International Journal of Information Security (2026) 25:57
https://doi.org/10.1007/s10207-026-01228-y

REGULAR CONTRIBUTION

Security and privacy in complex, context-aware systems: a comprehensive framework

Antoni Martínez-Ballesté[1] · Edgar Batista[1] · Elena Figueroa[1] · Kaouther Nouni[1] · Agusti Solanas[1] · Fran Casino[1]

Received: 17 December 2025 / Accepted: 1 February 2026 / Published online: 19 February 2026
© The Author(s) 2026

Abstract
Context-aware systems integrate environmental and user-related data to deliver intelligent and adaptive services. Their rising complexity, driven by advances in sensing technologies, Artificial Intelligence (AI), and the Internet of Things (IoT), introduces significant security and privacy challenges. This article presents a framework for the development and assessment of secure, privacy-preserving context-aware systems. Using the ISO/IEC 27002 standard as a foundation, we categorize and analyze common threats and propose a set of comprehensive protection strategies to guide the secure design of context-aware architectures. We further emphasize privacy-preserving practices aligned with ISO/IEC 27701 and the GDPR. To illustrate the applicability of the proposed framework, the smart classroom is presented as a representative example of a complex context-aware environment. The feasibility of implementing the proposed strategies is examined in light of the technological diversity that characterizes such ecosystems. Finally, we discuss the implications of emerging standards, such as ISO/IEC 27090, the European Union AI Act, and the NIST AI Risk Management Framework, and outline future research directions related to enhancing the medium-term resilience of context-aware systems.

Keywords Context-Aware Systems · Smart Classrooms · Information Security · Privacy Preservation

1 Introduction

In an increasingly interconnected world, the ability of systems to intelligently adapt to their surroundings has become essential. From personalized digital assistants to complex, intelligent environments, systems that understand and respond to their nearby environment are reshaping how users interact with technology. The latter is leveraged by context-aware systems, which use contextual information to provide services. Context is commonly defined as "any information that can be used to characterize the situation of users" [15]. This includes data such as user identity, location, time, and other data typically obtained through sensors and IoT devices deployed throughout the operational environment [46]. By acquiring and modeling such data, context-aware systems use reasoning mechanisms to intervene in particular situations through autonomous decisions or by providing recommendations to users [60]. Examples include a simple application that guides visitors through a museum based on their preferences and real-time location, or a climate control system that automatically adjusts air conditioning based not only on the current room temperature but also on the presence of people.

As sensing technologies and computational resources become increasingly ubiquitous, context-aware systems are evolving toward higher degrees of complexity and sophistication [51]. In this scope, novel paradigms within the "smart" ecosystem have emerged, giving rise to advanced applications in domains such as smart cities [53], smart healthcare [55], and smart industry [26], where systems must continuously adapt to dynamic environments to deliver personalized, efficient, and context-driven services.

However, the heterogeneity of devices, platforms, and communication protocols within complex context-aware systems introduce significant challenges, particularly with respect to interoperability, scalability, and data consistency, among others. A structured approach to effectively manage these challenges involves distributing data collection and context modeling across multiple data collecting agents (DCAs). These agents are software entities responsible for

✉ Edgar Batista
edgar.batista@urv.cat

[1] Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Av. Països Catalans 26, 43007 Tarragona, Catalonia, Spain

acquiring, aggregating, and modeling contextual information from the environment. DCAs operate on diverse hardware platforms, ranging from resource-constrained single-board computers (*e.g.,* Raspberry Pi) to online information systems (*e.g.,* cloud-based infrastructures). Communication among these agents occurs through local area networks, either wired or wireless, potentially involving application-layer APIs hosted in the cloud. By adopting standardized communication models, such as ontology-based representations, these systems can enable consistent semantic interpretation of data across diverse domains, enhancing interoperability and supporting more robust, context-aware decision-making [4].

Several aspects are critical to ensuring context-aware systems' proper functioning and reliability. For instance, the security, accuracy, and availability of contextual data must always be maintained. Any breach, alteration, or loss can result in incorrect system behavior, operational failures, or flawed decision-making. Moreover, since contextual data often include sensitive information (*e.g.,* health records, video footage,…), strong privacy protection mechanisms are essential to safeguard users' privacy and ensure compliance with legal and ethical requirements [54].

Contribution and plan of the article

Despite the rapid expansion of context-aware systems, the deployment of effective security and privacy measures typically remains at the discretion of system developers. In practice, there is a lack of standardized frameworks or methodologies that offer a systematic and comprehensive approach to cybersecurity assessment and mitigation tailored to context-aware systems. Existing efforts often address isolated technical components, overlooking the broader organizational, human, and regulatory dimensions that shape the trustworthiness of these systems. In this article, we present a framework for the development and assessment of secure and privacy-preserving complex context-aware systems, aimed at both practitioners and policymakers. To the best of our knowledge, this is the first work to explicitly map the security challenges of context-aware systems to the ISO/IEC 27002 standard while also discussing their interplay with emerging paradigms such as contemporary AI regulation.

To illustrate our theoretical framework in a realistic and application-relevant setting, we adopt the smart classroom as a representative use case of a complex, context-aware system.

The rest of the article is structured as follows: Section 2 introduces the smart classroom concept, and provides background on related previous work on security and privacy frameworks in context-aware systems. Section 3 examines the key security and privacy challenges that arise in such systems. Next, Section 4 presents strategies specifically tailored to mitigate these challenges, whose implementation feasibility is discussed in Section 5. Finally, Section 6 concludes the article with some final remarks and future research directions.

2 Background

This section introduces the smart classroom concept and its mapping to a complex, context-aware system. Additionally, it analyses previous work on security and privacy frameworks in context-aware and smart systems.

2.1 Smart classrooms

The education sector has made remarkable progress with integrating information and communication technologies (ICT), revolutionizing traditional teaching and learning practices. This has opened the door to novel learning environments: smart classrooms, complex, intelligent systems that provides teachers with timely and relevant insights to support informed and responsive decision-making [59].

Context-aware systems embedded in smart classrooms can enhance teaching efficiency by optimizing classroom conditions and supporting educators. For instance, by continuously monitoring air temperature, humidity, and CO_2 concentration, these systems can automatically regulate air quality and thermal comfort [9]. In parallel, student attentiveness and emotional states can be inferred using either computer vision techniques [43, 45] or biometric wearables [5].

Example Scenario Although there are different, sometimes fragmented or non-homogeneous interpretations of what constitutes a smart classroom, in this article we define this environment as a complex context-aware system [38], which allows for different configurations considering *e.g.,* regions, culture and scope. In the following, we present an illustrative example of a smart classroom ecosystem, which serves as the foundation for identifying the threats that may compromise such systems. This example is illustrated in Figure 1.

The smart classroom infrastructure consists of an ecosystem of hardware and software components designed to collect and process information relevant to the teaching and learning process. This information is formally represented through a smart classroom ontology, which defines the relationships between different sources of data. DCAs are organized in a hierarchical master–slave configuration, particularly when multiple units of the same type are deployed within the classroom. In this architecture, slave DCAs collect raw data and forward them to a master DCA, which aggregates the data, monitors the performance of slave units, and transmits high-level information to the Smart Classroom Central Server (SCCS), which includes the smart classroom data warehouse. To support context reasoning, statistical summaries

or ontology-aligned information are transmitted instead of raw microdata.

DCAs can be integrated into the smart classroom to monitor environmental conditions. For example, environment monitoring units (DCA_e) are deployed at specific locations to measure air quality. These units include sensors for temperature, humidity, CO_2 concentration, and pollutant levels, all managed by a single-board computer. Similarly, noise monitoring units (DCA_n) use a microcontroller connected to a microphone to capture ambient noise levels and assess classroom acoustics. Additional context-aware DCAs, such as those for monitoring lighting or detecting whether windows or doors are open, can also be implemented, though they are not detailed in this example for brevity.

Beyond environmental data, more sophisticated monitoring is handled by a behavior monitoring unit (DCA_b), which leverages machine learning techniques to detect and interpret classroom dynamics, *e.g.,* estimating the number of students present, detecting visual attention directed at the teacher, recognizing student participation (*e.g.,* hand-raising), and tracking the teacher's movements (*e.g.,* actively moving, remaining still…). To achieve this, the video controller (DCA_v) processes video feeds with gesture recognition and pose estimation models from a network of cameras strategically placed in the classroom. To complement these data, physiological signals are gathered using wearable smart bracelets worn by students and teachers. These signals are aggregated by the wearable controller (DCA_w), which collects biometric data to assess affective states such as stress or disengagement.

In addition to physical monitoring, several DCAs interfere with digital information systems relevant to classroom activities. For instance, the online learning analyzer (DCA_o) gathers data from online learning platforms, such as learning management systems or subject-specific platforms for maths or physics. This DCA_o communicates with these systems via APIs and, similar to the monitoring units, may apply artificial intelligence (AI) techniques before transmitting synthesized insights to the SCCS. Additionally, we also consider a classroom annotation system (DCA_a), a collaborative digital platform that allows teachers to log classroom observations, track students progress, organize notes, and record assessments. Together, all these DCAs provide high-level, processed information to the SCCS, enabling context reasoning and supporting real-time decision-making to optimize the learning process.

The smart classroom infrastructure uses a combination of both wired and wireless LANs. Specifically, environmental and noise monitoring units communicate over a wireless LAN in infrastructure mode thus requiring the use of an access point, while master units are also connected to the wired network. The SCCS, the behavior monitoring unit, and the back-ends of the classroom annotation and online learning analyzer systems also rely on wired connectivity to ensure reliable data transmission and system coordination.

Finally, our example smart classroom ecosystem considers two main user roles:

- Teachers, who interact with the system entirely through the smart classroom teacher assistant [59]. This user-friendly tool allows them to gain actionable insights during classroom sessions, obtain indicators derived from learning analytics, and perform basic setup tasks. For instance, through the assistant they receive alerts when certain conditions are met, such as prolonged exposure to high noise levels or a noticeable drop in student attentiveness. The system is designed to remain accessible to teachers with basic technical skills by incorporating explainability features and enriched human–computer interaction mechanisms [58]. Moreover, we assume that teachers receive initial mentoring as part of their role to ensure effective and confident use of the assistant.
- A designated system administrator (for whom the necessary technical skills are assumed) sets up and maintains both hardware and software components, ensuring the continuous operation of the system, and provides technical support to teachers as needed.

2.2 Previous work

Context-aware systems inherently rely on continuous sensing, processing, and reasoning over user-centric and environmental data. This makes them highly susceptible to security vulnerabilities and privacy breaches, particularly when deployed in open, dynamic, and heterogeneous environments such as smart cities, smart healthcare, or smart classrooms.

Several studies have proposed strategies to address context-aware systems' security and privacy challenges. From a general perspective, Temdee et al. [57] identified common security threats in context-aware applications operating over TCP/IP, such as routing attacks and man-in-the-middle attacks, and recommended the use of cryptographic primitives and authentication protocols to secure wireless sensor networks (WSN). Al-Muhtadi et al. [1] introduced a lightweight cybersecurity framework tailored for pervasive computing environments. Their approach focuses on securing interactions between context producers and consumers through encrypted communication, trusted certificates, and fine-grained access control mechanisms, thereby ensuring the confidentiality and integrity of contextual data. Focusing on smart home environments, Almusaylim et al. [2] provided a comprehensive review of security and privacy issues related to IoT devices and context-aware systems. By comparing existing approaches from the literature, the authors

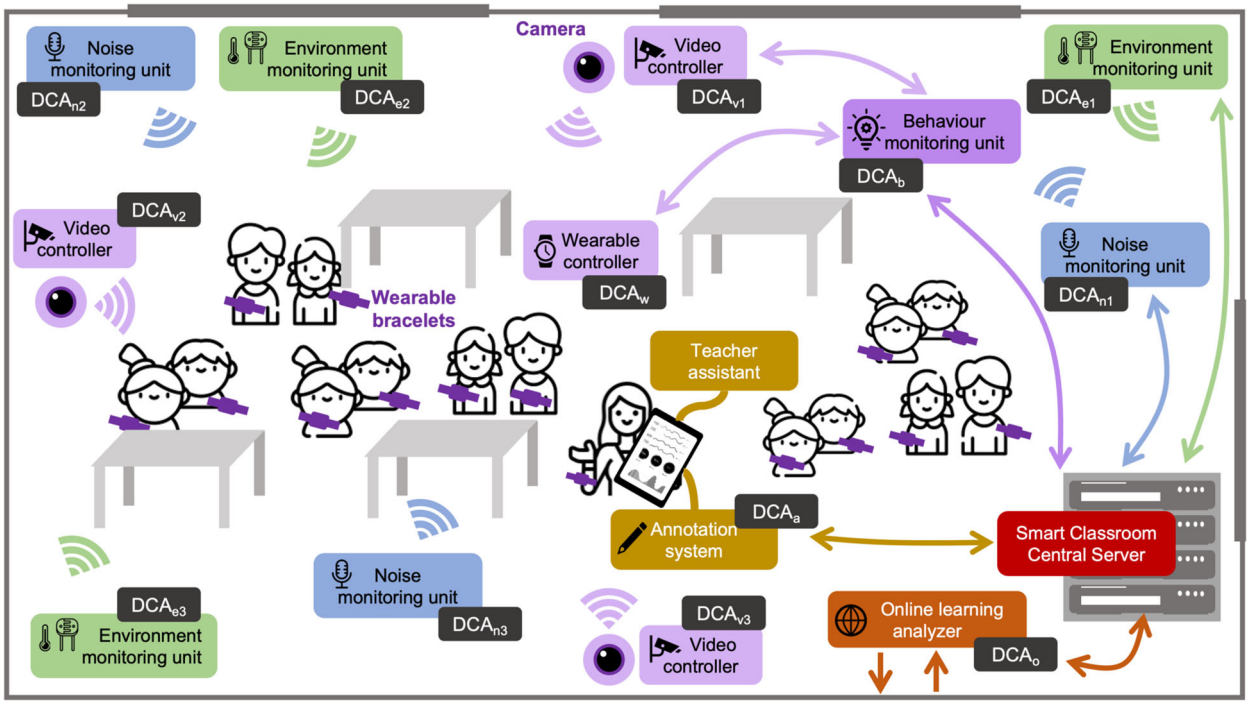


Fig. 1 Example of a smart classroom as a complex, context-aware system.

critically analyzed current solutions to protect these systems from cyber threats. In the domain of smart healthcare, Batista et al. [6] conducted a detailed review of vulnerabilities affecting context-aware systems, particularly those relying on WSN and wireless body area networks (WBAN). They proposed a general-purpose taxonomy for classifying attacks based on their targets and emphasized the importance of secure data transmission, protected storage, as well as the implementation of privacy-preserving mechanisms to build trustworthy systems. Within the context of smart classrooms, Dimitriadou et al. [17] highlighted the importance of addressing ethical aspects related to the use of data in AI-driven educational systems, which may inadvertently reinforce existing biases and lead to discriminatory practices, particularly against minority or underrepresented student groups. As context-aware systems evolve toward more advanced, learning-enabled architectures, commonly referred to as cognitive systems, the risks associated with security and privacy become even more pronounced. These systems rely on accurate and unaltered data to produce fair and unbiased behavior. Theoretical analyses in domains such as cognitive transportation [25] and cognitive cities [37] have already begun to foresee potential challenges.

In the deployment of complex, context-aware scenarios, security and privacy challenges are closely linked to three key dimensions: (i) the underlying systems and networks, (ii) the data that is acquired, processed, and stored, and (iii) the users who interact with the system. Accordingly, such context-aware systems are expected to adhere to robust security and data privacy policies supported by periodic risk assessments and system audits. The more critical a system is and the more sensitive the data it handles, the stricter the security and management policies that must be enforced. As such, compliance with established international standards, particularly those within the ISO/IEC 27000 family, is essential. The ISO/IEC 27000 series provides a comprehensive framework for information security management. Specifically, ISO/IEC 27002 [31] outlines a set of best practices and recommended controls for ensuring information confidentiality, integrity, and availability. It states that "information security is achieved by implementing a suitable set of controls, including policies, rules, processes, procedures, organizational structures and software and hardware functions". The standard also emphasizes the importance of continuously revising and improving these controls to adapt to evolving threats and system requirements. The security controls defined in ISO/IEC 27002 are organized into four thematic categories: (i) organizational controls, such as policies for information security and incident response procedures, (ii) people controls, addressing aspects like user awareness and remote work security, (iii) physical controls, including security areas and cable security, and (iv) technological controls, which cover access management, activity monitoring, cryptographic practices, and network security. Concerning privacy, ISO/IEC 27701 [29] provides a privacy-focused extension to ISO/IEC 27002. It provides specific

guidelines for implementing a Privacy Information Management System, supporting organizations in managing personal data and aligning with data protection regulations such as the General Data Protection Regulation (GDPR) [19]. The standard includes requirements for privacy risk assessment, data governance, and the implementation of privacy-specific controls to ensure lawful and ethical handling of personal information.

3 Security and privacy challenges

In this section, we examine the security and privacy challenges faced by context-aware systems, using the aforementioned smart classroom scenario as a real-world example. We adopt a classification scheme inspired by previous works in related domains [1, 6] to structure our analysis. Specifically, we categorize threats according to the primary system components involved: (i) DCAs (Section 3.1), (ii) communication channels (Section 3.2), and (iii) information systems within the smart classroom (Section 3.3). This actor-based perspective enables a comprehensive yet practical analysis of vulnerabilities in complex, context-aware environments. It is important to note that the proposed classification is not exhaustive, nor does it aim to define a universal taxonomy. Instead, it is a context-specific and illustrative framework highlighting common attack patterns within our scenario. Additionally, the boundaries between categories are not always clear, and certain threats may span multiple components or intersect across different system dimensions.

3.1 Attacks on DCAs

DCAs are exposed to various threats that can compromise the integrity and reliability of the contextual data they collect and transmit.

Node Compromise This attack refers to the unauthorized control of a device hosting a DCA, which may occur through physical tampering or remote exploitation of vulnerabilities. Typically, DCAs are often deployed on resource-constrained devices, such as microcontrollers or single-board computers, which may lack strong security mechanisms. For instance, an attacker with physical access to a noise monitoring unit could disable or reprogram DCA_{n3}, suppressing noise level reports and bypassing alert mechanisms. Alternatively, if DCA_{e1}, the master environmental agent, runs outdated software or exposed services, an attacker could exploit a vulnerability remotely to gain unauthorized access. Once compromised, the attacker can launch further attacks within the classroom network, such as those described below.

False Data Injection This kind of attack involves deliberately inserting false or manipulated data into the system with the ultimate goal of misleading the context inference mechanisms. This could relate to spoofed data streams sent by DCA_{e2}, a slave unit responsible for environmental sensing. The attacker may inject artificially high temperature or CO_2 readings, prompting unnecessary ventilation actions or triggering false alerts for the teacher. In more subtle situations, forged physiological data could be sent by DCA_w, simulating high stress levels and leading to inappropriate interventions.

Malicious Code Injection Another significant threat is when the attacker remotely or physically installs unauthorized software onto DCAs. This type of attack can be used to alter the normal behavior of a component, leak sensitive data, or create persistent backdoors. For example, if DCA_{n1}, which manages noise data aggregation, is compromised with malicious firmware, it could falsify noise readings. Similarly, an attacker targeting DCA_{v1}, responsible for behavior analysis using camera streams, might inject code that disables certain detection features, such as attention or movement tracking, compromising the understanding of classroom dynamics.

Denial of Service via Sleep Deprivation Denial of Service (DoS) attacks targeting energy efficiency are particularly relevant in context-aware systems with limited resources, *e.g.,* battery-powered devices. Particularly, in the example of sleep deprivation, the attacker repeatedly triggers a DCA to prevent it from entering low-power modes, eventually depleting its resources and disrupting its normal operation. For instance, DCAs in noise monitoring units are vulnerable to this attack. An attacker could keep these DCAs active indefinitely and exhaust their battery by continuously sending fake data requests or spoofed network pings.

3.2 Attacks on communication channels

Communication channels represent a critical attack surface in context-aware systems. These channels are particularly vulnerable in complex network environments, where a hybrid networking setup is often used. While wired connections offer greater protection through physical security and reduced exposure, wireless communication channels are inherently more susceptible to interception, interference, and spoofing. Attacks on communications can compromise the confidentiality, integrity, and availability of contextual information.

Eavesdropping Eavesdropping is a passive attack in which an adversary intercepts data as they travel through the network, aiming to access sensitive personal information without altering it. For example, DCA_n gather individuals' voices, DCA_v record video footage that can identify students and teachers, and DCA_w collect physiological data. Additionally, the SCCS stores student-related data, including personal details, social information, and medical conditions. If an attacker gains access to these data, they could transmit them to unauthorized external servers and use them for harmful purposes like blackmail or ransomware attacks, creating

serious privacy risks. For instance, a teacher's privacy could be compromised if recordings of their activities are made public.

Data Tampering This attack refers to the unauthorized modification of information while it is being transmitted across communication channels. If an attacker gains access to the network and intercepts traffic between a DCA and the SCCS, they could alter sensor values or behavior analysis results in transit. For example, modifying data sent by DCA_{e1} might cause the SCCS to believe that the classroom air quality is optimal, even if CO_2 levels are dangerously high. This compromises data integrity and can reduce system trust and decision-making accuracy.

Replay Attacks In replay attacks, the attacker intercepts legitimate messages (even encrypted) and re-sends them later to mislead the SCCS behavior and force it to take unnecessary actions. For example, an attacker could replay previously recorded temperature readings to simulate a comfortable environment and prevent proper ventilation. Similarly, replaying old biometric data from DCA_w might mislead the system into interpreting student stress as normal, so cognitive overload or anxiety periods have been omitted.

Spoofing Spoofing involves impersonating a legitimate network entity to inject false information or gain unauthorized access. An attacker could spoof the identity of an environmental DCA (*e.g.,* DCA_{e2}) and send forged data to the master unit DCA_{e1}. Consequently, the aggregated values sent to the SCCS are corrupted. More critically, spoofing DCA_v or DCA_w could allow an attacker to inject fabricated behavioral or physiological data to disrupt student monitoring features.

Flooding This type of DoS attack disrupts system functionality by overwhelming a target element (*e.g.,* DCA, SCCS) with excessive requests. Common techniques include TCP SYN floods (unfinished TCP handshake requests) and ping floods (high rate of ICMP echo requests). The impact of these attacks varies: flooding the SCCS can disrupt the entire system, while targeting other DCAs may cause more localized failures. Specifically, attacks DCAs within master units blocks contextual data from reaching the SCCS, leading to decisions made without full awareness of the contextual situation. In contrast, targeting DCA monitoring unit results in partial data loss, reducing the system's accuracy without completely disabling its functionality. In addition to targeting internal components, an attacker may launch DoS attacks from DCA_o against external online learning platforms. By sending an excessive number of automated requests to these platforms through the authenticated API access, an attacker can overload remote servers. This type of attack not only disrupts the local system but impacts multiple users and services who depend on the affected online learning platform.

Jamming Attacks This attack relies on jamming the wireless network. Unlike traditional DoS attacks that flood a system with excessive traffic, jamming attacks emit interference signals that disrupt wireless communications, preventing devices from transmitting data. Since jamming directly affects the physical communication channel, it makes communication unreliable and severely impacts system performance.

3.3 Attacks on information systems

The information systems in a smart classroom, such as the SCCS, the annotation system and the online learning analyzer, are responsible for aggregating, storing, and reasoning over context data. Unlike distributed sensor nodes or communication channels, these systems typically have higher computing power and broader access privileges, making them particularly attractive targets for attackers. Although they are often deployed on more robust platforms (*e.g.,* PCs or servers), their physical and logical exposure in a school environment increases their vulnerability.

Physical Attacks The physical infrastructure, *i.e.,* computers, cabling, and networking equipment coexist with users, objects, and furniture. This setting inherently lacks the physical protections in controlled environments like data centers, making critical infrastructure vulnerable to accidental or intentional physical damage. Even a minor incident, such as unplugging a cable, knocking over an access point, or displacing a desktop unit, can result in partial or complete service disruptions. For instance, if a student unintentionally disconnects the SCCS from the network, the entire system's functioning is interrupted.

User Impersonation User impersonation involves an attacker gaining unauthorized access by posing as a legitimate user, either by stealing credentials or exploiting weaknesses in the authentication process. If an attacker impersonates the system administrator, they could disable critical services, delete system components, or alter DCA configurations, leading to a complete DoS or irreparable system corruption. Even impersonation of a regular teacher or student carries significant risks, such as unauthorized access to sensitive data, manipulation of historical classroom records, or the reconfiguration of system parameters (*e.g.,* deactivating sensors or altering thresholds). Such attacks may result in data alteration, unauthorized disclosure, or loss of trust in the system's output.

Malware Infection Interactions with external platforms or removable storage devices expose information systems to malware infections, which can spread across interconnected classroom systems. An attacker could exploit vulnerabilities in components like the online learning analyzer or SCCS to install malicious software, such as ransomware, keyloggers, or remote-access trojans. Once deployed, the malware may silently exfiltrate sensitive information, alter system behavior, or provide persistent unauthorized access to the attacker.

For instance, ransomware on the SCCS could encrypt critical data and inference models, making the system unusable until a ransom is paid.

4 Proposed framework

Protecting complex, context-aware systems requires a comprehensive approach that secures the underlying technology and incorporates organizational policies that prioritize security and privacy. As mentioned in Section 1, the ISO/IEC 27002 standard provides a broad range of controls that extend beyond purely technological recommendations. Moreover, security and privacy are inherently interrelated: insufficient security may expose private data to misuse or unauthorized access, while data breaches can compromise the privacy rights of the involved actors.

Before detailing the specific strategies, we provide a structured overview of the different protection dimensions addressed by our framework. As illustrated in Figure 2, the proposed approach maps common attacks in context-aware environments to the ISO/IEC 27002 controls best suited to mitigate them. This mapping serves as a visual summary that groups the key recommendations and helps practitioners quickly identify which controls are relevant for particular threats.

To guide the reader through the more detailed analysis that follows, we organize the protection strategies into five complementary dimensions:

- *Data Protection* focuses on how confidentiality, integrity, and availability of contextual data are ensured through cryptographic mechanisms, secure storage, and authenticated communication.
- *Network Protection* addresses the safeguarding of both wired and wireless communication channels and the segmentation of network domains.
- *Infrastructure Protection* emphasizes the physical and operational security of deployed devices and equipment.
- *User Protection* covers authentication, awareness, and the mitigation of human-centric threats.
- *Privacy Protection* introduces GDPR-aligned practices such as data minimization, pseudonymization, and broader privacy-by-design principles.
- Finally, several complementary *Supporting Operational Strategies*, primarily aimed at system administrators, are presented to ensure consistent and resilient system operation.

Together, these dimensions provide a coherent structure for understanding how different threats interact with the layers of the context-aware system, while Figure 3 complements this view by illustrating how security measures integrate with the contextual system architecture.

4.1 Data protection

Ensuring the confidentiality, integrity, and availability of contextual data is central to the secure operation of context-aware systems. A widely adopted strategy to achieve this is through the use of cryptographic functions throughout the system architecture. Specifically, Control 8.24 (Use of Cryptography) recommends the adoption of cryptographic tools to protect the confidentiality, authenticity and integrity of data.

Data protection measures can be divided into two categories: protection at rest and protection in transit. To mitigate risks such as eavesdropping or unauthorized access, it is essential to store and transmit encrypted versions of data records. However, encryption should be applied selectively, targeting only those data records classified as sensitive. In this regard, ISO/IEC 27001 [30] defines sensitive data as "information that must be protected from unavailability, unauthorized access, modification, or public disclosure due to potential adverse effects on an individual, organization, national security, or public safety". Accordingly, Control 5.12 (Classification of Information) recommends identifying and understanding the protection requirements of information based on its relevance to the organization. For data at rest, encryption algorithms based on symmetric block ciphers offer strong protection. To protect against unauthorized alterations, cryptographic authentication codes generated using secure hash functions can verify that the has not been tampered with. Similarly, digital signatures based on public-key cryptography (PKI) further ensure proof of data authenticity and integrity. In scenarios involving secure key exchange or authentication processes, public-key certificates enable both encrypted communication and entity verification, thereby supporting both non-repudiation and authentication.

4.2 Network protection

Network-level security is essential for maintaining the integrity of communication between system components. While modern wireless networks often incorporate robust security mechanisms, such as credential-based authentication and digital certificates, wired networks can present greater vulnerabilities, as physical access to network ports may allow attackers to inject malicious traffic, turning wired infrastructure into a potential entry point for exploitation. To address these risks, Control 8.20 (Networks Security) emphasizes appropriate management, monitoring, and coordination of the network to protect information. Specifically, Control 8.22 (Network Segregation) involves segmenting networks into isolated, secure zones to prevent an attacker from easily propagating within the infrastructure. By enforcing strict

Target	Attack	Data protection	Network protection		Infrastructure protection		User protection		Privacy protection	
DCAs	Node compromise		IDPS	Segment.		Integrity checks	MFA		Cryptographic erasure	Pseudonyms
	False data injection	HMAC							Purge data	
	Malicious code injection	Digital Signatures				Integrity checks			Purge software	
	DoS via sleep deprivation		FW rate limiting				Restricted API access			
Communication Channels	Eavesdropping	AES	WPA3, TLS, DTLS	Segment.						Pseudonyms
	Data tampering	DS, HMAC							Purge data	
	Replay attacks	Nonces, timestamps								
	Spoofing	PKI								
	Flooding		FW rate limiting	Segment.						
	Jamming attacks		Channel hopping		Shielded enclosures					
Information Systems	Physical attacks			Segment.	Tamper-evident seals		MFA	Physical security policies		PS mapping separate and secure
	Impersonation	Digital Signatures	ACLs					Training and awareness		
	Malware infection		IDPS							
		Control 8.24	Control 8.20	Control 8.22	Control 7.8	Control 7.13	Control 8.5	Control 6.3	Control 8.10	GDPR

Fig. 2 Proposed framework to secure complex, context-aware systems. Abbreviations: HMAC: Hash-based Message Authentication Code; DS: Digital Signatures; AES: Advanced Encryption Standard; PKI: Public Key Infrastructure; IDPS: Intrusion Detection and Prevention Systems; FW: Firewall; WPA3: Wi-Fi Protected Access 3; TLS: Transport Layer Security; DTLS: Datagram Transport Layer Security; ACL: Access-Control List; MFA: Multi-Factor Authentication; API: Application Programming Interface; PS: Pseudonymization; GDPR: General Data Protection Regulation.

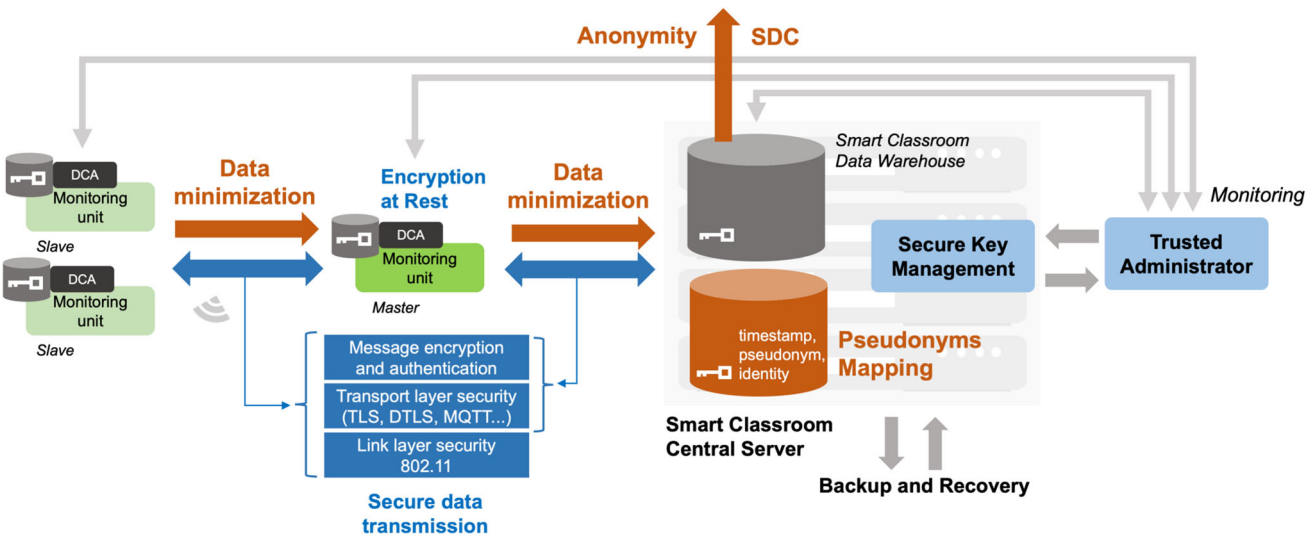


Fig. 3 Application of the framework to the core infrastructure of the smart classroom.

access control between these segments using virtual LANs and firewall technologies, the risk of a single compromised system impacting other critical components is substantially reduced.

From a physical layer perspective, strategies are needed to protect against jamming attacks. Although ISO/IEC 27002 does not explicitly address them, techniques such as channel hopping, redundant transmission paths, and advanced signal processing techniques can help mitigate the impact of interference by making communication more resilient. Some approaches may also involve strengthening signal transmission or implementing redundancy through multiple antennas to reduce vulnerabilities.

4.3 Infrastructure protection

The system's infrastructure comprises a range of essential components, including sensors, cabling, network devices, and servers, deployed throughout the classroom environment, a space where children are actively moving around. In addition to considering the concept of "invisible technology", where devices are seamlessly integrated into the setting, basic protection of equipment is crucial. This ensures that devices remain safe from physical damage and tampering. ISO/IEC 27002 provides guidelines on this matter, specifically in Control 7.8 (Equipment Siting and Protection), which offers recommendations on the appropriate placement and safeguarding of equipment to ensure its security and operational continuity in dynamic environments. Additionally, Control 7.13 (Equipment Maintenance) aims to prevent loss, damage, or compromise of information or interruption of organization's operations due to lack of maintenance. Therefore, the implementation of operational protocols to safeguard the elements of the smart classroom equipment is needed.

4.4 User protection

User protection strategies are focused on preventing impersonation and mitigating human-centric attacks, such as phishing and social engineering. While technical controls play a key role, user awareness and operational discipline are equally important. Control 8.5 (Secure Authentication) emphasizes the adoption of multi-factor authentication (MFA). Combining credentials such as passwords with biometric identifiers or hardware tokens significantly enhances resistance to credential theft. In the smart classroom context, teachers and administrators should authenticate via MFA before initializing any core system functions at the start of the day, ensuring that unauthorized individuals cannot gain access–even in the event of leaked credentials. Additionally, Control 6.3 (Information Security Awareness, Education, and Training) highlights the need to raise awareness towards a security-aware culture. Proper training helps prevent social engineering attacks, enhances users' ability to recognize potential threats, and strengthens the overall security posture of the system.

4.5 Privacy protection

According to ISO/IEC 27002, such data are sensitive and must be handled with strong protections against unauthorized access and disclosure. In context-aware systems, privacy-by-design [13] must be integrated from the earliest stages of development. However, beyond securing sensitive data, effective privacy protection requires implementing broader strategies, described below.

Data Minimization A core principle of GDPR is data minimization, *i.e.,* collecting only the PII strictly necessary for a clearly defined purpose. This means limiting data acquisition to what is essential for system functionality. The DCA-based architecture of context-aware system naturally supports this principle by processing much of the contextual information locally, reducing unnecessary data sharing. Similarly, Control 8.10 (Information deletion) reinforces this approach by requiring that data be securely deleted once it is no longer needed. Secure deletion methods (*e.g.,* cryptographic erasure or electronic overwriting) must be applied in accordance with legal and organizational requirements. Moreover, deletion events should be documented to provide an audit trail.

Use of Pseudonyms To reduce the risk of identifying individuals, pseudonymization techniques should be employed where feasible. Under GDPR, pseudonymization involves replacing direct identifiers with pseudonyms so that data can no longer be attributed to a specific person without additional information. While this can mitigate the impact of data breaches, it is not infallible. Re-identification remains a risk, especially if pseudonymized data are combined with external datasets. Although ISO/IEC 27002 and ISO/IEC 27701 do not explicitly address pseudonymization, its implementation is aligned with the broader goals of privacy protection. To be effective, the mapping between real identities and pseudonyms must be stored securely and separately from the pseudonymized data (see Figure 3 for an example in the SCCS).

4.6 Supporting operational strategies

Several system-wide operational strategies are essential to support the security and resilience of context-aware systems as a whole. For the sake of simplicity, these complementary strategies are not included in Figure 2.

Secure Key Management The effective use of cryptography depends on secure key management, which includes key generation, distribution, storage, rotation, and destruction. Control 8.24 emphasizes the need for robust procedures cov-

ering the entire key life-cycle to prevent unauthorized access and ensure the confidentiality of encrypted data.

Secure Administration Given the complexity of context-aware systems, administration must be tightly integrated with security practices. The system administrator (introduced in Section 2.1), must be regarded as a trusted administrator and, hence, is responsible for enforcing access control policies, maintaining secure configurations, managing encryption and authentication systems, monitoring potential security incidents, and maintaining compliance with security policies. In this line, the system counts with a secure key repository, accessed by software components upon authentication, and complemented by a digital identity life-cycle supporting system. Additionally, the administrator supervises routine security audits, software updates, and incident response. Relevant ISO/IEC 27002 controls include Control 5.15 (Access Control), Control 5.16 (Identity Management), and Control 5.17 (Authentication Information), and Control 5.18 (Access Rights). It is worth noting that the role of system administrator is not intended for a teacher but for a technical specialist. In the case of smart classrooms, this responsibility would typically fall to the team of computer technicians that educational authorities already employ to maintain and manage existing infrastructure.

System Monitoring and Logging Continuous monitoring is essential for the timely detection of problems that could compromise the overall functionality of the system and for preventing potential security issues. In this regard, Control 8.16 (Monitoring Activities) recommends implementing intrusion detection systems (IDS) that analyze logs from event collectors to identify anomalous behavior, such as repeated failed login attempts, unauthorized file modifications, or network scanning activity. Moreover, Control 8.15 (Logging) emphasizes the importance of maintaining detailed logs (potentially stored in the data warehouse) to trace and investigate incidents. Besides monitoring potential intrusions, it is paramount to monitor whether systems are up and running, *i.e.,* detect DoS attacks. Security Information and Event Management (SIEM) systems can help detect these disruptions by monitoring the status of essential components like DCAs and SCCS. Intermittent DoS attacks, however, may require more advanced heuristics due to their sporadic nature.

Vulnerability Management To prevent attacks exploit system weaknesses, Control 8.8 (Management of technical vulnerabilities) encourages organizations to identify, assess, and mitigate vulnerabilities through regular software patching and configuration updates. Vulnerability scanners can assist in detecting known flaws in software and network configurations. However, systems remain vulnerable to zero-day exploits, which pose an ongoing challenge due to their undisclosed nature.

Backup and Recovery Planning A robust backup policy is essential to ensure data availability and recovery following disruptive events, including ransomware attacks. As recommended by Control 8.13 (Information Backup), organizations should maintain encrypted backups, document recovery procedures, and store backup copies offsite. Backup policies should align with the defined Recovery Point Objective (RPO), *i.e.,* the maximum tolerable period of data loss, and Recovery Time Objective (RTO), *i.e.,* the target time to restore system functionality. Lower RPO and RTO values require more frequent backups, faster recovery mechanisms, and greater infrastructure resilience.

5 Discussion

This section discusses the feasibility of implementing the aforementioned protection strategies to enable the deployment of a secure, privacy-preserving context-aware system. For the sake of brevity, the discussion is limited to the main protection strategies. We also provide remarks on our test-bed proof-of-concept implementations of several of these measures. The supporting operational strategies are not addressed here, as they pertain to broader information-system practices rather than to the specific challenges of the context-aware system. Moreover, this section includes a discussion on adoption and the current landscape, particularly in light of emerging AI regulations.

5.1 Reducing data collection: balancing efficiency and privacy

The proposed context-aware system, based on distributed DCAs for data collection, modeling, and management, aligns with the principle of data minimization. Rather than storing large volumes of sensitive information related to students, teachers, and contextual parameters, DCAs locally process raw data into actionable insights. These insights are then transmitted from slave DCAs to a master DCA, which applies statistical methods and lightweight AI models to generate higher-level interpretations before forwarding them to the SCCS. For instance, environment monitoring units are designed to operate on an event-driven basis. Temperature sensors notify the SCCS only when significant fluctuations occur within specific classroom zones. Air quality sensors send alerts only when CO_2 levels exceed predefined safety thresholds. Likewise, noise monitoring units avoid transmitting raw audio; instead, they deliver aggregated data or frequency distributions when necessary. In the case of behavioral monitoring, the system avoids transmitting raw video footage or physiological data. Instead, it uses the system's ontology to extract and send summarized insights, such as "most students are losing attention" or "a specific number

of students appear stressed", preventing the transmission of biometric or visual data. Thus, such a design significantly reduces the overall transmitted data volume, which is particularly beneficial for resource-constrained devices. Moreover, local storage demands remain minimal since only the most recent and relevant information is retained.

We have demonstrated the feasibility of such a data-reduction operation by implementing different DCA-enabled monitoring units specialized in collecting air-quality data, noise-level information, and physiological parameters while operating in a master–slave fashion. These units have been deployed using Raspberry Pi boards and ESP32 microcontrollers, confirming the practicality of the proposed approach in resource-constrained environments [7].

Additionally, these DCAs implement periodic pruning of stored data after a defined retention period, ensuring both storage efficiency and compliance with data retention policies [5]. By embracing this data minimization strategy, the system significantly limits the transmission of PII and, therefore, enhances privacy.

5.2 Securing data storage

To safeguard data from ransomware attacks, it is essential to store data securely. While full encryption of all system data would provide robust protection, it is deemed unnecessary for all data. Encrypting and decrypting data, such as using Advanced Encryption Standard (AES), introduces computational overhead, which can impact performance, particularly for resource-constrained DCAs. Hence, DCAs should use lightweight flavors of AES or alternative lightweight encryption schemes [56].

Data-at-rest protection is implemented through two strategies. The first involves encrypting records within the SCCS before they are stored and decrypting them upon retrieval. While this method secures the data, it may complicate operations, such as performing join queries on encrypted attributes. The second strategy delegates encryption management to the database system itself, simplifying encryption tasks at the application level but ensuring compatibility between the SCCS key repository and the database's key management system.

Data stored in DCAs are assumed to be volatile, meaning they do not persist for extended periods. This temporal limitation reduces the potential impact of data breaches, as the exposure window is relatively short. In our implementations, to further mitigate the risk of unauthorized access, particularly in the event that a DCA is compromised, all locally stored data are encrypted using AES.

5.3 Securing data transmission

We adopt a multi-layered security strategy to ensure the confidentiality and integrity of data transmitted within the context-aware system. At the link layer, communication over wireless LANs may be protected by encryption protocols such as WPA (Wireless Protected Access). However, these mechanisms are insufficient if attackers gain unauthorized access to the wireless LAN. In such cases, higher-layer security becomes essential to maintain end-to-end protection.

To secure transport-layer communications, Transport Layer Security (TLS) [16] can be enabled since it is a well-known approach for securing transport-layer communications, with end-to-end encryption and mutual authentication. While server authentication is common in HTTPS-based systems, mutual authentication is more appropriate, ensuring that both the client and the server verify each other's identities using digital certificates issued by the system's certificate authority. This approach safeguards against various threats, including impersonation, eavesdropping, data tampering, and replay attacks. Cryptographic tools like OpenSSL can be seamlessly integrated into the system to manage key repositories and support TLS-based secure communication, particularly between the SCCS and master DCAs. To reduce latency in time-sensitive applications, independent packet communication (using UDP) may be preferred over connection-oriented transmissions like TCP. In such case, Datagram Transport Layer Security (DTLS) [49] is a suitable alternative. DTLS offers security features equivalent to TLS, including mutual authentication and encryption, and introduces mechanisms to prevent replay attacks, making it well-suited for unreliable or delay-sensitive networks.

At the application layer of master-slave DCA communications, we propose using MQTT (Message Queuing Telemetry Transport) [28], a lightweight messaging protocol specifically designed for constrained devices and unreliable networks. MQTT follows a publish-subscribe model, where slave DCAs publish data to topics managed by a central MQTT broker hosted by the master DCA. For instance, in our smart classroom scenario, DCA_{e1} acts as the broker, managing topics such as temperature and air quality. Slave units, such as DCA_{e2} and DCA_{e3}, act as publishers, sending data to these topics. To protect these communications, MQTT includes native support for authentication and encryption. Slave DCAs must authenticate using their username and password before they are permitted to publish or subscribe to any topic, ensuring that only authorized devices can participate in the system's data exchange.

We recommend integrating public-key cryptography or pre-shared keys to enforce end-to-end message integrity, authentication, and encryption for additional application-layer protection, particularly when transport-layer encryption is unavailable. We have performed proof-of-concept

implementations by modifying device firmware to add a custom security layer that encrypts messages using symmetric keys and appends authentication codes (*e.g.,* HMACs) to each message. In such cases, packet numbering mechanisms are necessary to detect duplicate packets and mitigate replay attacks. The mbedTLS library [3] is particularly well-suited to support application-layer security. It offers cryptographic primitives, such as hashing, digital signatures, and random number generators, optimized for both higher-performance systems and resource-constrained microcontrollers. By using mbedTLS, the system can maintain a consistent security framework even when lower-layer protections fail. Also, the use of Access Control Lists (ACLs) can restrict unauthorized traffic from suspicious IP addresses or limit traffic types.

To ensure trust across the ecosystem, all public keys within the system should be validated through a dedicated public-key infrastructure in the SCCA. This structured approach to key management allows devices to verify identities securely, enabling trustworthy communication across all system components.

5.4 Safeguarding the infrastructure

A critical aspect of context-aware systems is ensuring reliable communication at the physical layer, especially in environments with distributed sensors. Sensor interference, coexistence challenges, and environmentally induced faults can compromise data quality in such systems. These disruptions may cause inconsistencies in the collected data that degrade the system's performance. To mitigate these challenges, techniques such as wireless channel characterization can be employed [11, 47]. This approach helps identify and mitigate interference sources, ensuring more stable and reliable sensor readings once the infrastructure is deployed.

Once the network is deployed, firewalls are key in controlling traffic and safeguarding the system from attacks such as flooding or unauthorized access via open ports. We can distinguish between two main types: (i) packet filtering firewalls, which operate at the network and transport layers aiming to allow or deny packets based on attributes like IP addresses, port numbers, or protocol types, and (ii) application-layer firewalls that inspect packet contents at the application layer, often acting as TLS proxies to analyze encrypted traffic for threats like malware or injected scripts. Tamper-proof routers and firewalls can be deployed on network devices, such as routers that separate the system's wired network from the rest of the school's infrastructure or those that segment internal wireless LANs to isolate different classroom zones. In this context, off-the-shelf routers typically include basic packet filtering capabilities. However, their security depends heavily on proactive management by system administrators who regularly update firmware and close unused ports.

At the endpoint level, host-based firewalls offer another layer of protection by controlling traffic between devices (*e.g.,* SCCS, DCAs…) and the network. Several tools are available for Linux-based systems. In our implementations, we have used iptables, a well-known firewall utility for managing traffic rules, configured with a "deny by default" policy, permitting only explicitly authorized traffic. In addition, rate-limiting was enforced to reduce the risk of flooding attacks. Unfortunately, microcontrollers like the ESP32 and Arduino do not support traditional firewalls. These devices typically run a single application and lack a complete operating system with a network stack. As a result, security must be enforced at the application layer (*e.g.,* with the use of mbedTLS), requiring software to explicitly verify the authenticity of incoming packets before accepting them. This approach ensures security even in the absence of conventional firewall support. To reinforce security, integrity checks can ensure the non-manipulation of the software, configuration files, and data within DCAs.

All things considered, tamper-evident seals serve as a solution for protecting the physical infrastructure from unauthorized access. By clearly indicating any attempts to open or interfere with enclosures containing critical components, such as the SCCS, these seals are a low-cost and visible layer of protection that easily identifies malicious tampering.

5.5 Ensuring privacy and trust

In context-aware systems, privacy management is a key responsibility of the system administrator, who oversees compliance with privacy regulations like GDPR and standards such as ISO/IEC 27002 and ISO/IEC 27701. This role includes implementing privacy policies, ensuring lawful data processing, and responding to potential privacy breaches. Administrators must also guarantee the proper handling of personal data in line with relevant legal and ethical requirements. Ensuring privacy is an essential cornerstone for fostering trust in context-aware systems.

5.5.1 Pseudonyms

In some use cases, data aggregation provides basic privacy protection. In our example scenario, the SCCS aggregates data related to various aspects of the classroom dynamics and the learning process. For example, teachers may receive notifications such as "a specific number of students are inattentive" or "there is excessive noise in the classroom". These generalized insights enable teachers to take immediate action without exposing personal information. However, the system can also gather more granular, sensitive data on individuals, *e.g.,* physiological signals, health indicators, learning outcomes, or socioeconomic background. While valuable for longitudinal studies and institutional assessments, such data

pose a higher privacy risk. To mitigate this, pseudonymization is applied. Each participant is assigned a pseudonym for a defined period (*e.g.,* a school day), ensuring continuity across datasets without revealing actual identities. A secure mapping between real identities and pseudonyms is maintained separately using strong encryption at rest. If an event requires teacher intervention (*e.g.,* a behavioral alert), the system displays the student's real name on the interface but stores only the pseudonym and timestamp in the dataset. This enables later retrieval without persistent exposure of identifiable information.

5.5.2 Disclosure Control

When data are shared externally for research or policy evaluation, pseudonymization alone is insufficient to fully protect against re-identification. Quasi-identifiers, *i.e.,* attributes that are not explicit personal identifiers but may enable re-identification when combined, must be considered. In such cases, statistical disclosure control (SDC) techniques must be applied, including data generalization, suppression, noise addition, and k-anonymity [27, 61]. In a nutshell, data generalization replaces specific values with broader categories to reduce identifiability, while suppression removes or masks sensitive data elements that could lead to disclosure. Noise addition introduces random perturbations to prevent precise re-identification, and k-anonymity ensures that each record is indistinguishable from at least $k - 1$ other records with respect to quasi-identifiers. These techniques help preserve privacy while maintaining the utility of the dataset. However, they introduce a trade-off: increasing privacy often reduces data granularity and usefulness [12]. For example, encryption secures data during transmission and storage but may limit real-time processing unless decrypted. Finding the right balance requires techniques that protect privacy without compromising the system's objectives, such as real-time responsiveness or analytical accuracy. Therefore, we recommend applying SDC techniques only when data are shared externally, not when they remain within the system's protected environment. It is worth mentioning that pseudonymization should not be confused with anonymization. While anonymization irreversibly removes identifiers (making re-identification impossible), pseudonymization merely replaces them, allowing for data linkage and remaining subject to data protection laws [18].

Regarding video and audio processing, privacy risks may arise if the corresponding units are compromised. To reduce this risk, trustworthy privacy-aware video and audio systems can be employed. These systems process data locally within tamper-proofed hardware and encrypt all outputs. Access to raw data is limited strictly to authorized entities possessing the correct decryption keys. Without the key, intercepted data remain unintelligible, thus preserving individual privacy. Examples of these techniques include video encryption ensuring only authorized playback [39, 48], and sound shredding techniques to distort speech content while preserving acoustic features for context recognition [36]. These strategies support privacy-by-design principles and help protect the integrity and confidentiality of multimedia data within systems.

Although we present a general overview of privacy issues in complex, context-aware systems, this does not exclude the possibility that other contextual environments may involve additional privacy concerns [41]. Nevertheless, the perspective provided in this section paves the way for any future extensions.

5.5.3 Raising Awareness

Besides applying recommended privacy-enhancing technologies, raising awareness among stakeholders, is crucial for the successful and wide adoption of context-aware systems. To support awareness, we propose the creation of a privacy management and awareness service (PMAS). This element is responsible for generating documentation that outlines how personal data are collected, processed, and protected, as well as for managing informed consent to ensure that stakeholders are fully aware of data usage and their rights under applicable legislation.

In the context of our example, as new actors (students, teachers, families, administrators, etc.) become involved in the scenario, the PMAS develops customized communication materials and consent forms tailored to the comprehension levels and specific needs of each stakeholder group. It would also be responsible for collecting feedback on data collection and privacy practices, and for providing accessible communication channels through which individuals can exercise their rights. We have implemented a PMAS prototype that leverages large language models to analyze the context-aware scenario and generate awareness materials for diverse stakeholders, as well as technical protection checklists [40]. By increasing transparency and adapting materials to their target, the PMAS promotes both regulatory compliance and stakeholder trust.

5.6 Adoption and current landscape

The practical deployment and adoption of context-aware systems depend on both technical readiness and regulatory compliance. These systems operate at the intersection of AI, pervasive computing, and behavioral data processing, requiring robust frameworks to manage privacy, safety, and fairness. Their widespread integration in sensitive domains such as education necessitates alignment with emerging regulatory trends, standardization efforts, and human-centered design principles.

5.6.1 Regulatory Frameworks

From a legal perspective, the GDPR [19] remains the cornerstone of data protection within the European Union, regulating how personal data may be processed, stored, and shared. Principles such as purpose limitation, data minimization, and accountability are directly applicable to context-aware systems, particularly when handling sensitive information such as emotional states, facial expressions, or behavioral patterns. However, GDPR alone does not fully address the risks introduced by increasingly autonomous, complex, and opaque AI-driven systems. To fill this gap, the EU AI Act adopts a risk-based classification framework [21]. AI systems used in educational environments, especially those involving biometric identification, behavioral monitoring, or autonomous decision-making, are categorized as high risk. This classification triggers stringent obligations concerning data governance, transparency, robustness, and human oversight [20]. At the international level, complementary efforts are found in the NIST AI Risk Management Framework [42], which provides voluntary yet structured guidance for managing AI-related risks across the system lifecycle. Additionally, emerging standards such as ISO/IEC 27090 [33], focused on cybersecurity for AI systems, and ISO/IEC 23894 [32], addressing AI risk management, reinforce the importance of governance, assurance, and technical robustness. Ongoing work within ISO/IEC JTC 1/SC 42 reflects a movement toward harmonized practices for AI-based ambient and socio-technical systems.

Taken together, these regulatory and standardization frameworks raise awareness of the security, privacy, and fairness requirements that AI-enabled systems must fulfill. Their recommendations are intentionally broad and organized around high-level dimensions to ensure applicability across a wide range of AI applications, including relatively simple ones. In contrast, our framework is specifically tailored to complex context-aware ecosystems. It explicitly addresses the characteristic elements of these environments, not only the diverse contextual data types but also the heterogeneous devices, distributed components, sensing infrastructures, and human-centric aspects such as user awareness and operational roles. Our contribution is therefore intended to complement these broader standards by offering a more detailed, domain-specific perspective aligned with the unique challenges of contextual computing environments.

5.6.2 Trustworthy Context-Aware Systems

Adopting context-aware systems is strongly influenced by the degree of trust they inspire among stakeholders, which is not merely a matter of performance or accuracy but emerges from a complex intersection of transparency, fairness, reliability, and contextual sensitivity [22]. Regarding fairness, we acknowledge that potential biases in data collected from the devices in the context-aware system can impact the fairness of decision-making by intelligent systems, and such biases must be carefully considered to ensure equitable outcomes regardless of gender, religion, or other personal attributes.

AI tools must support clear and accountable decision-making processes, especially when influencing academic evaluation, behavioral interventions, or mental health alerts. The latter implies embedding mechanisms for algorithmic transparency and explainability, allowing students and educators to understand the rationale behind system outputs and to contest decisions when needed. In our smart classroom example, fairness and inclusion are critical in mitigating algorithmic bias, particularly when AI systems interact with students from diverse socioeconomic, cultural, and neurodiverse backgrounds. Thus, participatory design ensures that stakeholders such as teachers, students, and families are involved throughout the development lifecycle, leading to solutions that reflect real-world needs and ethical expectations [14, 22]. Such a strategy aligns with the human-centred AI principles advocated by organizations like the OECD and UNESCO.

Context-aware cybersecurity further adds complexity, as highlighted in [10, 24]. Context-aware systems must move beyond static security measures, incorporating dynamic policy enforcement and multimodal sensing to respond to evolving contexts. The latter introduces new dimensions to privacy management, requiring context-tagged metadata and semantic policy evaluation engines. Therefore, integrating aspects such as behavioral monitoring, environmental alerts, and physiological data into security protocols while preserving user privacy and autonomy is critical. Techniques such as adaptive authentication and anomaly detection based on contextual parameters are essential for operational resilience, providing context-aware risk mitigation measures [10]. In that regard, long-term adoption also necessitates cryptographic preparedness. With the emergence of quantum computing, classical encryption schemes face potential obsolescence [35]. Transitioning to post-quantum cryptography (PQC) is a complex socio-technical challenge involving inventory assessment, protocol redesign, and implementation of hybrid cryptographic schemes [34]. For smart classrooms, where sensitive behavioral and educational data may be retained long-term, cryptographic agility and early adoption of NIST-selected PQC algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium [8] are essential to safeguard against future threats.

Finally, institutional readiness plays a critical role in enabling trustworthy deployment. Schools and educational authorities must adopt clear governance frameworks for AI, including ethical oversight, transparency mechanisms, conformity assessments, and digital literacy initiatives. Certification processes and explainability toolkits can empower

educators to engage responsibly with AI-driven technologies while ensuring systems adhere to legal and ethical norms [44].

6 Conclusions and future work

In this article, we provided a theoretical framework for cybersecurity assessment and mitigation strategies specific to complex, context-aware environments. Using the smart classroom as an example scenario and the ISO/IEC 27002 standard as a reference framework, we analyzed various security risks and highlighted the importance of implementing robust protection strategies to mitigate potential threats. One of the main challenges in securing such systems is the dynamic nature of context-aware technologies and the variety and complexity of technologies and protocols involved. We have identified the following risks on an actor-based model: attacks on DCAs (node compromise, false data injection, malicious code injection, and sleep deprivation), attacks on communication channels (eavesdropping, data tampering, replay attacks, spoofing, flooding, and jamming attacks), and attacks on information systems (physical attacks, user impersonation, and malware injection).

Following the ISO/IEC 27002 recommendations, we have identified different controls that must be implemented to overcome the security and privacy challenges. Cryptography is the cornerstone of data and system security, achieving confidentiality and integrity, as well as authentication of data, users and systems within the classroom. Using cryptography entails that the administrator manages a secure key management and digital identity life-cycle supporting system. Regarding network protection, besides enabling firewalls in the network devices and on the end systems themselves, we highlighted the importance of relying on the invisible technology concept, aiming at seamlessly integrating devices and information systems in the context-aware environment. Regarding user authentication, we noted that raising awareness and providing proper training for teachers, students, and families is essential. In parallel, besides using data privacy protection techniques like pseudonymization and secure storage of PII, we discussed that our proposal based on distributed DCAs contributes to the data minimization principle. Also related to privacy, to ensure transparency and adherence to privacy regulations, we advocate for a PMAS integrated within the context-aware system. We discussed the feasibility of implementing such measures, considering the variety of devices that support our context-aware scenario, from microcontrollers and single-board computers to off-the-shelf higher capacity computers. Finally, including regulatory foresight and cryptographic preparedness in the architectural design strengthens the system's alignment with upcoming legislative and technical challenges, ensuring its long-term viability in diverse deployment scenarios.

The proposed framework can be applied in both small-scale environments (*e.g.,* smart classrooms) and larger deployments (*e.g.,* smart schools or smart hospitals). This scalability follows principles already established in the literature on secure IoT and distributed context-aware systems. Prior work demonstrates that hierarchical, distributed architectures and well-structured identity-management processes scale naturally as the number of devices grows [23, 50, 52]. Consequently, scaling our framework primarily requires administering additional resources and handling a larger set of digital identities, rather than modifying the underlying architecture.

Future work includes expanding the proposed architecture and fully integrating the discussed regulatory frameworks, such as the EU AI Act or the emerging ISO/IEC 27090 draft standard [33], offering a structured approach to managing AI-related risks. By aligning security practices with these regulatory and standardization efforts, organizations can ensure compliance while fostering trust in context-aware systems. Moreover, as context-aware systems evolve towards cognitive architectures, future work must consider advanced security measures that address emerging risks. Next-generation context-aware systems will require adaptive security mechanisms capable of handling increasingly sophisticated threats. Finally, we will explore the interdisciplinary nature of this research (*e.g.,* involving educators, psychologists, and ethicists) to further evaluate socio-technical implications.

Acknowledgements This research was supported by Ministerio de Ciencia, Innovación y Universidades, Gobierno de España (Agencia Estatal de Investigación, Fondo Europeo de Desarrollo Regional - FEDER, European Union) under the research grants PID2021-127409OB-C33 CONDOR and PID2024-158490OB-C31 ECEEAS. Also, this research was partially funded by AGAUR research group 2021SGR-00111: "ASCLEPIUS: Smart Technology for Smart Healthcare". Elena Figueroa was supported by Banco Santander under the Martí i Franquès grant number 2021PMF-BS-6. Fran Casino was supported by the European Commission under the Horizon Europe Programme, as part of the project SAFEHORIZON (Grant Agreement no. 101168562), and by the Spanish Ministry of Science and Innovation under the "Ramón y Cajal" programme (RYC2023-044857-I).

Author Contributions Antoni Martínez-Ballesté: Conceptualization, Formal analysis, Methodology, Visualization, Writing – original draft, Writing - review & editing, Funding acquisition, Supervision. Edgar Batista: Conceptualization, Formal analysis, Methodology, Visualization, Writing – original draft, Writing - review & editing. Elena Figueroa: Formal analysis, Methodology. Kaouther Nouni: Formal analysis, Methodology. Agusti Solanas: Conceptualization, Methodology, Writing – original draft, Writing - review & editing, Funding acquisition, Supervision. Fran Casino: Conceptualization, Formal analysis, Methodology, Writing – original draft, Writing - review & editing.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Al-Muhtadi, J., Saleem, K., Al-Rabiaah, S., Imran, M., Gawanmeh, A., Rodrigues, J.J.P.C.: A lightweight cyber security framework with context-awareness for pervasive computing environments. Sustain. Cities Soc. **66**, 102610 (2021). https://doi.org/10.1016/j.scs.2020.102610
2. Almusaylim, Z.A., Zaman, N.: A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). Wireless Netw. **25**, 3193–3204 (2019). https://doi.org/10.1007/s11276-018-1712-5
3. de Angelis, A., Elliott, P.: Mbed TLS: An open-source SSL/TLS library (2025). Available at: https://github.com/Mbed-TLS/mbedtls
4. Barangi, H., Rahimi, S.K., Zamani, B., Moradi, H.: An Ontology-based Approach to Facilitate Semantic Interoperability of Context-Aware Systems. In: 28th International Computer Conference, Computer Society of Iran (CSICC), pp. 1–5. IEEE, Tehran, Iran (2023). DOI: https://doi.org/10.1109/CSICC58665.2023.10105364
5. Batista, E., Cot, L., Pérez, V., Martínez-Ballesté, A.: Real-Time Emotion Assessment System in Smart Classrooms Using Wearable Bracelets. In: Proc. 18th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM), pp. 36–41. IARIA Press, Venice, Italy (2024)
6. Batista, E., Moncusi, M.A., López-Aguilar, P., Martínez-Ballesté, A., Solanas, A.: Sensors for context-aware smart healthcare: a security perspective. Sensors **21**(20), 6886 (2021). https://doi.org/10.3390/s21206886
7. Batista, E., Shoot, C., Solanas, A., Martínez-Ballesté, A.: Self-Organising and Autonomous IoT-based Monitoring Units for Smart Environments. In: Proc. 13th Int. Conf. on Applications in Electronics Pervading Industry, Environment and Society (2025). In press
8. Bavdekar, R., Chopde, E.J., Agrawal, A., Bhatia, A., Tiwari, K.: Post quantum cryptography: a review of techniques, challenges and standardizations. In: Proc. Int. Conf. on Information Networking (ICOIN), pp. 146–151. IEEE, Bangkok, Thailand (2023). DOI: https://doi.org/10.1109/ICOIN56518.2023.10048976
9. Brink, H.W., Loomans, M.G.L.C., Mobach, M.P., Kort, H.S.M.: Classrooms' indoor environmental conditions affecting the academic achievement of students and teachers in higher education: A systematic literature review. Indoor Air **31**(2), 405–425 (2021). https://doi.org/10.1111/ina.12745
10. Camacho, J.M., Couce-Vieira, A., Arroyo, D., Insua, D.R.: A cybersecurity risk analysis framework for systems with artificial intelligence components. Int. Trans. Oper. Res. (2025). https://doi.org/10.1111/itor.70049
11. Casino, F., Lopez-Iturri, P., Aguirre, E., Azpilicueta, L., Falcone, F., Solanas, A.: Enhanced wireless channel estimation through parametric optimization of hybrid ray launching-collaborative filtering technique. IEEE Access **8**, 83070–83080 (2020). https://doi.org/10.1109/ACCESS.2020.2992033
12. Casino, F., Patsakis, C., Solanas, A.: Privacy-preserving collaborative filtering: a new approach based on variable-group-size microaggregation. Electron. Commer. Res. Appl. **38**, 100895 (2019). https://doi.org/10.1016/j.elerap.2019.100895
13. Cavoukian, A.: Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era. In: Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, pp. 170–208. IGI Global (2012). DOI: https://doi.org/10.4018/978-1-61350-501-4.ch007
14. Chinta, S.V., Wang, Z., Yin, Z., Hoang, N., Gonzalez, M., Quy, T.L., Zhang, W.: FairAIED: Navigating Fairness, Bias, and Ethics in Educational AI Applications. arXiv preprint arXiv:2407.18745 (2024)
15. Dey, A.K.: Understanding and using context. Pers. Ubiquit. Comput. **5**, 4–7 (2001). https://doi.org/10.1007/s007790170019
16. Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.2 (2008). 10.17487/RFC5246. Available at: https://www.rfc-editor.org/rfc/rfc5246
17. Dimitriadou, E., Lanitis, A.: A critical evaluation, challenges, and future perspectives of using artificial intelligence and emerging technologies in smart classrooms. Smart Learn. Environ. **10**, 12 (2023). https://doi.org/10.1186/s40561-023-00231-3
18. European Data Protection Supervisor (EDPS): AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation (2021). Available at: https://www.edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en
19. Union, E.: Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation). Off. J. Eur. Union **L119**, 1–88 (2016)
20. European Union: Proposal for a regulation of the European Parliament and the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. EUR-Lex-52021PC0206 (2021)
21. European Union: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence. Official Journal of the European Union (2024). http://data.europa.eu/eli/reg/2024/1689/oj
22. Fenu, G., Galici, R., Marras, M.: Experts' View on Challenges and Needs for Fairness in Arti cial Intelligence for Education. In: 9th Int. Conf. on Artificial Intelligence in Education, LNCS, vol. 13355, pp. 243–255. Springer, Durham, UK (2022). DOI: https://doi.org/10.1007/978-3-031-11644-5_20
23. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (iot): a vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
24. Halgamuge, M.N., Niyato, D.: Adaptive edge security framework for dynamic IoT security policies in diverse environments. Computers & Security **148**, 104128 (2025). https://doi.org/10.1016/j.cose.2024.104128
25. Hasan, K.F., Overall, A., Ansari, K., Ramachandran, G., Jurdak, R.: Security, Privacy, and Trust of Emerging Intelligent Transportation: Cognitive Internet of Vehicles. In: Next-Generation Enterprise

Security and Governance, pp. 193–226. CRC Press (2022). DOI: https://doi.org/10.1201/9781003121541-8
26. Haverkort, B.R., Zimmermann, A.: Smart industry: how ICT will change the game! IEEE Internet Comput. **21**(1), 8–10 (2017). https://doi.org/10.1109/MIC.2017.22
27. Hundepool, A., Domingo-Ferrer, J., Franconi, L., Giessing, S., Nordholt, E.S., Spicer, K., De Wolf, P.P.: Statistical Disclosure Control. Wiley (2012)
28. Hunkeler, U., Truong, H.L., Stanford-Clark, A.: MQTT-S - A Publish/Subscribe Protocol For Wireless Sensor Networks. In: Proc. 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE), pp. 791–798. IEEE, Bangalore, India (2008). DOI: https://doi.org/10.1109/COMSWA.2008.4554519
29. International Organization for Standardization: ISO/IEC 27701:2019: Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines (2019). Available at: https://www.iso.org/standard/71670.html
30. International Organization for Standardization: ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection - Information security management systems - Requirements (2022). Available at: https://www.iso.org/standard/82875.html
31. International Organization for Standardization: ISO/IEC 27002:2022: Information Security, Cybersecurity and Privacy Protection – Information Security Controls (2022). Available at: https://www.iso.org/standard/75652.html
32. International Organization for Standardization: ISO/IEC 23894:2023: Information technology - Artificial intelligence - Guidance on risk management (2023). Available at: https://www.iso.org/standard/77304.html
33. International Organization for Standardization: ISO/IEC DIS 27090: Cybersecurity – Artificial Intelligence – Guidance for addressing security threats and failures in artificial intelligence systems (2025). Available at: https://www.iso.org/standard/56581.html
34. Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F.D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., Hansen, R.: Transitioning organizations to post-quantum cryptography. Nature **605**(7909), 237–243 (2022). https://doi.org/10.1038/s41586-022-04623-2
35. Kumar, M.: Post-quantum cryptography algorithm's standardization and performance analysis. Array **15**, 100242 (2022). https://doi.org/10.1016/j.array.2022.100242
36. Kumar, S., Nguyen, L.T., Zeng, M., Liu, K., Zhang, J.: Sound Shredding: Privacy Preserved Audio Sensing. In: Proc. 16th International Workshop on Mobile Computing Systems and Applications (HotMobile), pp. 135–140. Santa Fe, USA (2015). DOI: https://doi.org/10.1145/2699343.2699366
37. Machin, J., Batista, E., Martínez-Ballesté, A., Solanas, A.: Privacy and security in cognitive cities: a systematic review. Appl. Sci. **11**(10), 4471 (2021). https://doi.org/10.3390/app11104471
38. Martínez-Ballesté, A., Batista, E., Figueroa, E., Torruella, G.F., Llurba, C., Quiles-Rodríguez, J., Unciti, O., Palau, R.: A Proposal for the Smart Classroom Infrastructure Using IoT and Artificial Intelligence. In: Proc. 48th IEEE Annual Computers, Software, and Applications Conference (COMPSAC), pp. 109–114. IEEE, Osaka, Japan (2024). DOI: https://doi.org/10.1109/COMPSAC61105.2024.00025
39. Martínez-Ballesté, A., Rashwan, H., Puig, D., Solanas, A.: Design and implementation of a secure and trustworthy platform for privacy-aware video surveillance. Int. J. Inf. Secur. **17**, 279–290 (2018). https://doi.org/10.1007/s10207-017-0370-4
40. Martínez-Ballesté, A., Ferre, M., Solanas, A., Casino, F.: AI-based Privacy Management and Awareness for Smart Environments. In: Proc. 13th Int. Conf. on Applications in Electronics Pervading Industry, Environment and Society (2025). In press
41. Mehmood, T.: Ethical ai in education: addressing bias, privacy, and equity in ai-driven learning systems. AI EDIFY Journal **2**(1), 38–45 (2025)
42. National Institute of Standards and Technology: Ai risk management framework: Second draft. Technical Report NIST IR 8360 (2nd Draft), National Institute of Standards and Technology (2022). https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf
43. Pabba, C., Bhardwaj, V., Kumar, P.: A visual intelligent system for students' behavior classification using body pose and facial features in a smart classroom. Multimedia Tools and Applications **83**(12), 36975–37005 (2024). https://doi.org/10.1007/s11042-023-16388-5
44. Papagiannidis, E., Mikalef, P., Conboy, K.: Responsible artificial intelligence governance: a review and research framework. J. Strateg. Inf. Syst. **34**(2), 101885 (2025). https://doi.org/10.1016/j.jsis.2024.101885
45. Parambil, M.M.A., Ali, L., Alnajjar, F., Gochoo, M.: Smart Classroom: A Deep Learning Approach towards Attention Assessment through Class Behavior Detection. In: Proc. Advances in Science and Engineering Technology International Conferences (ASET), pp. 1–6. IEEE, Dubai, UAE (2022). DOI: https://doi.org/10.1109/ASET53988.2022.9735018
46. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Context aware computing for the internet of things: a survey. IEEE Communications Surveys & Tutorials **16**(1), 414–454 (2014). https://doi.org/10.1109/SURV.2013.042313.00197
47. Picallo, I., López Iturri, P., Celaya-Echarri, M., Azpilicueta, L., Falcone, F.: Deterministic wireless channel characterization towards the integration of communication capabilities to enable context aware industrial internet of thing environments. Mobile Networks and Applications **28**(1), 4–18 (2022). https://doi.org/10.1007/s11036-022-01993-9
48. Rashwan, H.A., Solanas, A., Puig, D., Martínez-Ballesté, A.: Understanding trust in privacy-aware video surveillance systems. Int. J. Inf. Secur. **15**, 225–234 (2016). https://doi.org/10.1007/s10207-015-0286-9
49. Rescorla, E., Tschofenig, H., Modadugu, N.: The Datagram Transport Layer Security (DTLS) Protocol Version 1.3 (2022). 10.17487/RFC9147. Available at: https://www.rfc-editor.org/rfc/rfc9147
50. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**(10), 2266–2279 (2013)
51. Sezer, O.B., Dogdu, E., Ozbayoglu, A.M.: Context-aware computing, learning, and big data in internet of things: a survey. IEEE Internet Things J. **5**(1), 1–27 (2018). https://doi.org/10.1109/JIOT.2017.2773600
52. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in the internet of things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
53. Singh, T., Solanki, A., Sharma, S.K., Nayyar, A., Paul, A.: A decade review on smart cities: paradigms. Challenges and Opportunities. IEEE Access **10**, 68319–68364 (2022). https://doi.org/10.1109/ACCESS.2022.3184710
54. Solanas, A., Batista, E., Casino, F., Papageorgiou, A., Patsakis, C.: Privacy-Oriented Analysis of Ubiquitous Computing Systems: A 5-D Approach. In: Security of Ubiquitous Computing Systems, pp. 201–213. Springer (2021). DOI: https://doi.org/10.1007/978-3-030-10591-4_12
55. Solanas, A., Patsakis, C., Conti, M., Vlachos, I.S., Ramos, V., Falcone, F., Postolache, O., Perez-Martinez, P.A., Pietro, R.D., Perrea, D.N., Martínez-Ballesté, A.: Smart health: a context-aware health

paradigm within smart cities. IEEE Commun. Mag. **52**(8), 74–81 (2014). https://doi.org/10.1109/MCOM.2014.6871673
56. Sonmez Turan, M.: Ascon-Based Lightweight Cryptography Standards for Constrained Devices (2025). https://doi.org/10.6028/nist.sp.800-232
57. Temdee, P., Prasad, R.: Security for context-aware applications. In: Context-Aware Communication and Computing: Applications for Smart Environment, pp. 97–125. Springer (2018). DOI: https://doi.org/10.1007/978-3-319-59035-6_5
58. Tyagi, A.K.: Applications of human computer interaction, explainable artificial intelligence and conversational artificial intelligence in real-life sectors. In: Data Analytics and Artificial Intelligence for Predictive Maintenance in Smart Manufacturing, pp. 282–325. CRC Press (2024)
59. Unciti, O., Palau, R.: Teacher decision making tool: development of a prototype to facilitate teacher decision making in the classroom. Journal of Technology and Science Education **13**(3), 740–760 (2023). https://doi.org/10.3926/jotse.1801
60. Yanwei, S., Guangzhou, Z., Haitao, P.: Research on the context model of intelligent interaction system in the internet of things. In: Proc. IEEE International Symposium on IT in Medicine and Education, vol. 2, pp. 379–382. Guangzhou, China (2011). DOI: https://doi.org/10.1109/ITiME.2011.6132129
61. Zigomitros, A., Casino, F., Solanas, A., Patsakis, C.: A survey on privacy properties for data publishing of relational data. IEEE Access **8**, 51071–51099 (2020). https://doi.org/10.1109/ACCESS.2020.2980235

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.