Artificial Intelligence in Campus Security and Crisis prediction: A Review of Current Applications and Future Trends

by Jana Publication & Research

Submission date: 14-Oct-2025 07:11AM (UTC+0300)
Submission ID: 2755411570
File name: IJAR-54329.pdf (619.78K)
Word count: 7582
Character count: 45295

Artificial Intelligence in Campus Security and Crisis prediction: A Review of Current Applications and Future Trends

ABSTRACT

Ensuring campus safety requires schools to implement systematic measures that protect the physical integrity, mental well-being, and property of students and faculty from har while maintaining a stable environment conducive to teaching and learning. This paper reviews the application of Artificial Intelligence (AI) in campus safety and crisis prediction over the past five years. By synthesizing findings from relevant literature, it provides an in-depth analysis of the key challenges in current applications, aiming to offer valuable insights for future practices in the field.

1. Introduction

1.1. Research Background

In an increasingly complex social environment, campus security faces correspondingly intricate challenges. Although the overall campus remains safe and orderly, there is a constant need to systematically manage routine duties such as monitoring pedestrian flow, identifying potential hazards, addressing student mental health, and responding swiftly to emergencies. From an operational standpoint, security departments must efficiently execute these diverse tasks, which require a management approach that is both comprehensive and precise. Yet, traditional methods relying primarily on personnel and physical measures are often labor-intensive and inefficient.

For instance, manually reviewing extensive surveillance footage, detecting anomalous behavior, and integrating multi-source risk intelligence depend heavily on the experience and sustained attention of security staff. This not only consumes substantial human resources but also increases the risk of oversights due to fatigue or information overload, thereby constraining the overall effectiveness of security management. Consequently, security teams often become preoccupied with daily inspections and post-incident responses, leaving limited capacity for proactive warning and strategic prevention.

Therefore, leveraging artificial intelligence (AI) to build an intelligent, forward-looking crisis prediction and intervention system has become an essential and urgent measure to enhance campus security governance and protect the well-being of students and faculty.

1.2. The Rise of the Technology

In recent years, artificial intelligence (AI) has seen rapid breakthroughs in fields such as computer vision, big data analytics, and natural language processing. These advancements, characterized by powerful perceptual and decision-making capabilities, are now widely deployed in public security contexts. From disaster and epidemic control to crowd management, and from crime surveillance to intelligent dispatch of fire alarms (Myagmar-Ochir & Kim, 2023), AI has significantly enhanced the efficiency and accuracy of security operations, facilitating a strategic shift from post-incident response to pre-emptive early warning.These successful practices provide valuable experience and technical pathways for security governance in campus settings—a specific type of public space.

Given the high density of people, complex environments, and the need for refined management in educational settings, AI-integrated intelligent early-warning and management systems are expected to form the core of next-generation smart campus security frameworks. Such systems can help create a safer and more focused teaching and learning environment for both students and faculty.

The introduction of AI technology aims to enhance existing security systems through big data analytics, intelligent sensing, and predictive modeling, enabling earlier and more accurate identification and warning of potential risks. This will significantly improve the efficiency and precision of security operations, injecting intelligent momentum into traditional security frameworks. It is important to emphasize that AI does not replace human decision-making. Instead, it augments situational awareness, optimizes resource allocation, and improves warning accuracy, thereby freeing security personnel from repetitive and mundane tasks. This allows them to focus on higher-value decision-making, communication,

and intervention, ultimately driving the transformation of campus security management from a “reactive response” model to a “proactive prevention” paradigm, leading to a comprehensive improvement in management effectiveness and safety standards.

1.3. Problem Statement

Research on the application of artificial intelligence (AI) in campus security and crisis prediction is growing rapidly. However, existing studies predominantly focus on applying specific technologies—such as facial recognition or behavior analysis—in isolated contexts like access control or public opinion monitoring. As a result, the research landscape appears fragmented and decentralized.

The findings from these studies often remain siloed, lacking a systematic framework that integrates multiple technologies, scenarios, and operational layers. This makes it difficult to form a holistic understanding of how AI can enhance campus security in a comprehensive manner. Moreover, there is still no widely accepted set of evaluation standards or implementation pathways established in the field.

To address these gaps, this review seeks to systematically organize and synthesize recent research progress, with the aim of offering an integrated perspective and identifying coherent directions for future development.

1.4. Article Structure:

This paper adopts a systematic review framework. It begins by introducing the research background, core issues, and academic value. The methodology is then outlined, detailing the literature search strategy, screening criteria, and analytical process. The core analysis categorizes AI applications in campus safety into three key areas: physical safety, cybersecurity, and mental health early-warning, integrating findings to present systematic insights. Subsequently, the paper examines key challenges in current applications, including technical bottlenecks, ethical issues, and implementation barriers. Following this analysis, future research directions are explored, such as multi-technology integration, paradigm evolution, and governance frameworks. The conclusion summarizes AI's transformative impact on the field, underscores the urgency of ethical governance, and calls for multi-stakeholder collaboration to foster its sustainable development.

2. Literature review methods

A literature search was performed in major academic databases, including Web of Science, Elsevier Science Direct, EBSCO, and the Chinese Science Citation Database (CSCD). The search aimed to identify studies concerning artificial intelligence (AI) in campus safety, using the keywords "artificial intelligence" AND "campus security" as well as "smart campus" AND "safety". The publication date was restricted to the last five years. Given the limited number of studies on AI applications in campus safety, no restrictions were placed on specific AI methodologies or research subjects.

The inclusion criteria were: (1) studies focusing on AI applications in campus safety, excluding reviews; and (2) studies employing verifiable methods and presenting detailed results with objective conclusions. Through this process, 26 studies were ultimately selected for inclusion in this systematic review. The literature screening procedure is illustrated in the figure below.

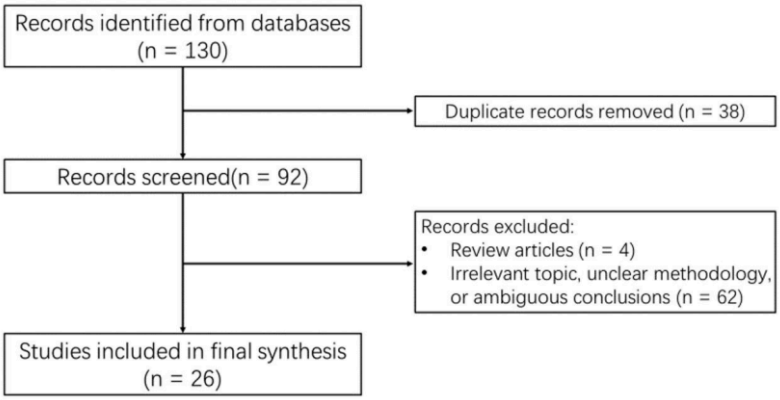

Figure 1. Literature Screening Flowchart

3. Major Application Areas of AI in Campus Security and Early Warning

3.1. Physical Security and Intrusion Detection

In the field of campus security, the application of artificial intelligence (AI) in physical security and intrusion detection is gradually expanding. This is primarily achieved through intelligent video surveillance systems and their integration with sensor networks and the Internet of Things (IoT), which together form a multi-layered and intelligent campus security protection system.By offering real-time monitoring of video feeds, access control mechanisms, and intrusion detection sensors, IoT-enabled security systems may increase campus safety. (Srhir et al., 2023)

3.1.1. Intelligent Video Surveillance and Anomalous Behavior Detection

As a pivotal application of AI in enhancing campus physical security, intelligent video surveillance systems utilize computer vision and deep learning to analyze real-time video feeds. These systems automatically detect abnormal behaviors, suspicious individuals, and emergency incidents, thereby overcoming the limitations of traditional manual monitoring in terms of efficiency and continuity. This significantly improves the capacity for rapid response to potential campus threats (Srhir et al., 2023). Key application areas include facial recognition, abnormal behavior detection, intrusion alarms, fire detection, and emergency disaster response.

Identity Recognition： Access control management is essential for safeguarding campus safety and maintaining the normal order of teaching and research. By regulating the entry and exit of personnel, it helps prevent external security threats and reduce incidents such as theft and fraud. Furthermore, it supports the optimized use of public resources and plays a key role during public health incidents, collectively fostering a stable environment where students and faculty can focus on their academic pursuits. The foundation of achieving such security control lies in the accurate verification of user identity.Common methods of identity authentication include password based authentication, smart card based authentication, biometric based authentication and so on. In order to improve security, the above methods can be combined to realize multi-factor authentication. (Niu et al., 2022)

Abnormal Behavior Detection: AI algorithms are capable of identifying activities that deviate from established normal behavior patterns. In campus settings, the system can automatically detect behaviors such as prolonged loitering, sudden running, unauthorized gatherings, climbing fences, lingering in restricted areas (Liao et al., 2024), and even carrying weapons (Sutton, 2025), subsequently triggering

relevant alerts. The underlying mechanism involves training on vast datasets of normal behavior to establish behavioral benchmarks, which enables effective anomaly recognition (Zhou et al., 2024). For instance, Liao et al. (2024) proposed a campus security system based on LoRa technology, which achieved a rapid response time of approximately one second for locating individuals in concealed or abnormal locations.

Intrusion Zone Alarm: In key campus areas such as laboratories, data centers, and dormitories, the installation of electronic fences can make up for the shortage of security personnel, realize all-weather and full-coverage protection for building perimeters, and effectively improve the security level. Within the electronic fences or sensitive areas set by the system, an alarm can be triggered immediately once unauthorized persons or objects are detected entering.

Disaster Monitoring and Rescue: In the context of campus fire prevention, a fire detection model leveraging object detection algorithms has been proposed. Trained on fire sample datasets, the model achieved an accuracy of 94% and a recall of 92% (Yang et al., 2025), demonstrating superior performance over traditional smoke detectors. It enables earlier identification of fire hazards and the issuance of proactive warnings, thereby significantly strengthening campus fire safety. To enhance rescue efficiency during disasters, Zhang and Xu (2021) suggested that facial recognition could be employed to locate trapped individuals. By integrating this positional data with building risk levels and road network models, their approach can generate intelligent rescue plans, facilitating rapid and precise emergency operations.

3.1.2. Sensor Networks and Internet of Things (IoT) Integration

Internet of Things (IoT) applications are increasingly being adopted on smart campuses to enhance operational efficiency, service quality, and the overall experience for students, teachers, and staff. The integration of IoT with Artificial Intelligence (AI) has significantly broadened the scope and real-time capabilities of campus physical security. By deploying a network of diverse sensors and intelligent devices, and leveraging AI for data analytics, campuses can now implement a range of functions such as intelligent access control, environmental monitoring, and early fire warning systems (Srhir et al., 2023). The key application areas are detailed below.

Intelligent Access Control Systems: The development of smart campuses commonly involves integrating IoT-based access control systems. By incorporating biometric technologies (e.g., facial or fingerprint recognition) and AI analytics, these systems enable precise management of personnel movement and trigger real-time alerts in case of unauthorized entry. A key emphasis lies in system integration, where access control is interconnected with platforms such as student information systems to improve both security and administrative efficiency.For example, through a unified intelligent identification platform, institutions can implement role-based personnel management, maintain real-time awareness of individuals on campus, and restrict access by outsiders. Should unauthorized persons enter, administrators can track their movements via the backend system, thereby significantly enhancing overall campus safety (Cao, 2022).Research has been conducted to evaluate the effectiveness of smart locks in campus settings. Findings suggest that while smart locks do not significantly reduce already-low crime rates, this may be because baseline security levels are already effective at controlling campus crime (Kaplan, 2023).

Environmental Monitoring and Risk Assessment: IoT sensors enable the continuous collection of data on building structural conditions and environmental parameters—such as temperature, humidity, and air quality. When integrated with AI modeling and analytics, this data can be used to predict potential structural failures or environmental hazards, facilitating proactive risk prevention (Dong, 2023). For example, IoT technology can support the construction of a factor model for campus safety risk assessment. Methods such as Interpretive Structural Modeling (ISM) and the Decision Making Trial and Evaluation Laboratory (DEMATEL) can then be applied to analyze correlations among factors, providing a foundation for a comprehensive evaluation of campus safety conditions (Dong, 2023).Beyond video surveillance, IoT sensor networks are also pivotal in fire detection. By deploying a combination of temperature, smoke, and flame sensors and employing AI algorithms for multi-source data fusion, these systems significantly improve the accuracy and speed of fire identification. Such integrated solutions facilitate the early detection of potential fires and enable timely alerts to relevant personnel through intelligent notification mechanisms (Yang et al., 2025).

Road Safety Monitoring: Campus roads are characterized by high-density, mixed-traffic conditions, where pedestrians, bicycles, e-scooters, and motor vehicles share limited space, forming complex and dynamic traffic flows (Gupta et al., 2021). These conditions necessitate not only strict speed limits for vehicles but also a dynamic supervision system capable of real-time response. By deploying sensors such as millimeter-wave radars and intelligent cameras, an always-active monitoring network can be established. This system collects and analyzes real-time data on vehicle speed, trajectory, and flow, enabling it to promptly identify risky behaviors—such as speeding or illegal parking—and trigger alerts for coordinated intervention. The result is a data-driven safety barrier that significantly improves the accuracy and proactivity of campus traffic management.Furthermore, some studies have explored the use of wearable devices to enhance e-scooter safety on campus. These devices can detect hazardous conditions like rider instability or road surface defects (e.g., potholes) and issue immediate alerts to users, thereby improving overall safety performance (Gupta et al., 2021).

Insights from broader IoT applications, such as device networking in smart homes and livestock tracking in smart agriculture, confirm the technology's suitability for monitoring high-value campus assets. This capability can be effectively applied to track items like laboratory equipment, library collections, and office supplies, thereby helping to prevent theft and significantly improve asset management efficiency.

3.2. Cyberspace Security and Cyberbullying Prevention

3.2.1 Natural Language Processing (NLP) for Cyberbullying and Hate Speech Detection

As students increasingly rely on online platforms for learning and socializing, ensuring cyberspace security and preventing cyberbullying have become crucial for safeguarding their well-being, maintaining a harmonious campus atmosphere, and supporting academic engagement and performance (Abbasi et al., 2025). Cyberbullying erodes trust and a sense of security, damages peer relationships, and negatively impacts the overall school climate (Jacek Pyżalski et al., 2022).

Natural Language Processing (NLP) technology offers a viable solution by automatically identifying, classifying, and flagging harmful content associated with cyberbullying through the analysis of large-scale text data. This enables timely intervention by campus authorities. AI models can scan online platforms—including social media posts, comments, and chat logs—to detect abusive, threatening, or demeaning language (Biernesser et al., 2023). For example, Biernesser et al. demonstrate that NLP can recognize hate speech, discriminatory terms, and specific phrasing patterns linked to bullying. The FACapsnet model, which integrates capsule networks with consistent attention mechanisms, extracts multi-dimensional features to accurately identify cyberbullying and distinguish among its various forms, such as those based on religion, age, race, or gender (Biernesser et al., 2023).

Key Applications and Effects

Automated Identification and Early Warning: NLP models facilitate the real-time or near-real-time monitoring of textual content across social media, forums, and campus communication platforms. By recognizing specific keywords, syntactic structures, and sentiment patterns, these systems automatically flag potential cyberbullying or hate speech. The integration of deep learning and self-optimizing neural networks enhances detection accuracy and improves the recognition of nuanced linguistic features, providing robust technical support for identifying complex language patterns in campus environments. Upon detection, the system generates immediate alerts to relevant personnel (e.g., counselors or teachers), significantly shortening intervention times and reducing the burden of manual monitoring.

Improved Accuracy and Broader Coverage: AI models can process vast datasets and identify subtle, often imperceptible patterns that escape manual screening. This capability is particularly critical for detecting concealed forms of bullying, such as sarcasm and indirect verbal aggression. Research indicates that Transformer-based models, for instance, have shown significant progress in identifying hate speech on social media.

Adaptability in Multilingual Contexts: In response to increasingly multicultural campuses, NLP technologies have been extended to support multiple languages—including Bengali, Norwegian, Polish, and Arabic dialects—to address the global challenge of cyberbullying. This expansion ensures equitable protection for students from diverse linguistic and cultural backgrounds.

Personalized Risk Analysis: Through in-depth analysis of digital text, AI systems can infer potential personality traits of individuals who post harmful content. This provides deeper insights for understanding the underpinnings of malicious behavior and enables more targeted and effective interventions.

3.3.2 Social Network Analysis (SNA) for Identifying Potentially Harmful Groups

The social influence among college students is strong, so social network analysis (SNA) may be useful in studying their health conditions (Patterson & Goodson, 2018). By conducting in-depth analysis of the structure, interaction patterns, and content of college students' social networks, SNA can help identify student groups at risk of mental health issues, internet addiction, harmful behaviors, academic difficulties, and cyberbullying, and provide a scientific basis for early intervention. For example, one study demonstrated the use of SNA to identify alcohol and substance addiction behaviors among college student groups (Mason et al., 2014).

During the student years, harmful behaviors such as alcohol abuse are relatively common and easily influenced by peers. SNA can reveal the impact of social networks on these behaviors; students with high-risk social networks (e.g., close friends who abuse alcohol) are 10 times more likely to engage in risky drinking (Mason et al., 2014). SNA can analyze students' perceptions of peer drinking and identify the correlation between an individual student's drinking behavior and the drinking behavior of their closest social connections. Beyond alcohol, social network factors are also associated with other addictive behaviors among college students—factors such as internet exposure, centrality, reciprocal relationships, and network density all influence addictive behaviors (Rinker et al., 2016).

There are two main methods of social network analysis (SNA): ego-centered network analysis and whole-network analysis. Ego-centered network analysis focuses on the individual perspective, making data collection relatively easy, but it has limited structural variables. Whole-network analysis studies all relationships within a given network, enabling the measurement of multi-level patterns, but it has poor generalizability and more complex data collection (Patterson & Goodson, 2018).

This technology quantifies the "strength of relationships" between individuals based on students' social media interactions, communication records, and other collectible offline behavior data, and identifies "strong-tie" networks centered on core individuals. Through algorithms that automatically map group structures, it accurately locates three types of key nodes: "opinion leaders" who influence group orientation, "bridge figures" who connect different communities, and marginalized isolated groups prone to forming an "echo chamber" effect. This allows administrators to accurately identify social structures with closed and extreme characteristics, enabling early detection and proactive prevention of potential crises.

Key Applications and Effects:

Detecting Abnormal Group Dynamics: Social Network Analysis (SNA) represents students as nodes and their interactions as edges to construct a social graph. Community detection algorithms can then identify tightly-knit subgroups. When a group exhibits abnormal characteristics—such as strong exclusivity, concentrated negative sentiment, or frequent discussions of harmful topics—the SNA-based system can flag it as potentially hazardous.

Identifying Key Influential Nodes: By calculating centrality metrics (e.g., degree, betweenness, closeness), SNA assesses the influence of individual students, such as opinion leaders or potential instigators. This helps administrators pinpoint key players in information diffusion and group dynamics, enabling targeted interventions. This method of influence analysis is a cornerstone in frameworks designed to detect online extremism, radicalization, and politicized hate speech.

Tracing Information Diffusion Paths: SNA can map the propagation pathways of cyberbullying content or inflammatory speech across a network. This allows administrators to quickly identify the origins and spread of harmful information, facilitating timely measures to contain its dissemination and minimize its impact on the campus environment.

Supporting Early Warning Systems: The integration of SNA into student behavior Early Warning Systems enables a more holistic risk assessment. By analyzing patterns in student interactions, the system can predict potential behavioral issues, providing psychological counselors and educators with data-driven evidence for proactive intervention, thereby helping to prevent bullying incidents before they occur.

3.3Student Psychological Crisis Early Warning

Student mental health is a cornerstone of campus safety, with importance equal to that of physical security. Traditional assessment methods, which rely heavily on periodic surveys and self-reporting, suffer from significant limitations including delayed feedback, limited coverage, and susceptibility to response bias, making early crisis warning difficult. In contrast, artificial intelligence enables proactive risk assessment by continuously analyzing multi-dimensional data—such as behavioral patterns (e.g., attendance, consumption records), textual emotional cues, and social dynamics. AI models can keenly identify abnormal patterns and issue timely alerts, thereby overcoming the shortcomings of traditional approaches. This provides a critical window for targeted intervention, facilitating proactive prevention and systematic protection against psychological crises, as well as the early detection of abnormal mental states and potential risks (Yang et al., 2020).

The following sections detail two core components of this approach: predicting abnormal student behaviors and early warning of depression and suicide risk. By systematically integrating campus behavioral data, textual content, and non-verbal information, and leveraging multi-modal fusion and machine learning algorithms, a proactive mental health protection system can be effectively constructed.

3.3.1 Prediction of Student Abnormal Behaviors

(1) Campus Card Consumption Data

Students' campus card consumption data can effectively reflect their economic status, living habits, and behavioral patterns. Significant fluctuations in consumption amount, sudden changes in dining patterns, or consumption behaviors at abnormal times or locations can all serve as potential signals of psychological crises (He et al., 2024). This type of data boasts strong timeliness and accuracy, providing data support for campus administrators to promptly detect student abnormalities. Relevant studies typically focus on "campus-card consumption data" or "student consumption behavior," and emphasize the advantages of big data methods in improving the efficiency and accuracy of behavioral analysis (He et al., 2024).

(2) Learning Behavior Data

Students' learning behavior data includes academic performance, attendance, library book borrowings, and online learning engagement, which can be used to assess their level of academic investment and psychological state. Abnormal patterns—such as a sharp decline in academic performance, a sudden drop in attendance rate, or a significant reduction in study time—may indicate difficulties in psychological adaptation or emotional problems (Wang et al., 2022). Studies usually construct accurate student profiles based on "multi-indicator student behavior data" to achieve abnormal identification and early intervention (Wang et al., 2022).

(3) Textual Emotion Analysis

Emotional information expressed by students in social media, forums, and academic texts provides an important basis for judging their psychological state. Textual Emotion Detection (TED), a key branch of natural language processing, is widely used to identify negative emotions such as despair, depression, and anxiety (Zuberi et al., 2025). Emotion analysis methods based on machine learning have been applied in educational institutions for psychological monitoring and suicide prevention, identifying psychological crisis signals by analyzing public or private texts (Zuberi et al., 2025).

3.4.2 Early Warning of Depression and Suicide Tendency

(1) Risk Factor Identification

Mental health conditions such as depression, anxiety, and post-traumatic stress disorder (PTSD) are well-established risk factors for suicidal ideation (Casey et al., 2022). Behavioral issues—including self-harm, substance abuse, and sleep or eating disorders—are also strongly associated with elevated suicide risk (Danielsen et al., 2025). Furthermore, social and environmental stressors such as academic pressure, interpersonal conflict, family instability, and bullying significantly exacerbate psychological vulnerability among adolescents (Wang et al., 2024). Research indicates that diagnosed mental disorders and current depressive or anxiety symptoms in college students are significantly correlated with suicidal tendencies (Casey et al., 2022), while adverse family environments and depression or suicidal ideation in Chinese schoolchildren demonstrate a syndemic interaction.

Artificial intelligence (AI) has substantially enhanced the scope and precision of risk factor identification by integrating multi-source heterogeneous data. Machine learning techniques can

automatically extract latent risk patterns from large-scale behavioral datasets and uncover subtle correlations that are challenging to detect through conventional methods. For example, by analyzing associations between campus card usage, academic behavior, and social media content, AI systems can reveal complex interactions among financial strain, social isolation, and depressive symptoms (Atmakuru et al., 2025). Deep learning models are capable of processing unstructured data—such as text, images, and voice—to extract psychological risk features from semantic content and emotional tendencies expressed by students. Moreover, advanced algorithms like graph neural networks (GNNs) can analyze student social network structures to identify isolated individuals or track the dynamics of high-risk groups (He & Li, 2025). These AI-driven approaches not only enable the quantitative assessment of known risk factors but also aid in the discovery of novel risk markers, thereby offering more precise targets for early intervention.

(2) Early Intervention and AI-Assisted Warning

Early warning systems leverage multi-source data and AI technologies to achieve timely identification of high-risk students and deliver personalized interventions. These may include psychological counseling, peer support, and academic or life skills coaching (Saliba, 2024). Compared to traditional self-reporting and manual screening, AI techniques—such as natural language processing, machine learning, and deep learning—can detect psychological crisis signals earlier and with greater accuracy (Zuberi et al., 2025). For instance, multi-modal AI systems integrate neuroimaging, behavioral sensor data, and natural language processing to enable early detection of anxiety, depression, and suicide risk. They also support the enhancement of adolescents' emotional resilience through personalized intervention strategies (He & Li, 2025).

4. Discussion: Challenges, Limitations, and Ethical Considerations

4.1. Technical Challenges

Model Interpretability and Fairness: The "black box" nature of AI models may lead to opaque decision-making processes, raising concerns about fairness—particularly in contexts involving student behavior evaluation and intervention. Improving model interpretabilityis a key focus for future research to ensure that the application of AI systems in campus security is just and responsible.

Technical Robustness and Adversarial Attacks: Malicious users may attempt to evade AI detection systems, for instance, by using ambiguous language or images. Therefore, AI systems must exhibit strong robustness to withstand adversarial attacks and adapt to continuously evolving new threats.

Data Silos Issue: Smart campus systems typically collect data from multiple sources—such as student information systems, access control systems, video surveillance, online learning platforms, and social media interactions. These data are often stored across different databases with varying formats and standards, making integration challenging. For example, a student behavior early warning system requires integrating academic performance, attendance records, participation in extracurricular activities, and online interactions to comprehensively assess a student's risk profile. When these data remain fragmented across systems without unified interfaces or protocols, forming a holistic student profile for risk assessment becomes difficult. This directly limits the effectiveness of AI systems, leading to partial analysis outcomes and constrained model performance.

High False Positive Rate:

- Increases Manual Review Burden: When a system generates a large number of false positives, school staff (such as counselors and teachers) must devote considerable time and effort to verifying these "false alarms," diverting attention from genuinely urgent cases and increasing their workload.
- Causes Student Frustration and Distrust: Frequent false positives may lead students to feel over-monitored or distrusted, fostering resistance and damaging mutual trust between students and the institution. For instance, if a student's normal social expression is mistakenly flagged as bullying or hate speech, it could cause unnecessary distress and psychological pressure.
- Raises Ethical and Privacy Concerns: False positives may result in misguided interventions. In some cases, unwarranted investigations or behavioral restrictions might be imposed on students without their knowledge, infringing upon their privacy and personal freedom.

4.2. Ethical and Social Challenges

Privacy Infringement

AI systems rely on vast amounts of data for training and operation, especially in student behavior analysis, which involves personal private information. This raises ethical and legal issues concerning data collection, storage, usage, and sharing. For example, the EU's AI Act focuses on risks associated with AI systems and categorizes AI applications into unacceptable risk, high risk, limited risk, and minimal risk levels(Prainsack & Forgó, 2024). In campus settings, indiscriminate collection of facial images to build recognition databases, or emotion recognition in workplaces and educational institutions, is considered an "unacceptable risk"(Prainsack & Forgó, 2024).

"Digital Panopticon"

Pressure from Invisible Surveillance: Students may feel watched by an invisible yet omnipresent "eye." Even without specific violations, the fear of being misjudged or over-interpreted by AI can cause tension. This persistent, potential sense of being judged may lead to anxiety and discomfort.

Self-Censorship of Behavior: To avoid triggering AI alerts, students may consciously alter their behavior, refraining from activities or expressions that could be misinterpreted. For instance, normal social interactions or emotional expressions might be suppressed or hidden due to concerns about being misclassified as anomalous.

Loss of Privacy: Continuous digital monitoring entails extensive collection of personal information and behavioral data. Students may feel their privacy is violated and that they lack personal space and freedom, undermining their trust and sense of belonging within the school.

Constraints on Innovation and Expression: A highly controlled environment may stifle students' innovative spirit and freedom of expression. If students worry that their unconventional ideas or speech might be flagged by AI, they may become more conservative and compliant, thereby dampening campus vitality and creativity.

Erosion of Trust: Frequent false positives or opaque decision-making processes in AI systems may lead students and faculty to doubt the system's fairness and accuracy, resulting in distrust toward the entire campus security management framework.

4.3. Implementation and Management Challenges

High Costs: The implementation of AI technology and its applications often involves substantial costs. Initial investments are significant: deploying AI systems requires purchasing high-performance hardware, establishing sophisticated data infrastructure, and acquiring or developing expensive software solutions. These are frequently accompanied by high R&D expenditures, as many AI applications are not plug-and-play and require extensive customized development to adapt to specific scenarios. Additionally, ongoing operational and maintenance costs—such as data management, model retraining, system integration, and troubleshooting—must be factored in.

Shortage of Professionals: The complexity of AI technology demands professionals with expertise in machine learning, deep learning, data science, and related domains. Such talent is scarce within the field of campus security management. To bridge this gap, substantial investment may be needed for staff training or to attract specialized personnel with competitive salaries. A lack of technical knowledge and experience can not only hinder the deployment and maintenance of AI systems but also introduce vulnerabilities in data processing and storage.

Lagging Policies and Regulations: The rapid advancement of AI technology has in many cases outpaced the updating of existing laws and regulations, resulting in policies that lag behind technological developments. This delay can lead to potential ethical and privacy issues, as AI systems raise numerous concerns regarding data collection, processing, and decision-making.

5. Future Trends and Research Directions

5.1. Technology Integration

The further development of artificial intelligence in the field of campus security will rely on the deep integration of various cutting-edge technologies. Multimodal AI can integrate multi-source heterogeneous data such as video, text, audio, sensor data, and behavioral logs to construct a more comprehensive and

robust student safety profile, significantly improving the accuracy of anomaly detection and crisis early warning. Federated Learning enables collaborative modeling across systems and institutions while protecting data privacy, effectively addressing the challenge of "data silos" and promoting multi-party security collaboration. Generative AI can synthesize diverse training data, simulate campus crisis scenarios, and assist in generating personalized intervention strategies, providing more flexible and intelligent decision support for campus security management.

5.2. Paradigm Evolution

Future campus security systems will gradually shift from a passive response model to an intelligent paradigm centered on prediction and prevention. Based on big data and AI analysis, the system can achieve early identification and dynamic risk assessment of student psychological crises, behavioral anomalies, and security threats, enabling truly "pre-incident warning." Furthermore, through deep integration with campus management systems, psychological counseling platforms, and emergency service units, the AI system can initiate automated or semi-automated intervention mechanisms during events—such as real-time warning, activating emergency protocols, and allocating counseling resources—ultimately forming a closed-loop process of "monitoring-warning-intervention-feedback," greatly enhancing the proactivity and response efficiency of campus security.

5.3. Human-Centered Design

As AI becomes more deeply embedded in campus environments, its design must place greater emphasis on human factors. Research should focus on improving model interpretability, enabling administrators, teachers, and even students to understand the decision-making logic of AI, thereby enhancing trust in the system. At the same time, algorithmic bias and decision-making unfairness must be systematically addressed through the use of debiasing algorithms, diverse datasets, and fairness evaluation frameworks. Transparency building also needs to advance simultaneously, including clarifying the scope of data usage, disclosing system design principles and performance boundaries, and ensuring that AI applications operate under democratic supervision and ethical constraints.

5.4. Policy and Governance

To regulate the rational use of AI technology on campus, top-level design and institutional guarantees must be strengthened. Schools should collaborate with policymakers, ethics committees, and technical experts to develop specialized AI ethical guidelines that explicitly prohibit high-risk applications such as large-scale indiscriminate monitoring and emotion recognition, and establish accountability and audit mechanisms. 28 multaneously, strict data governance policies should be introduced to standardize the processes of data collection, storage, use, and sharing, protecting the privacy rights of students and staff. Additionally, regulatory frameworks must remain dynamic to address new risks and ethical challenges arising from rapid technological advancements.

6. Conclusion

Artificial intelligence technology has brought fundamental changes to campus security governance, transitioning it from a traditional model reliant on physical and personnel-based measures to a new intelligent paradigm characterized by data-driven operations, smart early warning, and precise intervention. By integrating multi-source sensing data and advanced algorithms, AI systems enable early insight, dynamic assessment, and rapid response to security threats and psychological crises, significantly expanding the coverage, improving the response speed, and enhancing the management efficacy of campus security.

However, this transformation process still faces a series of core challenges, with ethical 10 ues being particularly prominent. These include privacy erosion due to large-scale monitoring, lack of transparency and fairness in algorithmic decision-making, and the erosion of trust and inhibition of student behavior caused by false positives. If these ethical and social acceptance issues are not properly addressed, AI may not only fail to deliver its intended effectiveness but could also negatively impact the campus atmosphere and student development.

The healthy development of AI in campus security in the future urgently requires breaking down disciplinary and industry barriers to build a cross-sector collaborative community. Relying solely on technologists cannot fully address ethical, legal, and social concerns. It is essential to involve educators,

psychologists, ethicists, policymakers, and student representatives in the process to ensure that the design, deployment, and governance of AI systems align with educational philosophy, respect human dignity, and ultimately contribute to building a safer, healthier, and more inclusive smart campus environment.

References

Abbasi, I. A., Shoaib, M., Alshehri, M., & Aldawsari, M. (2025). Utilizing CBNet to effectively address and combat cyberbullying among university students on social media platforms. Scientific Reports, 15(1).

Atmakuru, A., Shahini, A., Chakraborty, S., Seoni, S., Salvi, M., Hafeez-Baig, A., Rashid, S., Tan, R. S., Barua, P. D., & Molinari, F. (2025). Artificial intelligence-based suicide prevention and prediction: A systematic review (2019–2023). Information Fusion, 114.

Biernesser, C., Ohmer, M. L., Nelson, L., Mann, E., Farzan, R., Schwanke, B., & Radovic, A. (2023). Middle School Students' Experiences with Cyberbullying and Perspectives Toward Prevention and Bystander Intervention in Schools. Journal of School Violence, 22, 339 - 352.

Cao, R. (2022). Promoting Digital Campus to Smart Campus Based on Artificial Intelligence 2022 International Conference on Computer Engineering and Artificial Intelligence (ICCEAI),

Casey, S. M., Varela, A., Marriott, J. P., Coleman, C. M., & Harlow, B. L. (2022). The influence of diagnosed mental health conditions and symptoms of depression and/or anxiety on suicide ideation, plan, and attempt among college students: Findings from the Healthy Minds Study, 2018-2019. Journal of affective disorders(298PA-), 298PA.

Danielsen, S., Strandberg-Larsen, K., Orri, M., Nordentoft, M., Erlangsen, A., & Madsen, T. (2025). Mental health, risk behaviors, and social life factors in relation to adolescents' suicide ideation, plans and attempt. European Child & Adolescent Psychiatry, 34(6).

Dong, B. (2023). Research on the Construction of Campus Security System in Colleges and Universities Guided by the Thought of the New Era. Frontiers in Educational Research.

Gupta, D., Xu, W., Yu, X., Huang, M.-C., & Ieee. (2021, 2021

Jul 27-30). Campus safety and the internet of wearable things: assessing student safety conditions on campus while riding a smart scooter.International Conference on Wearable and Implantable Body Sensor Networks [2021 ieee 17th international conference on wearable and implantable body sensor networks (bsn)]. 17th International Conference on Wearable and Implantable Body Sensor Networks (BSN), Athens, GREECE.

He, C., & Li, Z. (2025). AI-Driven Multimodal Preventive System for Adolescent Mental Health: A Randomized Controlled Trial. American Journal of Preventive Medicine, 69(2-Sup1).

He, Q., Liu, J., Zhou, G., & Gao, M. (2024, 2024

Jul 05-07). Research on Student Behavioral Advanced Warning Based on Campus-Card Consumption Data.ACIS International Conference on Software Engineering Artificial Intelligence Networking and Parallel Distributed Computing-SNPD [27th ieee/acis international summer conference on software engineering artificial intelligence networking and parallel/distributed computing, snpd 2024-summer]. 27th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Beijing, PEOPLES R CHINA.

Jacek Pyzalski, Piotr Plichta, Anna Szuster, & Barlinska, J. (2022). Cyberbullying Characteristics and Prevention—What CanWe Learn fromNarratives Provided by Adolescents and Their Teachers? International Journal of Environmental Research and Public Health. https://doi.org/https://doi.org/10.3390/ijerph191811589

Kaplan, J. (2023). The (In)Effectiveness of Campus Smart Locks for Reducing Crime. Journal of Applied Security Research, 18(1), 86-105. https://doi.org/10.1080/19361610.2021.1915054

Liao, S.-H., Jiang, J.-D., & Yang, C.-F. (2024). Integration of LoRa-enabled IoT infrastructure for advanced campus safety systems in Taiwan. Internet of Things, 28, Article 101347. https://doi.org/10.1016/j.iot.2024.101347

Mason, M. J., Zaharakis, N., & Benotsch, E. G. (2014). Social Networks, Substance Use, and Mental Health in College Students. Journal of American College Health, 62(7), 470-477.

https://doi.org/10.1080/07448481.2014.923428

Myagmar-Ochir, Y., & Kim, W. (2023). A Survey of Video Surveillance Systems in Smart City. Electronics, 12(17), Article 3567. https://doi.org/10.3390/electronics12173567

Niu, Y., Jiang, H., Tian, B., Xiang, H., Liu, Y., Xia, X., & Zhao, Y. (2022). An efficient access control scheme for smart campus. Eai Endorsed Transactions on Scalable Information Systems, 9(6), Article e5. https://doi.org/10.4108/eai.21-3-2022.173712

Patterson, M. S., & Goodson, P. (2018). Social network analysis for assessing college-aged adults' health: A systematic review. Journal of American College Health, 67(1), 59-67. https://doi.org/10.1080/07448481.2018.1462820

Prainsack, B., & Forgó, N. (2024). New AI regulation in the EU seeks to reduce risk without assessing public benefit. Nature medicine, 30(5), 1235-1237.

Rinker, D. V., Krieger, H., & Neighbors, C. (2016). Social Network Factors and Addictive Behaviors Among College Students. Current Addiction Reports, 3(4), 356-367. https://doi.org/10.1007/s40429-016-0126-7

Saliba, S. M. (2024). The University Chaplain: An Often Unrecognised Resource in Suicide Prevention—Initial Qualitative Results from Exploratory Research into the Roles of University Chaplains at One Australian University. Journal of Religion & Health, 63(3).

Srhir, A., Mazri, T., & Benbrahim, M. (2023). Towards secure smart campus: security requirements, attacks and counter measures. Indonesian Journal of Electrical Engineering and Computer Science, 32(2), 900-900. https://doi.org/10.11591/ijeecs.v32.i2.pp900-914

Sutton, H. (2025). Gain insight into potential of artificial intelligence to boost campus safety. Student Affairs Today, 28(1), 4-5. https://doi.org/10.1002/say.31531

Wang, H., Lu, J., Zhao, H., Li, L., & Zhou, X. (2024). Vulnerable conditions syndemic, depression, and suicidal ideation among school children in China: cross-sectional census findings. Child & Adolescent Psychiatry & Mental Health, 18(1).

Wang, Y., Wen, J., Zhou, W., Wu, Q., Wei, Y., Li, H., & Tao, B. (2022). Research on Abnormal Behavior Prediction by Integrating Multiple Indexes of Student Behavior and Text Information in Big Data Environment. Wireless Communications and Mobile Computing, 2022(1). https://doi.org/10.1155/2022/1902155

Yang, C. Y., Liu, J. Y., & Huang, S. (2020). RESEARCH ON EARLY WARNING SYSTEM OF COLLEGE STUDENTS' BEHAVIOR BASED ON BIG DATA ENVIRONMENT. The International Archives of the Photogrammetry Remote Sensing and Spatial Information Sciences, XLII-3/W10, 659-665. https://doi.org/10.5194/isprs-archives-xlii-3-w10-659-2020

Yang , , K., Zhao , , J., , , J. L., & Xia, C. (2025). Real-time intelligent fire identification and early warning method based on campus surveillance video. Proceedings in civil engineering.

Zhang, L., & Xu, L. (2021). Research on Earthquake Disaster Emergency Rescue Method based on Smart Campus Face Recognition. Journal of Catastrophology, 36(4), 152-155,162, Article 1000-811x(2021)36:4<152:Jyzhxy>2.0.Tx;2-2. <Go to ISI>://CSCD:7081139

Zhou, F., Lv, H., Zhou, K., Sheng, M., & Jiang, J. (2024). Innovative Application and Societal Impact of AI in Student Behavior Early Warning Systems within Smart Campuses. Philosophy and Social Science, 1(5), 33-40. https://doi.org/10.62381/p243506

Zuberi, A. H., Anees, A., Anjum, N., Warsi, A. H., Khan, P. R., & singh, S. K. (2025). Machine Learning-Based Sentiment Analysis for Suicide Prevention and Mental Health Monitoring in Educational Institutions. Journal of Neonatal Surgery.

Artificial Intelligence in Campus Security and Crisis prediction: A Review of Current Applications and Future Trends

ORIGINALITY REPORT

5%	4%	3%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	publications.eai.eu Internet Source	1%
2	ijeecs.iaescore.com Internet Source	1%
3	mmcalumni.ca Internet Source	<1%
4	"Advances in Computational Vision and Robotics", Springer Science and Business Media LLC, 2025 Publication	<1%
5	He-Yau Kang, Amy H. I. Lee, C.-Y. Yang. "A fuzzy ANP model for supplier selection as applied to IC packaging", Journal of Intelligent Manufacturing, 2010 Publication	<1%
6	"Smart Computing Paradigms: Artificial Intelligence and Network Applications", Springer Science and Business Media LLC, 2024 Publication	<1%
7	Steven Engler, Michael Stausberg. "The Routledge Handbook of Research Methods in the Study of Religion", Routledge, 2021 Publication	<1%
8	Submitted to University of Idaho Student Paper	<1%

9	journal.achsm.org.au Internet Source	<1 %
10	link.springer.com Internet Source	<1 %
11	scholarworks.wm.edu Internet Source	<1 %
12	www.livemint.com Internet Source	<1 %
13	Debasis Chaudhuri, Jan Harm C Pretorius, Debashis Das, Sauvik Bal. "International Conference on Security, Surveillance and Artificial Intelligence (ICSSAI-2023) - Proceedings of the International Conference on Security, Surveillance and Artificial Intelligence (ICSSAI-2023), Dec 1–2, 2023, Kolkata, India", CRC Press, 2024 Publication	<1 %
14	uwe-repository.worktribe.com Internet Source	<1 %
15	www.aeph.press Internet Source	<1 %
16	Anirudh Atmakuru, Alen Shahini, Subrata Chakraborty, Silvia Seoni et al. "Artificial intelligence-based suicide prevention and prediction: A systematic review (2019–2023)", Information Fusion, 2025 Publication	<1 %
17	Cecilia Ka Yuk Chan, Tom Colloton. "Generative AI in Higher Education - The ChatGPT Effect", Routledge, 2024 Publication	<1 %

18	Mohiuddin Ahmed, Nazim Choudhury. "Cybersecurity for Internet of Health Things", CRC Press, 2025 Publication	<1 %
19	Naveen Kumar Chaudhary, Archana Patel, Abinash Mishra, Chothmal Kumawat. "Artificial Intelligence and Digital Forensics - Advancements, Applications, Challenges, and Solutions", CRC Press, 2025 Publication	<1 %
20	jneonatalsurg.com Internet Source	<1 %
21	oaktrust.library.tamu.edu Internet Source	<1 %
22	www.frontiersin.org Internet Source	<1 %
23	Al-Sakib Khan Pathan. "Securing Cyber-Physical Systems", CRC Press, 2019 Publication	<1 %
24	Mohamed Lahby, Al-Sakib Khan Pathan, Yassine Maleh. "Combatting Cyberbullying in Digital Media with Artificial Intelligence", CRC Press, 2023 Publication	<1 %
25	Ruixia Cao. "Promoting Digital Campus to Smart Campus Based on Artificial Intelligence", 2022 International Conference on Computer Engineering and Artificial Intelligence (ICCEAI), 2022 Publication	<1 %
26	ebin.pub Internet Source	<1 %

27	Rishabha Malviya, Swati Verma, Harish Kumar. "Intelligent Data Analytics in Media Communication to Improve Public Health Care", Apple Academic Press, 2025 Publication	<1 %
28	Wasswa Shafik, Adel Ben Youssef, Chithirai Pon Selvan, Pushan Kumar Dutta. "Sustainable Healthcare Systems in Africa - Technologies, Practices, and Management", Routledge, 2025 Publication	<1 %
29	www.hindawi.com Internet Source	<1 %
30	www.science.gov Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		