because biased quality deterioration may produce security risks—e.g., increased false positives for a demographic. Most distributional fairness-maintaining methods can be arranged into three categories: pre-processing (e.g., data re-weighting), in-processing (e.g., adversarial learning), and post-processing (e.g., classifier correction). Some de-biasing methods can lead to a substantial reduction in accurate rates in favor of protected groups. Exposing the shortest paths in security operations also helps reduce the costs of accident and incident disclosure and uncover UI bugs. The same UI design considerations also are valid for dashboard design.

9.2. Data governance and retention

A data-governance framework comprises the collection, retention, and deletion policies that apply to sensitive or private data, including personally identifiable information (PII) or payment information, whose unauthorized access or release poses a significant risk for data subjects. Sensitivity classification, data usage and access audit trails, and a documented rationale for the data's retention period, purpose, and policies enable risk identification, proactive management, and GDPR compliance.

A probable data-retention policy requires all data collected and retained for support purposes to serve a direct business need, such as security incident resolution or analysis. Data not related to an active business process is deleted or anonymized after a period. The retention period must be as short as possible and aligned with the data owner's and service or product manager's interest and legal obligations. Data from moved, decommissioned, or hacked systems must be deleted, while official incident-response procedures must include clear guidance about data retention and disposal.

Equation 4. True Positive Rate / Recall

Since the stresses maximize correct positive detection, recall is directly implied.

Step 1: Again, actual positives are

$$TP + FN$$

Step 2: Correctly detected positives are TP.

Step 3: So recall is

$$\text{Recall} = \frac{TP}{TP + FN}$$

Step 4: Percentage form:

$$\text{Recall (\%)} = \frac{TP}{TP + FN} \times 100$$

10. Evaluation and Metrics for Success

A three-layer evaluation framework considers overall effect (System-Effect), user experience (User-Satisfaction), and user adoption (User-Adoption) of the proposed AI-based self-service physical security systems. User-Experience metrics evaluate Usability, whereas User-Adoption considers levels of Acceptance and Usage. The combined metrics comprehensively validate Self-Service Security Systems through scores across Security-Attacks, Usability and User-Experience. Empirical User-Experience metrics assess Deterrence-Effect and Perceived-Trust, whereas expert evaluations measure actual Security-Security.

Security-Efficiency Indicators gauge Deterrence, Efficacy, Authenticity and Trustworthiness of Security. Efficacy is determined by Detection-Effectiveness (True-Positives, False-Negatives, True-Negatives, False-Positives, Recommendation-Completion-Time, Avg-Completion-Time-for-Security-Expert, Avg-Prevention-Time-for-Security-Expert). Speedy well-justified recommendation delivery is vital for Non-AI-users and Goods-Deliverers, thus TP-Fullness must be maximized. AI-side false-recommendations and decisions of Non-AI-users need optimization. Done-and-Pending counts of AI-recommendations and Non-AI-Decision Positive-Detected incidents are also monitored.

Usability-Adoption criteria examine Perceived-Trust and Deterrent-Effect. Usability is flagged if Task-Success/Error-Rate<0.95, Time-on-Task significantly lower than critical overload, Sufficient-Peer-Adoption-Intention-designated for easy-appearance-complaint criteria, and User-Satisfaction-Basic Graph-Level-Label markers higher than 3 in trials.

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 04 Issue: 02
RECEIVED: APRIL 07 REVISED: APRIL 26 ACCEPTED: MAY 08 PUBLISHED: MAY 17

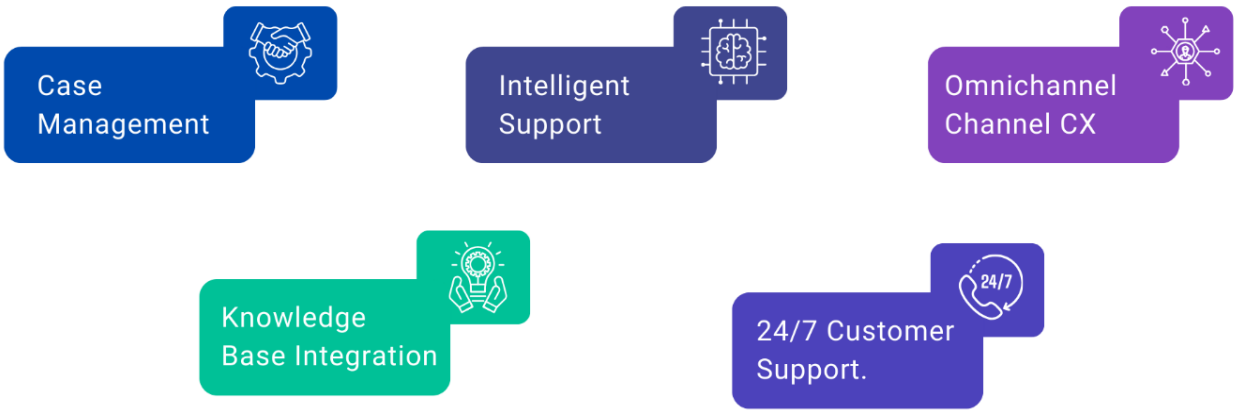


Fig 5: Implement AI-powered Customer Service using Salesforce

10.1. Security effectiveness metrics

A comprehensive set of security metrics is essential for assessing the success of a security model. The following indicate the security effectiveness of a model: detection accuracy, response time, number of false positives, and number of false negatives. To avoid sheltered environments, response time should be in the range of immediate (for large-scale operation) to within the scope-of-control for immediate action. Redundant and/or assisted layered detection systems could mitigate detection accuracy but have no effect on acceptance—result in less memorable experience and the chance of psychological fatigue.

Detection accuracy shows the correct ratio of detection, and it has a serious socio-political risk in a surveillance environment if public sentiments for human encroachment are also considered. Hence, acceptance rate of detection and true positives needs to be calculated from collected data and used as a metric as “user sensitivity”. Firewalls and antivirus solutions report the number of vulnerabilities/attacks faced, and observation shows that high-end networks get hundreds of attacks a day and may be in the range of thousand for IoT. Hence, high number of false positives indicates how much time the responders are unnecessarily played with notifications during regular operations.

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 04 Issue: 02
RECEIVED: APRIL 07 REVISED: APRIL 26 ACCEPTED: MAY 08 PUBLISHED: MAY 17

Table 3. Data sources for the proposed architecture

Data source	What it contributes	Why it matters
SIEM	Alerts, logs, incident indicators	Core detection and incident visibility
Firewall / VPN / IDS / IPS / DLP	Security telemetry	Supports event classification
IP telephony	User context	Helps explain activity and availability
Ticketing systems	Workflow and issue status	Connects incidents to support processes
PACS	Physical access profiles	Essential for physical security authorization
Video surveillance	Evidence and incident imagery	Adds contextual verification
Weather data	Environmental context	Supports risk-aware physical operations
Vulnerability data	Threat exposure	Informs prioritization and response

10.2. Usability and adoption metrics

Positive user experience is essential for any self-service model. Failure to deliver an engaging user experience may limit the model's adoption by customers, and the potential benefits arising from the service may not be realized. Several metrics can be proposed to evaluate this aspect, including:

- Task success: Percentage of users completing a security task from beginning to end without external help.

- Time on task: Average duration users require for self-service incident management and security task execution.

- User satisfaction: Degree to which users enjoy using the self-service functionality for security task execution. The System Usability Scale (SUS) is used as an overall usability indicator.

- Learning curve: Degree to which system usage becomes easier with experience.

Equation 5. Precision

The mentions optimization of AI-side false recommendations and positive detections. That implies a precision-style measure.

Step 1: All positive predictions made by the AI are

$$TP + FP$$

Step 2: Of those, the correct ones are TP.

Step 3: Therefore,

$$\text{Precision} = \frac{TP}{TP + FP}$$

Step 4: Percentage form:

$$\text{Precision (\%)} = \frac{TP}{TP + FP} \times 100$$

11. Results

Alignment with AI-assistant Drivers

Personalized self-service interfaces for physical-security management in data centers reflect the characteristics, knowledge, and needs of distinct user segments. Grouping users based on similarities along the surface dimension allows identifying dedicated methods to understand and assess their needs. The buildup of dedicated group profiles can subsequently inform the personalization of service interfaces. Two segments emerged as relevant in this case study: data-center operators and customers. Their difference in experience, used tools, and code and script

expertise drives different expectations and request modalities around the self-service security interface.

The data-center operator segment is more experienced with respect to the infrastructure's normal operation and the security system. Hence, their needs focus more on operations' optimization than on improving convenience. On the other hand, customers are less involved with the infrastructure—its normal operational profile is not under their control, and they typically just require a few additional slots in the event logs. The differences between the two groups manifest in trust, as operators feel highly qualified in assessing the request legitimacy and therefore can have a less strict process; whereas, for customers, the trust level drops, resulting in a stricter process, together with higher time investments to complete the requests.

Overall, addressing trust considerations and understanding the needs of the user segments through dedicated work is beneficial to the personal experience of any self-service interface. In the specific case of Security Management, by considering these aspects together with the facts of data-centers domains and the profile of the typical customers, the user experience can be significantly enhanced.

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 04 Issue: 02
RECEIVED: APRIL 07
REVISED: APRIL 26
ACCEPTED: MAY 08
PUBLISHED: MAY 17

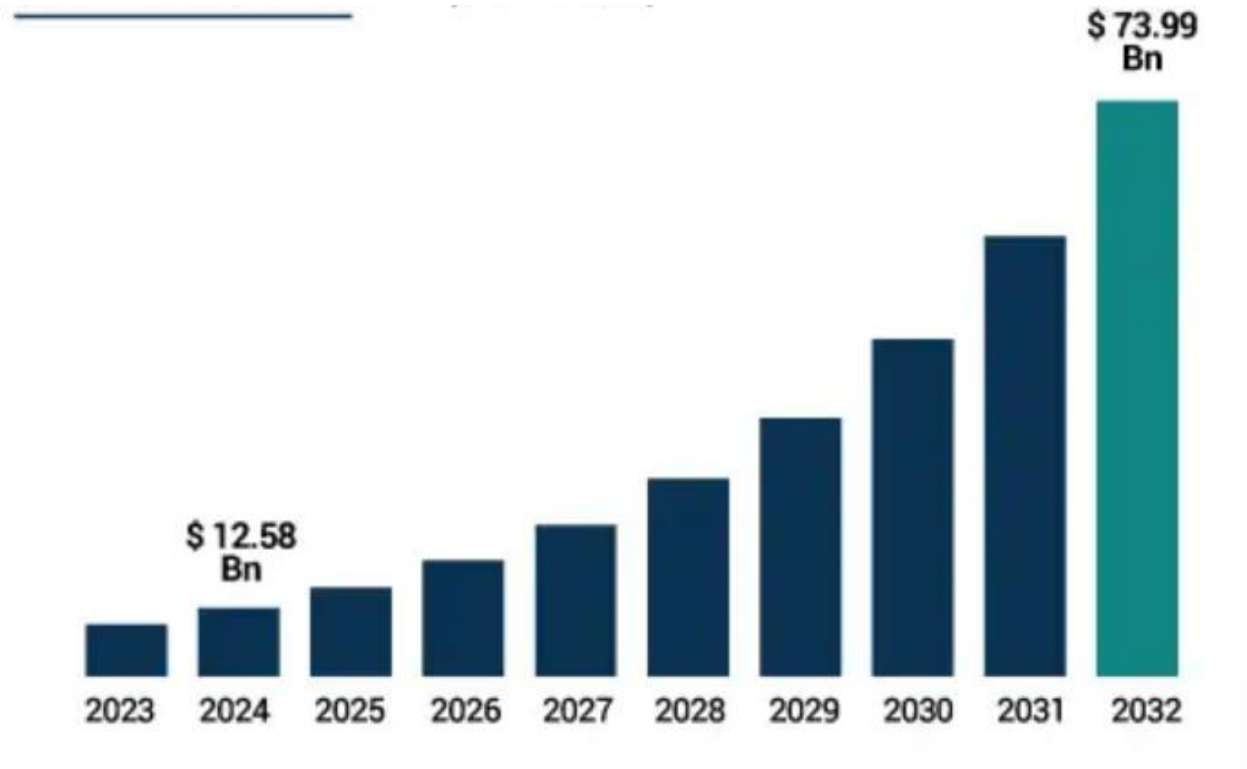


Fig 6: AI For Customer Service Market Size

12. Conclusion

Binaural earphones provide a realistic three-dimensional experience for the user. They can be used for entertainment or relaxation purposes. Because of digitization, it has also become possible to simulate distances by calculating the time difference between sound reaching each ear, and thus enabling the user to spatially pinpoint the origin of the sounds. The spatial audio system, therefore, can provide a virtual recreation of binaural hearing for a particular key position (the sweet spot) using plain stereo headphones. The theory of using head-related transfer (HRTF) functions to recreate binaural hearing is mature, and open-listening binaural audio has been supported in many recent sound ecosystems.Binaural sound processing focuses on creating a dataset of high-fidelity head-related transfer (HRTF) functions for the sound generator, which uses different speakers to present different panoramas to the listener. The support of headphone

3D ensures that the user can experience different positions in a joint sandplay environment. This panoramic video system displays a scene with a left and right stereo view for different users. The visual system captures the movements of the users in the sound-presentation position. Therefore, the user will see different scenes based on their position in the environment. The research conducted the environment design using Google SketchUp and tested it using virtual reality glasses. The result shows that the use of panoramic video and binaural sound processing can enhance the immersive experience of virtual reality applications.

References

1. Sánchez, F. L., Hupont, I., Tabik, S., & Herrera, F. (2020). Revisiting crowd behaviour analysis through deep learning: Taxonomy, anomaly detection, crowd emotions, datasets, opportunities and prospects. Information Fusion, 64, 318–335.
2. Wu, P., Liu, J., Li, M., Sun, Y., & Shen, F. (2020). Fast sparse coding networks for anomaly detection in videos. Pattern Recognition, 107, 107515.
3. Mangalampalli, B. M., Kolla, S. K., Bandi, V. D. V. K., Yandamuri, U. S., & Rani, P. S. (2025). Designing Intelligent Healthcare Ecosystems through Adaptive Data Integration and Autonomous Learning Systems. Vascular and Endovascular Review, 8(20s), 330-347.
4. Tang, Y., Zhao, L., Zhang, S., Gong, C., Li, G., & Yang, J. (2020). Integrating prediction and reconstruction for anomaly detection. Pattern Recognition Letters, 129, 123–130.
5. Nayak, R., Pati, U. C., & Das, S. (2021). A comprehensive review on deep learning-based methods for video anomaly detection. Image and Vision Computing, 106, 104078.
6. Paleti, S., Baliyan, M., Aitha, A. R., Reddy, B. A., Bhadauria, G. S., & Sing, S. A. (2025, August). Graph—LSTM Hybrid Model for Improving Fraud Detection Accuracy in E-Commerce Financial Services. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.
7. Doshi, K., & Yilmaz, Y. (2021). Online anomaly detection in surveillance videos with asymptotic bound on false alarm rate. Pattern Recognition, 114, 107865.
8. Feng, J., Liang, Y., & Li, L. (2021). Anomaly detection in videos using two-stream autoencoder with post hoc interpretability. Computational Intelligence and Neuroscience, 2021, 7367870.
9. Kolla, S. H., & Mangala, N. (2025). DESIGNING AUTONOMOUS LLM AGENT FRAMEWORKS USING GEN AI PIPELINES TO ENHANCE CUSTOMER SERVICE MANAGEMENT AND KNOWLEDGE WORKFLOWS. Lex Localis-Journal of Local Self-Government, 23, 9719-9733.

10. Cob-Parro, A. C., Losada-Gutiérrez, C., Marrón-Romera, M., Gardel-Vicente, A., & Bravo-Muñoz, I. (2021). Smart video surveillance system based on edge computing. Sensors, 21(9), 2958.
11. Ahmed, I., Ahmad, M., Rodrigues, J. J. P. C., & Jeon, G. (2021). Edge computing-based person detection system for top view surveillance: Using CenterNet with transfer learning. Applied Soft Computing, 107, 107489.
12. Mattaparthi, R. (2025). GenAI-Augmented Diagnostic Reasoning for Diesel Engine Fault Triage: A Large Language Model Framework for Technician Decision Support at Scale. Journal of Material Sciences & Manufacturing Research, 6(12), 1.
13. Rameswari, R., Naveen Kumar, S., Aananth, M. A., & Deepak, C. (2021). Automated access control system using face recognition. Materials Today: Proceedings, 45(2), 1251–1256.
14. Bentafat, E., Rathore, M. M., & Bakiras, S. (2021). Towards real-time privacy-preserving video surveillance. Computer Communications, 180, 97–108.
15. Loganathan, R. (2025). AGENTIC AI FRAMEWORKS FOR AUTONOMOUS RISK DETECTION AND COMPLIANCE REMEDIATION IN ENTERPRISE DATA CENTER OPERATIONS. Lex Localis-Journal of Local Self-Government, 23 (S6), 9672–9697.
16. Ye, M., Shen, J., Lin, G., Xiang, T., Shao, L., & Hoi, S. C. H. (2022). Deep learning for person re-identification: A survey and outlook. IEEE Transactions on Pattern Analysis and Machine Intelligence, 44(6), 2872–2893.
17. Behera, N. K. S., Sa, P. K., Bakshi, S., & Padhy, R. P. (2022). Person re-identification: A taxonomic survey and the path ahead. Image and Vision Computing, 122, 104432.
18. Wei, W., Yang, W., Zuo, E., Qian, Y., & Wang, L. (2022). Person re-identification based on deep learning—An overview. Journal of Visual Communication and Image Representation, 82, 103418.
19. Mangalampalli, B. M., Bandi, V. D. V. K., Kolla, S. K., & Kumar, M. V. K. (2025). Towards Self-Evolving Healthcare Intelligence: Integrating Advanced Learning Systems with Real-Time Clinical Data Pipelines. Cultura: International Journal of Philosophy of Culture and Axiology, 22(12s), 464-486.
20. Gaikwad, B., & Karmakar, A. (2022). End-to-end person re-identification: Real-time video surveillance over edge-cloud environment. Computers & Electrical Engineering, 99, 107824.
21. Khan, S. W., Hafeez, Q., Khalid, M. I., Alroobaea, R., Hussain, S., Iqbal, J., Almotiri, J., & Ullah, S. S. (2022). Anomaly detection in traffic surveillance videos using deep learning. Sensors, 22(17), 6563.
22. Mangalampalli, B. M., & Kolla, S. K. (2025). Large Language Models for Automated Healthcare Data Dictionary Generation and Maintenance. Vascular and Endovascular Review, 8(20s), 363-375.

23. Fan, Z., Yi, S., Wu, D., Song, Y., Cui, M., & Liu, Z. (2022). Video anomaly detection using CycleGAN based on skeleton features. Journal of Visual Communication and Image Representation, 85, 103508.
24. Maqsood, M., Yasmin, S., Gillani, S., Bukhari, M., Rho, S., & Yeo, S.-S. (2023). An efficient deep learning-assisted person re-identification solution for intelligent video surveillance in smart cities. Frontiers of Computer Science, 17(4), 174329.
25. Mahadevan, S. (2025). DRIVING SUSTAINABILITY IN AUTO & MANUFACTURING SECTORS: THE ROLE OF CLOUD-BASED SERVERLESS AUTOMATION FOR ERP SYSTEMS. International Journal of Applied Mathematics, 38(7s), 1813-1825.
26. Villegas-Ch, W., & García-Ortiz, J. (2023). Authentication, access, and monitoring system for critical areas with the use of artificial intelligence integrated into perimeter security in a data center. Frontiers in Big Data, 6, 1200390.
27. Singh, A., Bhatt, S., Nayak, V., & Shah, M. (2023). Automation of surveillance systems using deep learning and facial recognition. International Journal of System Assurance Engineering and Management, 14(Suppl. 1), 236–245.
28. Kolla, S. K., & Reddy, V. A. R. (2024). Evaluating Cloud-Native vs. Hybrid Architectures for Health Benefit Administration Systems. International Journal of Medical Toxicology and Legal Medicine, 27(5), 1042-1053.
29. Duong, H.-T., Le, V.-T., & Hoang, V. T. (2023). Deep learning-based anomaly detection in video surveillance: A survey. Sensors, 23(11), 5024.
30. Pattnaik, I., Dev, A., & Mohapatra, A. K. (2023). A face recognition taxonomy and review framework towards dimensionality, modality and feature quality. Engineering Applications of Artificial Intelligence, 126, 107056.
31. Kalisetty, S., & Inala, R. (2025). Designing Scalable Data Product Architectures With Agentic AI And ML: A Cross-Industry Study Of Cloud-Enabled Intelligence In Supply Chain, Insurance, Retail, Manufacturing, And Financial Services. Metallurgical and Materials Engineering, 86-98.
32. Lee, J.-W., & Kang, H.-S. (2024). Three-stage deep learning framework for video surveillance. Applied Sciences, 14(1), 408.
33. Duja, K. U., Khan, I. A., & Alsuhaibani, M. (2024). Video surveillance anomaly detection: A review on deep learning benchmarks. IEEE Access, 12, 164811–164842.
34. Mahadevan, S. (2024). Intelligent Serverless Process Automation for Scalable Cloud Operations and Dynamic Resource Optimization. Journal of Computational Analysis and Applications (JoCAAA), 33(06), 4207-4221.

35. Hussain, A., Ullah, W., Khan, N., Khan, Z. A., Kim, M. J., & Baik, S. W. (2024). TDS-Net: Transformer enhanced dual-stream network for video anomaly detection. Expert Systems with Applications, 255, 124846.
36. Elmetwally, A., Eldeeb, R., & Elmougy, S. (2025). Deep learning based anomaly detection in real-time video. Multimedia Tools and Applications, 84, 9555–9571.
37. Huang, C., Li, Q., & Zhang, B. (2025). Prototype-guided and dynamic-aware video anomaly detection. Neural Networks, 189, 107583.
38. Mangala, N., & Kolla, S. H. (2025). Real-Time Feature Engineering for Streaming AI Workloads Using PySpark and Azure Event Hubs. International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management, 1(6), 93-105.
39. Li, N., Yang, X., Chen, T., Wang, T., & Ji, G. (2025). Applying usability assessment method for surveillance video anomaly detection with multiple distortion. Journal of Visual Communication and Image Representation, 108, 104417.
40. Lin, N., Ding, Y., & Tan, Y. (2025). Optimization design and application of library face recognition access control system based on improved PCA. PLOS ONE, 20(1), e0313415.
41. Hsieh, W.-B. (2025). BF-ACS—Intelligent and immutable face recognition access control system. IET Information Security, 2025(1), 6755170.
42. Nagubandi, A. R. (2024). Breakthrough Real-Time AI-Driven Regulatory Intelligence for Multi-Counterparty Derivatives and Collateral Platforms: Autonomous Compliance for IFRS, EMIR, NAIC, SOX & Emerging Regulations. Journal of Information Systems Engineering and Management, 9(4).
43. Hemavathi, S., & Chakravarthi, R. (2025). AI-powered security and attendance management system using deep learning and facial recognition. Journal of Information Systems Engineering and Management, 10(35s), 372–381.