Scientific Research Publishing

Open Journal of Applied Sciences, 2026, 16(3), 832-853
https://www.scirp.org/journal/ojapps
ISSN Online: 2165-3925
ISSN Print: 2165-3917

Design of an Intelligent Campus Surveillance System, Based on Cognitive Security and the Internet of Things, for the Detection of Suspicious Activities

Chely Ongondza[1], Vivien Armel Eyangolo[1], Katalay Pierre Kafunda[2]

[1]Department of Bachelor's Degrees, Faculty of Applied Sciences, Denis Sassou Nguesso University, Brazzaville, Republic of the Congo
[2]Faculty of Science, Laboratory of Mathematics and Computer Science, University of Kinshasa, Kinshasa, Democratic Republic of the Congo
Email: cheongondza@gmail.com, vivieneyangolo@yahoo.fr, Pierre.kafunda@unikin.ac.cd

How to cite this paper: Ongondza, C., Eyangolo, V.A. and Kafunda, K.P. (2026) Design of an Intelligent Campus Surveillance System, Based on Cognitive Security and the Internet of Things, for the Detection of Suspicious Activities. *Open Journal of Applied Sciences*, **16**, 832-853.
https://doi.org/10.4236/ojapps.2026.163051

Received: December 2, 2025
Accepted: March 13, 2026
Published: March 17, 2026

Abstract

University campus security has become a major issue with the increasing digitization and interconnection of infrastructure. This article proposes the design of an intelligent surveillance system based on a cognitive security approach integrating the Internet of Things (IoT). The model combines computer vision, behavioral analysis, and machine learning to detect suspicious movements and abnormal behavior in real time. IoT sensors collect data from multiple sources (videos, motion detectors, access control devices), while the cognitive layer provides contextual interpretation and adaptive decision-making. The proposed architecture aims to improve responsiveness, detection accuracy, and resilience against physical and cyber threats, while respecting the confidentiality and reliability constraints inherent in smart environments.

Keywords

Cognitive Security, Internet of Things (IoT), Suspicious Activity Detection, Computer Vision, Machine Learning

1. Introduction

The rise of digital technologies and the Internet of Things (IoT) has profoundly transformed the management and security of university environments. Smart campuses now integrate a multitude of connected devices (cameras, sensors, ac-

cess control systems, wireless networks) that continuously generate vast amounts of data [1]. This interconnectedness paves the way for new models of intelligent surveillance, capable of ensuring proactive and adaptive security.

However, the proliferation of access points and the increasing complexity of networks also amplify the risks of physical and cyber threats. Traditional security approaches, based on static rules and human intervention, are proving inadequate in the face of dynamic behaviors and rapidly evolving threats. In this context, it is becoming essential to design systems capable of learning, analyzing, and reacting in real time to unusual situations.

The cognitive security approach addresses this need by combining the perception capabilities of the Internet of Things (IoT), the analytical power of artificial intelligence, and cybersecurity principles. It enables the development of systems where the physical and digital layers cooperate to detect, interpret, and anticipate suspicious behavior.

The aim of this article is to propose an intelligent campus surveillance architecture, based on cognitive security and IoT technologies, to improve the detection of abnormal movements while ensuring data protection and network resilience. The study focuses on modeling the interactions between sensors, cognitive analytics modules, and autonomous decision-making mechanisms.

This contribution builds upon previous work on intelligent security systems and explores new perspectives for the automated management of connected environments.

2. Computer Vision

Computer vision is a branch of artificial intelligence (AI) that allows machines to see, analyze, and interpret the content of images or videos, in a manner similar to human perception.

It aims to give computers the ability to understand the visual world in order to make decisions or perform actions based on what they "see" [2].

2.1. Main Objectives

- Detection: Identify the presence of objects or shapes in an image (e.g., detecting faces, vehicles, industrial defects).
- Recognition: Classify or name detected objects (e.g., recognize a person, an animal, or a road sign).
- Tracking: Follow the movement of an object or person in a video sequence.
- Scene Analysis: Understand the overall context of an image (e.g., recognizing activities, analyzing behaviors).

2.2. Techniques Used

Computer vision relies on several methods derived from:

- Machine learning, and especially deep learning (convolutional neural networks or CNNs).

- Image processing, to improve quality, detect edges, or extract visual features.
- Geometric analysis and 3D modeling, to estimate the depth, position, or shape of objects.

2.3. Practical Applications

- Facial recognition and biometrics.
- Autonomous vehicles and driver assistance systems.
- Intelligent surveillance and security.
- Image-assisted medical diagnosis.
- Industry 4.0 (automated inspection, robotics).
- Augmented reality and human-machine interaction.

2.4. The Importance of Computer Vision

Computer vision now occupies a central place in the development of artificial intelligence and the digital transformation of societies. Its importance lies in its ability to allow machines to understand the visual world automatically and intelligently, paving the way for countless applications in scientific, industrial, medical, and social fields.

2.5. Automation and Efficiency Gains

Computer vision can replace or assist human perception in repetitive, dangerous, or highly precise tasks.

Examples: product inspection on production lines, infrastructure monitoring, automated quality control, etc.

➞ Result: reduced human error, improved productivity, and lower operating costs.

2.6. Security and Protection [3]

It plays a key role in public safety and physical cybersecurity, thanks to facial recognition, intrusion detection, and the analysis of suspicious behavior in sensitive areas.

➞ This strengthens risk prevention and responsiveness to threats.

2.7. Innovation in Transportation and Healthcare

In autonomous vehicles, computer vision enables pedestrian detection, sign reading, and understanding of the road environment.

In the medical field, it assists doctors in diagnosis using images (X-rays, MRIs, CT scans), enabling faster and more accurate analyses.

➞ It saves lives and improves the quality of care.

2.8. Accessibility and Inclusion

Computer vision promotes social inclusion: it helps visually impaired people orient themselves through object and text recognition, and facilitates human-ma-

chine communication through gestures and expressions.

2.9. A Source of Intelligence for the Future

By combining computer vision, deep learning, and robotics, we are paving the way for autonomous systems capable of understanding, learning, and interacting with their environment. This represents a fundamental pillar for smart cities, Industry 4.0, and intelligent security systems.

In summary:

The importance of computer vision lies in its ability to give machines "sight," improve decision-making, and transform industries by making systems smarter, safer, and more efficient.

2.10. Safety and Security

The terms safety and security both refer to measures aimed at protecting people, property, and systems, but they differ in the nature of the threats they address.

Security

Security (from the Latin securitas) concerns protection against intentional acts, that is, threats caused by human beings.

It aims to prevent, detect, and counter malicious or deliberate actions.

Examples:

- Cyberattacks, hacking, data theft;
- Terrorism, sabotage, burglary;
- Fraud, scams, malicious manipulation.

➞ Objective: to prevent or limit damage caused by intentional acts.

2.11. Safety

Safety (from the Latin securitas, but in the sense of "stability") concerns protection against unintentional accidents, failures, or errors.

It addresses technical, human, or environmental risks that can threaten a system without any intent to harm.

Examples:

- Failure of industrial equipment or software;
- Transportation accident;
- Human error or power outage;
- Natural hazards (fires, floods, earthquakes).

➞ Objective: to guarantee the reliability, robustness, and continuity of operations despite unforeseen events.

2.12. Complementarity of Safety and Security

In modern organizations, these two dimensions are inseparable.

An infrastructure (digital or physical) must be:

- Safe, to function correctly and prevent accidents;
- Secure, to withstand attacks and intrusions.

Example: a computer network must be safe (without failures, well-configured) and secure (protected against cyberattacks).

In summary:

- Safety = protection against accidents or unintentional errors.
- Security = protection against malicious and intentional acts.

Both are essential to ensure the overall protection of people, property, and systems.

2.13. Operational Effectiveness in Disseminating Best Practices in Cognitive Security

Operational effectiveness refers to an organization's ability to achieve its objectives optimally by efficiently utilizing its human, technical, and organizational resources.

In the context of cognitive security, this translates to how an institution, such as a university or a company, manages to integrate, disseminate, and sustainably promote best practices in cybersecurity among its members.

2.14. Cognitive Security: Primarily a Human Issue

Cognitive security relies on users' understanding, vigilance, and behavior in the face of digital threats.

It aims to raise awareness of risks (phishing, social engineering, digital negligence, etc.) and encourage safe habits in the use of technology.

- Operational effectiveness, therefore, depends on the ability to bring about lasting changes in behavior.

3. Factors of Operational Effectiveness

For a strategy to disseminate best practices in cognitive security to be truly effective, several levers must be mastered:

- a. Targeted awareness:

Adapt messages to different profiles (students, faculty, administrative staff) so that everyone understands the issues and their role.

- b. Ongoing training:

Integrate cognitive security into training programs, seminars, and the university's daily activities.

- c. Effective internal communication:

Use a variety of media (posters, emails, digital platforms, interactive campaigns) to disseminate best practices regularly and in an engaging way.

- d. Monitoring and evaluation:

Implement indicators (participation rates, incidents avoided, improvement in digital behavior) to measure the real impact of the actions taken.

4. Benefits of Operational Effectiveness

A well-managed dissemination of cognitive security best practices enables:

- A significant reduction in cybersecurity incidents caused by human error;

- Strengthening digital culture and trust within the organization;
- Improving institutional resilience to cyber threats;
- Fostering a secure digital environment conducive to innovation and learning.

In summary:

Operational effectiveness in disseminating cognitive security best practices consists of transforming awareness into concrete, measurable, and sustainable behaviors [4].

This is a strategic approach that combines training, communication, and change management to make each user an active participant in collective digital security.

5. How Computer Vision Works in Disseminating Best Practices in Cognitive Security?

Computer vision is an artificial intelligence technology that allows machines to analyze, interpret, and understand images or videos. In the context of cognitive security, it can play a key role in observing, evaluating, and reinforcing users' security behaviors in a digital or physical environment.

5.1. General Operating Principle

Computer vision relies on several successive technical steps.

5.1.1. Image or Video Acquisition

Cameras, sensors, or surveillance systems capture visual streams from the environment (laboratories, computer rooms, access areas, etc.).

5.1.2. Image Preprocessing

Images are cleaned and optimized (contrast enhancement, noise reduction, resizing) to facilitate analysis.

5.1.3. Detection and Recognition

Deep learning algorithms (such as convoluted neural networks—CNCs) identify specific objects, faces, gestures, or behaviors.

5.1.4. Behavioral and Decision Analysis

The system interprets visual data to detect risky behaviors (e.g., unauthorized access, leaving workstations locked, failure to comply with safety rules).

5.1.5. Feedback and Continuous Improvement

The information collected can be used to inform awareness programs, adjust training, or trigger alerts in case of suspicious behavior.

5.2. Application to Cognitive Security

Computer vision supports the dissemination of the best practices in cognitive security through several concrete applications:

1) Intelligent monitoring: automatically detecting behaviors that violate cybersecurity rules in sensitive areas (for example, someone leaving a connected work-

station unattended).

2) Immersive training: using image and gesture recognition in educational simulations to train users to adopt good security practices.

3) Objective assessment: non-intrusively measuring the implementation of digital security guidelines in work or study environments.

4) Proactive protection: combining computer vision with alert systems to prevent human error or intrusions before they cause an incident.

6. Advantages in Disseminating Best Practices

1) Enhanced cognitive vigilance through continuous observation and contextual reminders;

2) Automation of human error detection, contributing to a reduction in the risk of negligence;

3) Personalized awareness training, adapting messages or training based on observed behaviors;

4) Improved safety culture through a proactive and educational technological approach.

In summary: The role of computer vision in disseminating best practices for cognitive safety relies on the intelligent analysis of images to observe, correct, and reinforce safe behaviors.

It allows for the combination of technology and education to transform individual vigilance into a collective culture of digital safety [5].

7. Mathematical Formalisms of Computer Vision in the Dissemination of Best Practices for Cognitive Security

Computer vision relies on a solid foundation of mathematical modeling, enabling the transformation of visual data (images, videos) into actionable information to enhance cognitive security.

At Denis Sassou Nguesso University, these formalisms can be used to observe, analyze, and improve cybersecurity behaviors within a digital ecosystem based on secure Wi-Fi, multi-factor authentication (MFA), and Zero Trust architecture.

7.1. Mathematical Representation of the Image

A digital image can be modeled as a matrix:

$$I(x,y)=\begin{vmatrix} p_{11} & p_{12} & p_{1n} \\ p_{21} & p_{22} & p_{2n} \\ p_{m1} & p_{m2} & p_{3n} \end{vmatrix} \tag{1}$$

where each p_{ij} represents the light intensity of the pixel at that position.

Image transformations (blurring, edge detection, filtering) use matrix operations such as convolution:

$$x^{i}(x,y)=\sum_{i=-k}^{k}\sum_{j=-k}^{k} I(x+i,y+j)\cdot K(i,j) \tag{2}$$

where K is a convolution kernel (filter).

7.2. Feature Extraction

To detect behaviors or objects (e.g., detecting an unauthorized user), computer vision extracts features from the image.

These features (edges, textures, points of interest) are represented by feature vectors:

$$f = [f_1, f_2, \cdots, f_n] \tag{3}$$

These vectors feed into machine learning models (neural networks, SVMs, k-means) that learn to distinguish between conforming and risky behaviors.

7.3. Deep Learning Modeling

Convolutional neural networks (CNNs) are widely used in computer vision.

Each layer of the CNN applies a mathematical transformation:

$$a^{(l)} = f\left(w^{(l)} a^{(l-1)}\right) + b^{(l)} \tag{4}$$

where:

- $W^{(l)}$ is the weight matrix,
- $b^{(l)}$ is the bias,
- f is the activation function (ReLU, sigmoid, etc.),
- $a^{(l)}$ is the output of layer l.

These models allow for the recognition of faces, gestures, or behaviors related to digital security (e.g., a user failing to activate MFA or connecting to an unsecured network) [6].

7.4. Application to University Cognitive Security

In a university environment integrating secure Wi-Fi, MFA, and Zero Trust:

- Smart cameras, coupled with computer vision models, can analyze physical and digital behaviors (access, posture, interactions with workstations).
- Statistical models (such as Bayesian probabilities) can estimate the level of compliance of a behavior based on visual and access data.
- These observations then feed into cognitive awareness-raising mechanisms: notifications, reminders of good practices, adjustment of the level of access according to the observed behavior.

7.5. Integration into the Zero Trust Model

The mathematical formalism supports the Zero Trust principle, where trust is never implicit:

Each access or behavior is evaluated according to a risk score (RRR) calculated by:

$$P(Sécurité|Données) = \frac{P(Données|Sécurité) \times P(Sécurité)}{P(Données)} \tag{5}$$

where:

- Cv = vision score (observed visual behavior),
- Cn = network score (activity on the secure Wi-Fi network),
- Cb = biometric score (MFA, facial recognition),
- αi\alpha_iαi = weighting coefficients.

If $R >$ Rthreshold, access is denied or subject to enhanced authentication.

In summary:

The mathematical formalisms of computer vision enable us to:

- Model and analyze visual behaviors related to cybersecurity;
- Integrate these analyses into a Zero Trust approach to dynamically adjust trust levels;
- Enhance cognitive security through detection, awareness, and intelligent feedback. Thus, the combination of computer vision, MFA, secure Wi-Fi, and Zero Trust architecture provides Denis Sassou Nguesso University with an integrated, proactive, and intelligent approach to cybersecurity.

8. The Internet of Things (IoT)

Refers to all connected devices capable of collecting, exchanging, and processing data via the internet.

In a university context, the IoT encompasses computers, tablets, smartphones, surveillance cameras, environmental sensors, access cards, Wi-Fi hotspots, and smart learning equipment.

These interconnected objects constitute a living digital infrastructure, essential to the digital transformation of Denis Sassou Nguesso University.

However, this increased connectivity requires enhanced cybersecurity, both technical and cognitive, that is to say, based on user vigilance and behavior.

8.1. Role of IoT in Cognitive Security

IoT can play a major role in disseminating best practices in cognitive security by making security more visible, smarter, and more interactive.

8.1.1. Intelligent Monitoring and Behavioral Learning

IoT sensors can detect risky behaviors (unauthorized access, connection to an unsecured network, failure to log out of an account, etc.) and send real-time alerts.

8.1.2. Cognitive Feedback and Awareness

Connected devices (interactive whiteboards, smartphones, information displays) can broadcast personalized awareness messages when non-compliant behaviors are detected.

8.1.3. Contextual Risk Analysis

By combining data from connected devices, secure Wi-Fi, and MFA systems, the university can establish a cognitive risk profile for each user, in order to adapt security measures (e.g., strengthening authentication if unusual behavior is observed).

8.2. Interaction with Cybersecurity Technologies

8.2.1. Secure Wi-Fi

The IoT relies on a high-performance and secure wireless network (WPA3, network segmentation, stream encryption).

Secure Wi-Fi guarantees the confidentiality of data exchanged by connected devices and limits the risk of intrusion into the university ecosystem [7].

8.2.2. Multi-Factor Authentication (MFA)

The IoT facilitates the implementation of contextual MFA:

Connected objects (bracelets, smartphones, RFID badges) can serve as physical or biometric authentication factors, strengthening user identity verification while improving the cognitive experience (perceived security and user engagement).

8.2.3. Zero Trust Architecture

In a Zero Trust model, each connected object must be authenticated, verified, and authorized before accessing the network.

The IoT provides behavioral data to feed trust algorithms:

$$T = f\left(Id, Cn, Au\right) \tag{6}$$

where:

- Id = device or user identity,
- Cn = network context (location, time, connection type),
- Au = observed activity or behavior.

If the confidence score T is below a defined threshold, multifactor authentication (MFA) or access restriction is applied.

8.3. IoT and Cognitive Security: Towards an Integrated Approach

At Denis Sassou Nguesso University, the IoT can be integrated into a three-dimensional cognitive security strategy:

8.3.1. Technical

Deployment of a network of secure, interoperable, and monitored connected objects.

8.3.2. Behavioral

Training users to understand the risks associated with connected objects and to adopt best practices (do not share passwords, avoid open networks, keep up to date).

8.3.3. Cognitive

Using the IoT to strengthen digital awareness through intelligent alerts, security reminders, and interactive training scenarios.

9. Expected Benefits

- Strengthening the university's digital resilience.
- Early detection of risky behaviors.
- Dynamic and personalized user awareness training.

- Concrete application of the Zero Trust principle through real-time traceability and analysis.
- Creation of a self-learning cognitive security ecosystem, combining technology, behavior, and human learning.

In summary:

The Internet of Things (IoT) is a strategic driver for disseminating best practices in cognitive security at Denis Sassou Nguesso University.

By interacting with secure Wi-Fi, multi-factor authentication (MFA), and Zero Trust architecture, the IoT enables the construction of a smart digital environment capable not only of protecting data but also of training and empowering users to address cyber threats.

10. General Context

The objective is to create an intelligent ecosystem, a CNN, that helps:

- Detect abnormal behavior;
- Analyze;
- Promote cognitive security best practices to users;
- Strengthen Zero Trust policies.

Reminder: What is a CNN?

A CNN enables:

- Image and pattern recognition;
- Spatiotemporal data classification, etc.

But it can also be applied to cognitive cybersecurity, both against and by detecting threats.

10.1. CNN Application in a Cognitive Security Framework

Detection of Abnormal Behavior (IoT and Users)

- The CNN analyzes Wi-Fi data streams.
- It learns normal behavior.
- It detects abnormal behavior that blocks access.
- The CNN continuously monitors Wi-Fi network connections and MFA authentication.
- It can detect suspicious patterns.
- It helps strengthen cognitive awareness: are you in a Zero Trust architecture?
- It is part of the behavioral analysis engine.
- It classifies requests according to their risk level.
- It provides an adaptive trust score.

It integrates with a cognitive Zero Trust gateway.

Figure 1: Simulation Results and Analysis

Simulations performed using the CNN application architecture within a cognitive security framework for smart campuses demonstrate how sensors from different objects communicate with each other to collect networked data. The integration of the CNN architecture ensures the extraction of behavioral patterns, dimensionality reduction and classification (normal and abnormal), and the zero-

module Trust + cognitive AI for adaptive access control, alerts, and automated actions to train and raise user awareness through the dissemination of best practices via IoT screens, emails, and notifications.

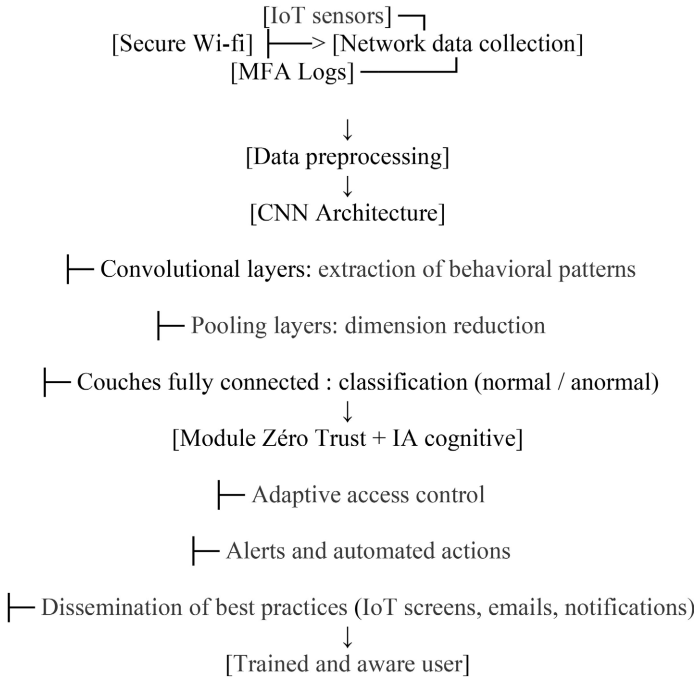

Figure 1. First application architecture of the CNN in a cognitive security framework within the smart campus.

10.2. Functioning of the CNN in Campus Cognitive Security

The CNN acts as the cognitive brain at the heart of the security system.

Step 1: Data Collection

- R (with)
- M (or)
- IoT Objects (c)
- Record (a)

Step 2: Processing by the CNN

- The CNN model learns the usual behaviors.
- It adapts new data to known patterns.
- If it detects unusual or risky behavior.

AND

The system provides an appropriate response:

- Notification or reminder of best practices.
- Mandatory MFA re-authentication.
- Invitation to attend awareness training.

Table 1: Results obtained after functional analysis of the CNN in campus cognitive safety

The CNN analyzes traffic to detect abnormal connection patterns, identifies suspicious authentication attempts and triggers preventative measures, feeds the

Zero Trust gateway with risk scores for each user or device and triggers the dissemination of personalized advice based on the profile and observed behavior.

Table 1. Functioning of the CNN in campus cognitive security.

Element	Role in the ecosystem	Interaction with CNN
Secure Wi-Fi (WPA3)	Collection of traffic and access data	CNN analyzes the traffic to detect abnormal connection patterns.
MFA (Multi-Factor Authentication)	Verifies user identity	CNN detects suspicious authentication attempts and triggers preventative measures
Zero Trust	Ne fait confiance à aucun appareil par défaut	The CNN feeds the Zero Trust gateway with risk scores for each user or device.
Cognitive IoT (sensors, screens, kiosks)	Disseminate educational messages	CNN triggers the dissemination of personalized advice based on the profile and observed behavior.

Figure 2: The second application architecture of the CNN in the cognitive security of the smart campus comprises secure Wi-Fi with multi-factor authentication (MFA) and internet-connected devices for data collection and preprocessing. It is combined with convolutional neural networks and cognitive artificial intelligence for anomaly detection and classification of normal and abnormal behavior. A zero-trust application with dynamic access control is used to initiate preventative actions (MFA, blocking).

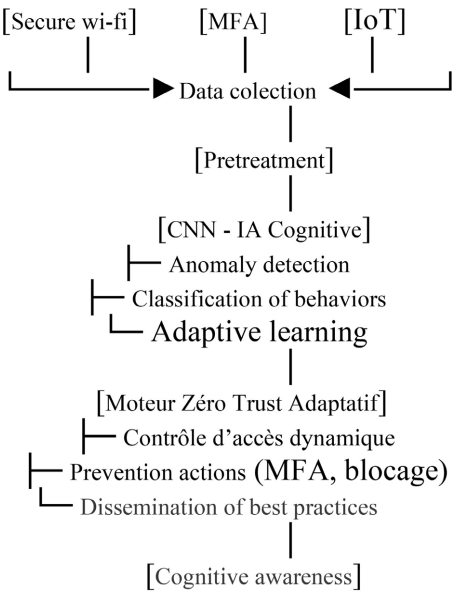

Figure 2. Functioning of the CNN in campus cognitive security.

Table 2: CNN Results in the Cognitive Security of an Intruder (Student)

A student logs in from an unknown device. The CNN detects the abnormal pattern, and the system sends a message to "enable MFA to protect your account".

An IoT camera sends unusual traffic. The CNN detects the IoT anomaly, and the system isolates this sensor using the Zero Trust application and notifies the administrator.

Table 2. Results obtained from the CNN regarding the cognitive security of an intruder (student) gaining abnormal access to this smart campus.

Situation observed	CNN Analysis	System action
A student logs in from an unknown device	Abnormal pattern detection	Sending a message "Enable MFA to protect your account"
An IoT camera is sending unusual traffic	IoT Anomaly Detection	Sensor isolation (Zero Trust) and administrator notification
Multiple MFA authentication failures	CNN model identifies a risk of attack	Temporary blockage and reminder of safety instructions
Wi-Fi connection in an unusual location	CNN detects a change in behavior	Additional check + educational message

Table 3: Key element and function in the operation of the CNN in Security

The convolutional neural network's main role is to learn and detect risky behaviors. Secure Wi-Fi protects the wireless network. MFA verifies identities and strengthens trust. Zero Trust enables dynamic access control. Cognitive diffusion allows for the automatic training and awareness-raising of users.

Table 3. Key element and function in the operation of the CNN in the cognitive security of the campus.

Key element	Function
CNN (convolutional neural network)	It learns and detects risky behaviors.
Secure Wi-Fi	Secure Wi-Fi
MFA	Verifies identities and builds trust.
Zéro Trust	Enables dynamic access control
Cognitive diffusion	It automatically trains and educates users.

10.3. Scientific Context and Objective of the CNN Model

The Denis Sassou Nguesso University aims to implement an intelligent cognitive cybersecurity platform:

- Analyzes the digital behaviors of users and IoT devices connected to secure Wi-Fi;
- Automatically detects behavioral anomalies (with Broadcasts cognitive awareness messages).

The CNN model is the core analytical tool, identifying patterns of normal and abnormal behavior. A multi-layered CNN comprises:

1) An input layer.
2) Several convolutional layers.
3) Pooling layers.
4) One or more fully connected layers.

5) An output layer:

Consider a set of input data.

Or: $X \in R^{H\times L\times C}$.

11. Convolution Operation

$$Y[n]=(x\cdot x\cdot h)[n]=\sum_{k=\infty}^{\infty} x|h|[n-k] \tag{7}$$

where x is the input, h the impulse response, and k the summation index.

After convolution, a nonlinear function, often ReLU, is applied.

$$A(l)_{i,j,k} = f\left(Z(l)_{i,j,k}\right)=\max\left(0,Z(l)_{i,j,k}\right) \tag{8}$$

This function allows the model to capture complex and non-linear behaviors (e.g., rare fraudulent connections).

And pooling reduces the data size while preserving dominant patterns.

$$P(l)_{i,j,k} = \max_{(m,n)\in R} A(l)_{(i+m-1),(j+n-1),k} \tag{9}$$

The outputs of the convolutional and pooling layers are flattened:

$$Z^{(l)} = w^{(l)}\cdot vec\left(P^{(l-1)}\right)+b^{(l)} \tag{10}$$

The model produces a prediction:

$$Yi=\frac{\sum e^{z(l)}}{\sum ie^{z(l)}} \tag{11}$$

where each I represents the probability of a behavior class:

Table 4: Presents the probability of a behavior class in the convolution.

C_1 signifies normal behavior (Co), C_2 signifies suspicious activity (Acti) and (C_3) signifies critical threat, *i.e.*, intrusion via the Internet of Things.

Table 4. Representation of the probability of a behavior class in the convolution.

Class	Interpretation
(C_1)	Normal behavior (Co)
(C_2)	Suspicious Activity (Acti_)
(C_3)	Critical threat (e.g. IoT intrusion)

11.1. The 3rd Application Architecture of the CNN for Cognitive Security (Wi-Fi, MFA, Zero Trust) of the Smart Campus

Table 5: The 3rd application architecture of the CNN for cognitive security (Wi-Fi, MFA, Zero Trust) of the smart campus with input data

After inputting WPA3 logs, IP addresses, session duration, and location to the secure Wi-Fi network, the CNN analyzes network traffic and detects anomalous connections. After inputting failed login attempts, device type, and connection frequency in the MFA (Multi-Factor Authentication) domain, the CNN detects suspicious login behavior. After inputting access data, behavioral signatures, and

IoT traffic in the Zero Trust domain, the CNN assigns a dynamic trust score to each user/device.

Table 5. The 3rd application architecture of the CNN for cognitive security (Wi-Fi, MFA, Zero Trust) of the smart campus.

Domain	Role of the CNN	Input data
Secure Wi-Fi	Analysis of network flows, detection of abnormal connections.	WPA3 logs, IP addresses, session duration, location.
MFA (Multi-Factor Authentication)	Detection of suspicious login behavior	Failed attempts, device type, connection frequency
Zero Trust	Assigning a dynamic trust score to each user/device	Access data, behavioral signatures, IoT traffic
Cognitive security	Automatic generation of educational messages based on risk level	User profile, interaction history, awareness level

11.2. Conceptual Architecture

Figure 3: Conceptual Architecture

This secure Wi-Fi (WPA3) collects data from the external environment, including multi-factor authentication and associated logs from internet-connected devices, as well as a Zero Trust system that preprocesses and normalizes the data. It is equipped with a multi-layer convolutional neural network (CNN) that extracts behavioral characteristics, performs dimensionality reduction, and classifies the data. This results in a risk score and a Zero Trust alert.

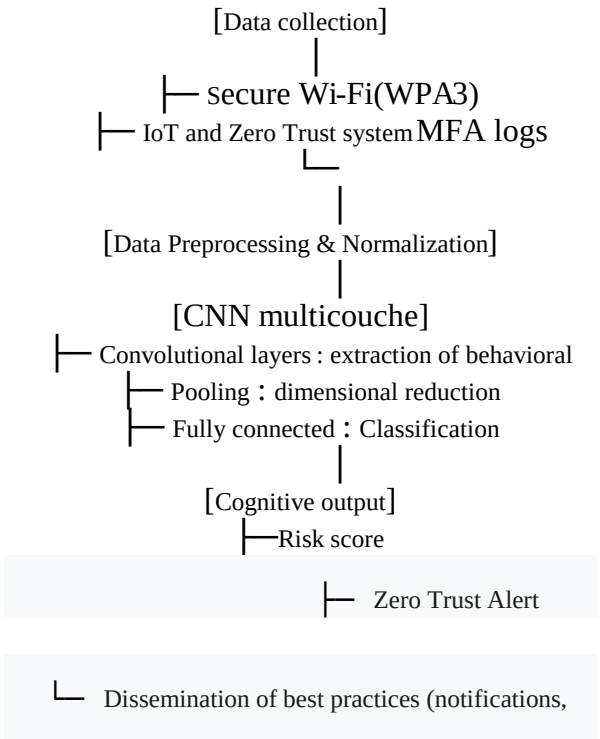

Figure 3. Conceptual architecture.

11.2.1. Cognitive Interpretation and Intelligent Dissemination

The CNN powers a cognitive dissemination engine, which:

1) Analyzes detected abnormal behaviors;

2) Assesses the user's cognitive risk level (low, medium, high);

3) Automatically disseminates appropriate messages:

- Low level → reminder of a best practice;
- Medium level → MFA recommendation.

High level → temporary block + short online training.

11.2.2. Advantages of This Formalism

Table 6 presents the advantages Mathematical rigor enables precise and measurable supervised training.

- Adaptability allows the CNN to learn and adapt to the local behaviors of campus users.
- Interoperability ensures compatibility with Zero Trust policies and MFA authentication.
- Augmented human cognition enables students and staff to receive personalized and automated security training.

Table 6. Advantages of this formalism.

Appearance	Profit
Mathematical rigor	Enables precise and measurable supervised training.
Adaptability	The CNN learns and adapts to the local behaviors of campus users.
Interoperability	Compatible with Zero Trust policies and MFA authentication.
Augmented human cognition	Students and staff receive personalized and automated safety training.

12. Contribution of the Work [8]

In the context of a connected university where digital transformation is accelerating, the proliferation of IoT devices, personal terminals, and online platforms exposes Denis Sassou Nguesso University to new digital threats.

Users (students, teachers, administrative staff) are becoming key players in security. However, users' limited ability to spontaneously adopt good security practices is a significant challenge.

This work makes a scientific, technical, and pedagogical contribution to the intelligent cognitive security ecosystem:

- A unified Wi-Fi network.
- Multi-factor authentication (MFA).
- A Zero Trust architecture.

This work proposes an integrated cognitive security architecture.

With:

- Development of a conceptual model for cognitive cybersecurity.
- Integration of a multi-layered CNN model for anomaly detection in network behavior (Wi-Fi, MFA, IoT).
- Implementation of a cognitive decision engine.

13. Securing the University Network (Secure Wi-Fi + MFA)

This work contributes to strengthening access security through:

- Implementation of a WPA3-Enterprise Wi-Fi network with centralized authentication (RADIUS);
- VLAN segmentation;
- Introduction of multi-factor authentication (MFA);
- Reduction of the risk of identity theft and session hijacking.

The proposed architecture applies the principle of "Never trust, always verify."

1) Support

- Definition of a dynamic trust assessment model.
- Association of the CNN (Cognitive Network).
- Development of an adaptive micro-segmentation logic for the network based on risk levels.

The project is not limited to technical security: it also addresses behavioral and cognitive security.

2) Within

- Development of a cognitive dissemination system.
- Personalization of educational messages according to the user profile.
- Creation of a repository of best practices for inspectors.

3) The work proposes a methodology for integrating cognitive cybersecurity:

- Collect.
- Classify behaviors.
- Integrate CNNs into a Zero Trust cognitive architecture.
- Reduce risky behaviors.

14. Contribution

Impact on Denis Sassou Nguesso University

- Implementation of a smart digital infrastructure hub.
- Creation of an experimental prototype for university-level cognitive cybersecurity.
- Strengthening of digital resilience.
- Development of a shared security culture.
- Replication.
- Contribution to digital sovereignty and training in cognitive cybersecurity.

Scientific basis for future research in AI applied to behavioral security.

Table 7: Impact on Denis Sassou Nguesso University

The implementation of this infrastructure offers the following types of contributions:

- On the technical side, there is the integration of secure Wi-Fi + MFA + Zero Trust to achieve a resilient and intelligent network;
- On the scientific side, there is multi-layered CNN modeling for cognitive security to detect behavioral anomalies;
- On the educational side, there is a cognitive dissemination system for best practices to provide ongoing user training;
- On the institutional side, there is improved cybersecurity governance to achieve a sustainable digital policy outcome.

Table 7. Impact on Denis Sassou Nguesso University.

Axis	Type of contribution	Concrete result
Technical	Secure Wi-Fi integration + MFA + Zero Trust	Resilient and intelligent network
Scientist	Multilayer CNN modeling for cognitive safety	Detection of behavioral anomalies
Educational	Cognitive dissemination system for best practices	Continuing user training
Institutional	Improving cybersecurity governance	Sustainable digital policy

15. Conclusions

This work proposes a holistic approach to cognitive security in universities:

- Technology (Wi-Fi, MFA, AI, Zero Trust),
- Human behavior (cognitive security),
- And adaptive pedagogy (contextual delivery).

This is an original innovation that places behavioral and cognitive cybersecurity at the heart of the university's digital transformation.

15.1. Implementation of the Dissemination of Cognitive Security Best Practices

15.1.1. Implementation Objectives

The main objective is to create a secure and intelligent digital ecosystem where:

- Users automatically adopt best security practices.
- The Wi-Fi network is secure and segmented.
- Access is dynamically controlled via MFA and the Zero Trust principle.
- Cognitive cybersecurity is delivered in a personalized way to students, faculty, and administrative staff.

15.1.2. Technical Infrastructure: [9]

a) Secure Wi-Fi:

- Security Protocols: WPA3-Enterprise for encryption.

- Network Segmentation: Separate VLANs for students, teachers, IoT, and administration.
- Monitoring: IDS/IPS to detect network anomalies.
- Access Control: RADIUS server to centralize identities.

b) Multi-Factor Authentication (MFA):

- Integration with the LDAP/Active Directory server.
- MFA Methods: OTP (mobile application), codes via email, NFC badges for certain services.
- MFA logs are collected for behavioral analysis.

c) Zero Trust Architecture:

- Principle: "Never trust, always verify".
- Every user, device, or service is verified before and during access.
- Access policies adapt in real time according to the trust score generated by the cognitive model.

15.1.3. Cognitive Dissemination of Best Practices

a) Behavior Collection and Analysis:

- Collection of Wi-Fi, MFA, and IoT logs.
- Real-time analysis via an artificial intelligence model (e.g., CNN) to detect:
- Normal behavior.
- Suspicious behavior.
- High-risk behavior.

b) Personalized Dissemination:

- Notifications via email, captive portal, or interactive IoT screens.
- Messages tailored to the user profile and the severity of the situation:
- Simple tips on MFA and passwords.
- Micro-lessons on cognitive security.
- Alerts in case of suspicious login attempts.

c) Feedback Loop:

- User actions are fed back into the system to improve the model.

Allows for continuous improvement of recommendations and awareness.

15.1.4. Functional Implementation Diagram: [10]

1) User Login → Secure Wi-Fi.

2) Identity Verification → MFA.

3) Behavioral Analysis → CNN Model/Zero Trust Engine.

4) Access Decision → Allowed/Enhanced MFA/Blocked.

5) Best Practice Dissemination → Personalized Messages, Notifications, Micro-learning.

Table 8: Component and expected outcome of the implementation

The implementation of this intelligent infrastructure includes various components and their results, namely:

- Secure Wi-Fi for reduced intrusions and improved traceability;
- MFA for enhanced authentication and reduced impersonation;

- Zero Trust for adaptive access and dynamic control;
- Cognitive diffusion for proactive awareness and adoption of best practices.

Table 8. Component and expected result of the implementation.

Component	Expected result
Secure Wi-Fi	Reduced intrusions and improved traceability
MFA	Strengthening authentication and limiting identity theft
Zéro Trust	Adaptive access and dynamic control
Cognitive diffusion	Proactive awareness-raising and adoption of best practices

16. Future Development Prospects

- Development of a cognitive cybersecurity dashboard for overall monitoring.
- Extension of the model to other campuses or university institutions.
- Integration of a hybrid CNN + LSTM model to improve the detection of complex behaviors.

Coupling with an e-learning platform to enhance continuing education.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Alia, A. (2023) Effect of Cybersecurity Awareness among Students in the Education Framework Using the Internet, E-Learning Platforms and Social Networks. *International Journal of Computer and Information Technology*, **12**, 72-78. https://doi.org/10.24203/ijcit.v12i2.350

[2] Armas, R. and Taherdoost, H. (2025) Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm. *Information*, **16**, 336. https://doi.org/10.3390/info16050336

[3] Titi, K.M.I. (2025) Comprehensive Analysis of Cybersecurity Awareness among Students' Universities. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5201990

[4] Kandula, S.R., Kassetty, N., ALANG, K.S. and Pandey, P. (2024) Context-Aware Multi-Factor Authentication in Zero Trust Architecture: Enhancing Security through Adaptive Authentication. *International Journal of Global Innovations and Solutions*. https://doi.org/10.21428/e90189c8.f525ef41

[5] Liu, Y. (2024) Analysis of Multi-Factor Authentication (MFA) Schemes in Zero Trust Architecture (ZTA): Current State, Challenges, and Future Trends. *International Journal of Computer Applications*, **186**, 30-36. https://doi.org/10.5120/ijca2024924310

[6] Marafo, M.P., Palayen, B., Kiniway, J.S., Dulagan, G., Bugalin, F., Bacasen, J. and Guaki, G.S. (2024) Zero Trust Security in WFA Platforms: A Literature Review of Principles, Challenges and Best Practices. *Southeast Asian Journal of Science and Technology*, **9**, 9-17.

[7] Metin, B., Özhan, F.G. and Wynn, M. (2024) Zero Trust Cybersecurity: Critical Success Factors and A Maturity Assessment Framework.

[8] Moustafa, A.A., Bello, A. and Maurushat, A. (2021) The Role of User Behaviour in

Improving Cyber Security Management. *Frontiers in Psychology*, **12**, Article ID: 561011. https://doi.org/10.3389/fpsyg.2021.561011

[9] Mony, V.O., Ikoha, A.P. and Maroko, R.O. (2025) An Intelligent Zero Trust Architecture Model for Mitigating Authentication Threats and Vulnerabilities in Cloud-Based Services. *Journal of Cyber Security*, **7**, 395-415. https://doi.org/10.32604/jcs.2025.070952

[10] Sapanca, H.F. and Kanbul, S. (2022) Risk Management in Digitalized Educational Environments: Teachers' Information Security Awareness Levels. *Frontiers in Psychology*, **13**, Article ID: 986561. https://doi.org/10.3389/fpsyg.2022.986561