IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 6, December 2026, pp. 5486~5499
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i6.pp5486-5499

Integrated school safety infrastructure utilizing internet of things and machine learning algorithms

Angelo Pera[1], Marco Jr. Del Rosario[2]
[1]Faculty of Information Technology, Polytechnic University of the Philippines, Unisan, Philippines
[2]Faculty of Information Technology, Laguna State Polytechnic University, San Pablo City, Philippines

Article Info

Article history:

Received Oct 6, 2025
Revised Jul 21, 2026
Accepted Aug 31, 2026

Keywords:

Internet of things
Machine learning
Polytechnic University of the Philippines
Random forest
School safety
Technology acceptance model

ABSTRACT

This study addresses the safety and security challenges in a public kindergarten through grade 12 (K-12) schools in the Philippines by developing an internet of things (IoT) and machine learning-enabled surveillance system. The system integrates IoT cameras, sensors, radio frequency identification (RFID), and smart gate with face recognition, body temperature and metal sensors. Development and descriptive-correlational research design utilizing modified technology acceptance model (TAM) evaluated the acceptability of system. TAM is a theoretical framework that aims to explain and predict user acceptance of technology. Machine learning evaluation results show high accuracy and performance in face recognition, smart gate access control, and fire detection models. Functionality testing confirms the system's reliability in various conditions. Survey results reveal strong user satisfaction and intentions to adopt the system, supported by significant relationships identified in the modified TAM. In conclusion, the system effectively enhances school safety and security, with continued refinement in terms of scalability, integration of additional machine learning models, user training, student and staff awareness programs and monitoring are recommended for sustained efficacy.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Angelo Pera
Faculty of Information Technology, Polytechnic University of the Philippines
Unisan Campus, Brgy. Kalilayan Ibaba, Unisan, Quezon, Philippines
Email: angeloppera@gmail.com

1. INTRODUCTION

In a time marked by technological advancements and growing educational landscapes, the safety and security of public kindergarten through grade 12 (K-12) schools have emerged as top concerns, not only in the Philippines but also worldwide. The sanctity of these institutions, where young minds are nurtured, requires an unwavering commitment to safeguarding students and staff. Threats and violence are some of the top problems that most schools encounter, not to mention health risks during pandemic days [1]. Several situations about these were elaborated, and it was clearly emphasized that school safety is a top priority and safety alert systems are a necessity nowadays.

In the Philippines, K-12 public schools face different challenges regarding safety and security. School shootings are a growing concern in educational environments, emphasizing the need for awareness and prevention programs [2]. In the Philippines, a Department of Education (DepEd) supervisor and his wife were shot by a gunman in Insulan Elementary School in Insulan, Sultan Kudarat. In Tacloban City, a teacher at Hindang National High School said in a phone interview that a two-hour fire made their school library, computer laboratory, science laboratory, canteen, and other offices burn down to ashes. This can be due to a lack of awareness and training in fire safety, poor electrical installations, negligence, financial constraints,

and insufficient fire safety resources, all of which hinder effective emergency preparedness and response [3]. Also, the country is highly prone to natural hazards as one of the archipelagic countries in the Pacific Typhoon belt like flooding. In 2022, the DepEd released new guidelines about suspension of classes and work during disasters. According to DepEd Order No. 037 series of 2022, when a flood warning is issued at a time when classes have already begun, the classes and work shall be "immediately suspended" and the schools are obligated to keep the students and staff safe inside school premises while sending everyone home [4]. Lastly, DepEd condemns the rape and robbery incidents happened in two schools in Camarines Sur Province urging every public school to have at least one security guard in the whole country [5].

To address these multifaceted challenges, this study introduces an innovative approach that is associated with current technology, namely the internet of things (IoT) and machine learning. IoT refers to interconnected devices and systems that share data via the internet, utilizing sensors and communication software [6]. On the other hand, machine learning is a branch of artificial intelligence where computers learn from data to identify patterns, make decisions, and improve performance over time without explicit programming [7].

The researchers developed and implemented a comprehensive IoT-enabled surveillance system. The system starts with networked IoT cameras along with several sensors that will continuously capture live feeds and send to a server that acts as the Central Hub of the system for aggregation and analysis through machine learning algorithms such as single shot multibox detector (SSD) and random forest (RF). The SSD for real-time face detection and recognition; and the RF algorithm that integrates the output of multiple decision trees to achieve a single result, is utilized for accurate fire detection by classifying sensor data to distinguish fire from non-fire scenarios. They were applied to the network of strategically positioned IoT devices, analyzing the live feeds in real-time, detecting objects of interest, and classifying them. Afterwards, the system will trigger alerts, notify the departments concerned and students through mobile devices, and all data collected will be sent and handled by the personnel from an emergency control room (ECR) to resist or minimize disaster.

Furthermore, recognizing the impact of the proposed system on the beneficiaries in the educational setting, this research seeks to measure the perceptions of students and other stakeholders from educational institution, Philippine National Police (PNP), Municipal Risk Reduction and Management Office (MDRRMO), and Bureau of Fire Protections (BFP) about the IoT system designed to enhance school safety and security guided by the technology acceptance model (TAM) a theoretical framework that aims to explain and predict user acceptance of technology [8]. By incorporating their perspectives, the study aims to ensure that the proposed technological advancements align with the needs and expectations of those directly impacted by its implementation. Lastly, this study contributed to the United Nations (UN) sustainable development goals (SDG) such as SDG 3 Good Health and Well–Being by safeguarding students and staff from environmental and security threats; SDG 4 Quality Education by fostering a safe learning environment; SDG 11 Sustainable Cities and Communities by enhancing disaster resilience; and SDG 16 Peace, Justice, and Strong Institutions through ethical and transparent security measures [9].

2. METHOD

This study utilized a multi–method approach combining developmental and descriptive-correlational research designs. The developmental research design was chosen to effectively develop and implement the IoT and machine learning-enabled system, while descriptive-correlational approach was adopted to measure the perceptions of students, school staff, members of the PNP, MDRRMO, and BFP regarding the enhancement of school safety and security [10], [11]. The acceptability level of the system was measured following the modified TAM shown on Figure 1 and structural equation modeling (SEM) to examine relationships between its variables. The TAM describes how users will accept and use technology by focusing on key constructs such as perceived usefulness (PU) and perceived ease of use (PEOU), which influence users' attitude toward using (ATU) and behavioral intention (BI) to use the system. In this study, TAM was modified by adding constructs such as trust and features of the system to better reflect the context of school safety and security systems [12].

Based on the TAM, the following hypotheses were derived namely: H1: PU has significant influence on ATU; H2: PEOU has significant influence on ATU; H3: PU has significant influence on BI; H4: ATU has significant influence on BI; H5: trust in the system has significant influence on ATU; H6: trust on the system has significant influence on BI; H7: features of the system has significant influence on PU; H8: features of the system has significant influence on PEOU. Meanwhile, SEM was employed to test the proposed hypotheses and analyze the relationships among the modified TAM constructs. It fits with this study as it analyses complex relationships among multiple variables while accounting for measurement errors [13].

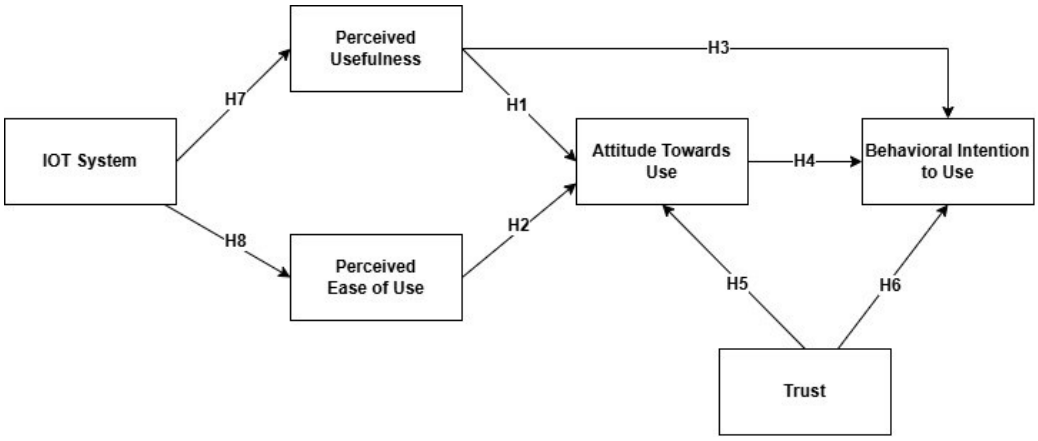


Figure 1. Modified TAM

With SEM, variables are classified into latent and observed variables. Latent variables are abstract constructs that cannot be measured directly, such as PU, PEOU, ATU, BI, trust, and features of the system. These variables are measured using observed variables, which are the respondents' answers to specific questionnaire items constructed to correspond to each construct. These variables serve as indicators that reflect the underlying latent variables in the SEM model.

This study was conducted at Calauag National High School (CNHS) located in Calauag, Quezon, catering to a population of approximately 2,700 including school staff and junior and senior high school students. The CNHS was chosen because they suffer issues and concerns regarding school safety and security. One notable issue is the risk of flooding, due to the creek located inside their campus that experiences a rapid surge in water levels during heavy rainfall, and there are reports from staff members of missing items and unauthorized access to various facilities within school premises.

To determine the sample size, an a priori sample size calculator for SEM was utilized and set the anticipated effect size to 0.3, desired statistical power level of 0.8, number of latent variables to 6, number of observed variables to 24 and probability level of 0.05, resulting to 161 samples. Additionally, to properly distribute the target samples among the different stakeholders, stratified sampling was used by having different strata comprising 130 students, 15 school staff, 5 PNP, 5 MDRRMO, and 6 BFP respondents.

Data were collected using a triangulation strategy that includes surveys, interviews, and focus group discussions (FGD). The survey was administered to 161 respondents to measure perceptions of the adoption of new technology according to the given TAM framework. Meanwhile, key informant interviews (KIIs) were conducted with selected school staff and local authorities (PNP, BFP, and MDRRMO) to gather insights into current challenges, contextual requirements, and possible benefits of the safety and security system. Lastly, FDGs were held with student groups, parents' associations, and faculty members to gain qualitative feedback on system impact on school safety, usability, experiences, suggestions, and improvements of the system.

2.1. System overview

The system is composed of different modules shown in Figure 2, such as IoT cameras, a smart gate with face recognition, infrared (IR) thermometer and metal detector, smart door with radio frequency identification (RFID) scanner and magnetic door sensor, a flood detector utilizing an ultrasonic sensor, and flame detector comprising gas, flame, temperature, and humidity sensors. All modules will continuously capture live feeds. All data are sent to a server that acts as the Central Hub of the system through firebase database for analysis with machine learning algorithms such as SSD and RF.

The SSD was utilized for rapid object detection, specifically optimized for real-time face recognition at smart gates [14]. To ensure high performance, the model was trained on a dataset of 1,250 images, all of which were preprocessed through mean subtraction and resized to a uniform 300 × 300 pixels resolution to maintain consistency. The model was validated using a confusion matrix–based binary classification approach.

Meanwhile, RF algorithm can classify data and predict fire incidents accurately from learning various data supplied during the training of model [15]. The model was trained on a dataset of 25,000 samples containing temperature, smoke, and humidity readings. Preprocessing involves feature encoding and outlier removal to minimize noise.

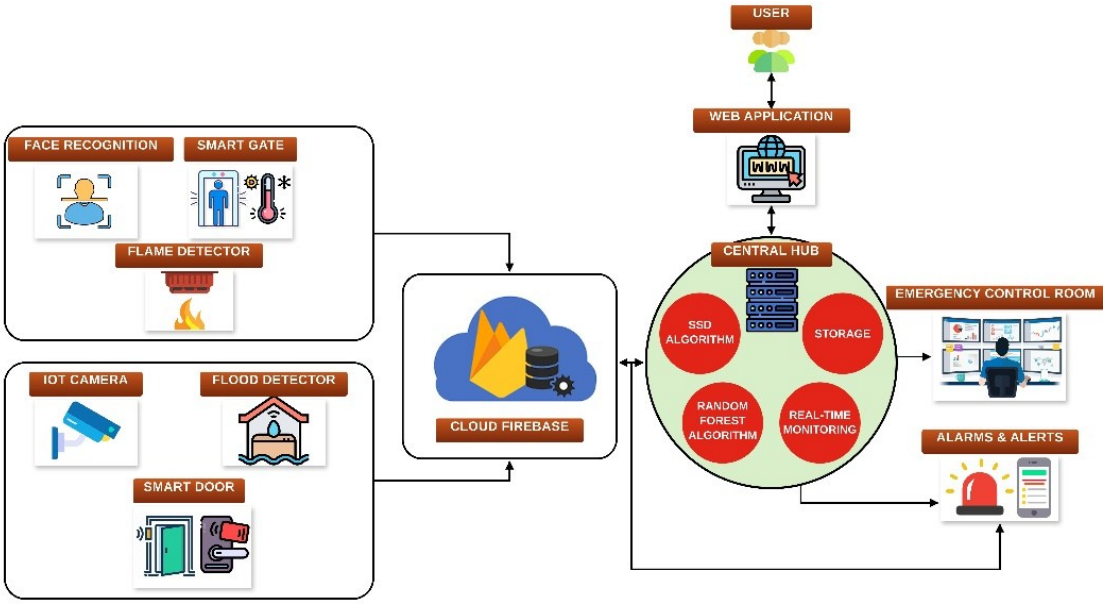


Figure 2. System architecture

For validation, an 80/20 train-test split was utilized on both models, ensuring reliability on unseen data. True positives, true negatives, false positives, and false negatives were computed to derive accuracy, precision, recall, and F1-score, providing an overall assessment of classification performance confirmed by the confusion matrix. Distinguishing between no fire (0), possible fire (1), and fire (2), and face and not face labels for RF and SSD models.

Afterwards, the system will trigger alerts, notify concerned departments and students through mobile devices via mobile application and short message services (SMS) notifications via the Semaphore SMS API. Lastly, all data collected will be sent and handled by personnel from an ECR to resist or minimize unnecessary events. Despite advancements in smart security, research gaps exist in the development of unified, multi-hazard IoT frameworks that combine environmental monitoring with biometric access control [16]. Most existing literature shown in Table 1 focuses on "siloed" systems—either specialized in fire detection or facial recognition—which leads to fragmented data and delayed emergency responses [17]. This study addresses these gaps by proposing an integrated architecture that synchronizes SSD-based face recognition and RF-based fire detection with centralized ECR oversight, providing a more resilient and context-aware security infrastructure for educational environments.

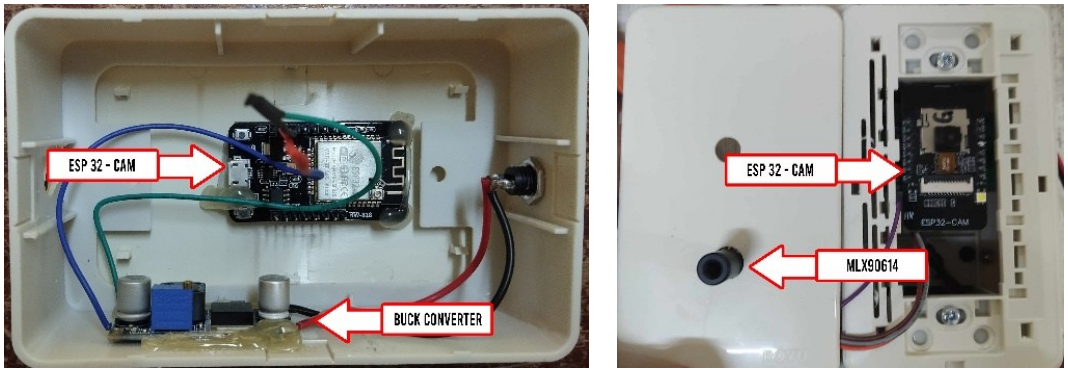
Table 1. Test cases of functionality testing

System overview	Scope	Performance
Raspberry Pi + OpenCV [17]	Fire and face	Focused on residential door locks; limited to single-sensor flame detection.
ESP32 + threshold logic [18]	Industrial fire	Real-time monitoring but lacks machine learning-based predictive analytics; high risk of false alarms.
ResNet + Dlib [19]	Intruder only	Achieved 96% accuracy but lacks integrated environmental hazard (fire/flood) monitoring.

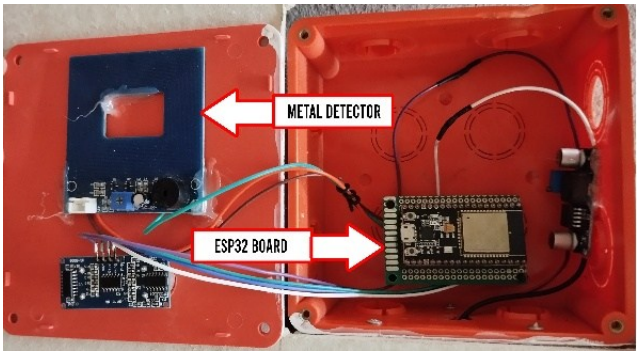
2.2. System design

The IoT Cameras for monitoring school premises were built with ESP–32 Cam while face recognition feature of smart gate also built with same device alongside MLX90614 contactless temperature sensor and with metal detection module as shown in Figure 3 smart gate IoT devices, where IoT camera as shown in Figure 3(a) and metal detector module as shown in Figure 3(b). The flame detector is composed of a DHT22 (temperature and humidity) sensor, flame sensor, and MQ2 gas sensor module to allow the system to accurately predict fire incidents in the area where it was installed. On the other hand, smart door is equipped with an RFID scanner, a solenoid lock and magnetic door switch modules depicted in Figure 4 to perform its job of sending door activity logs into central hub. Lastly, Figure 5 shows the composition of the flood detection module that uses JSN-SR04T (waterproof ultrasonic distance sensor) to detect water level at the bridge within the school campus. All modules have ESP32 development boards that serve as central microcontroller units responsible for collecting sensor data, processing inputs, and real-time data

transmission to the central server via Firebase [20]. The ESP32 boards also enable seamless integration of sensors and actuators and support deployment of lightweight machine learning models.



(a)



(b)

Figure 3. Smart gate IoT devices of (a) IoT camera and (b) metal detector module



Figure 4. Smart door

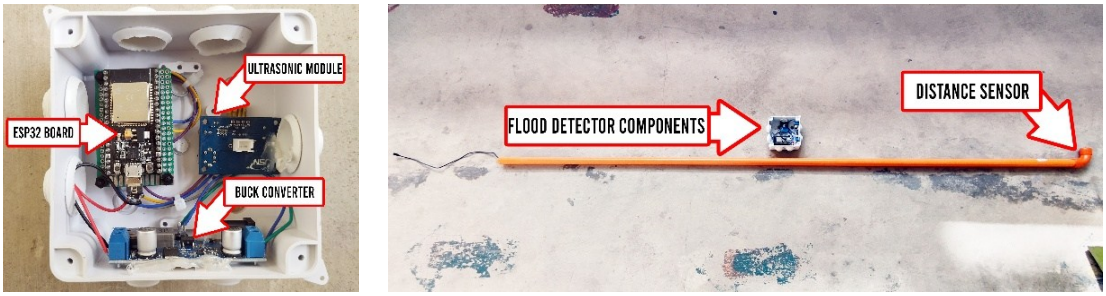


Figure 5. Flood detector

2.3. System implementation

All hardware modules were strategically installed on various places of CNHS premises, as shown on Figure 6 implementation plan. Smart gate with face recognition, metal and body temperature detectors were positioned at the school entrance, and ECR was located on guard house near school entrance. Meanwhile, smart doors are installed on the computer laboratory and admin office where the central hub, important documents and properties are located. Fire detectors are used in places where there is a risk of fire such as the cooking laboratory and flood detector was connected to monitor the water level on the bridge. Lastly, IoT cameras are connected to open grounds for monitoring safety and security purposes.



Figure 6. Implementation plan

All IoT devices were connected to the school's network infrastructure through access points for them to transmit data to the firebase real time database. Mobile application received real–time alerts and evacuation instructions directly from thru firebase cloud messaging push notification feature based on data given by the Central Hub [21]. ECR is connected to the Central Hub to receive alerts from the system and monitor the surroundings with surveillance cameras. Lastly, PNP, BFP, and MDRRMO will receive text messages from the system if unauthorized entry, fire incident, or early flood warning are detected.

The implementation of the system adheres with the Philippine's National Privacy Commission (NPC) Advisory No. 2020–04 to the principles of proportionality, transparency, and data security. Biometric processing is limited to legitimate access control at smart gates, ensuring data collection remains necessary and not excessive. Informed consent is secured from students or guardians prior to SSD enrollment, supported by prominent signage at entry points to satisfy the "right to be informed." To ensure compliance with the Data Privacy Act of 2012, all biometric templates are encrypted on the server, managed by authorized personnel, and purged upon the termination of institutional affiliation to prevent unauthorized data retention.

3. RESULTS AND DISCUSSION

The system undergoes testing procedures such as confusion matrix and classification metrics for machine learning models, functionality testing, and acceptability testing to measure perceptions of school's stakeholders regarding the adoption of the new system [22]. Researchers utilized different tools to facilitate the testing of the system's features. For instance, classification and confusion matrix reports were used in machine learning models, test cases for functionality, and researchers made survey instrument for acceptability.

3.1. Machine learning models evaluation

The evaluation of machine learning models used on the system is shown in Figure 7, classification and confusion matrices. According to Luo and Liu [23], the SSD network structure for local attribute detection due to its efficiency in extracting face features quickly with fewer parameters and lower computational workload compared to other models like you only look once (YOLO) or deep neural network (DNN). In this study, the SSD model's evaluation revealed strong performance as shown in Figure 7(a). Based on the analysis of the confusion matrix, the model accurately identified 604 faces and 600 non–faces, with only 25 false positives and 21 false negatives. Meanwhile, for classification metrics, the model achieved exceptional performance with the following scores: accuracy (96%), precision (97%), recall (sensitivity) (97%), and F1-score (96%). The results suggest that the model is highly effective and correctly identifies authorized and unauthorized individuals.

Meanwhile, RF algorithms were proven effective for fire detection as it outperforms other algorithms such as logistic regression and decision trees in terms of accuracy and reliability [24]. The trained RF model's evaluation revealed strong performance as shown in Figure 7(b). Based on the analysis of the confusion matrix, the model accurately identified if there is fire (2), possible fire (1), and no fire (0). Out of 25, 000 data, 24, 299 were predicted correctly, while 701 remained below positive and negative. Meanwhile, for classification metrics, the model achieved exceptional performance with the following scores: accuracy (97%), precision (97%), recall (sensitivity) (97%), and F1-score (97%). The results underscore the model's reliability in triggering timely response and mitigation efforts, enhancing overall safety measures within the school environment.

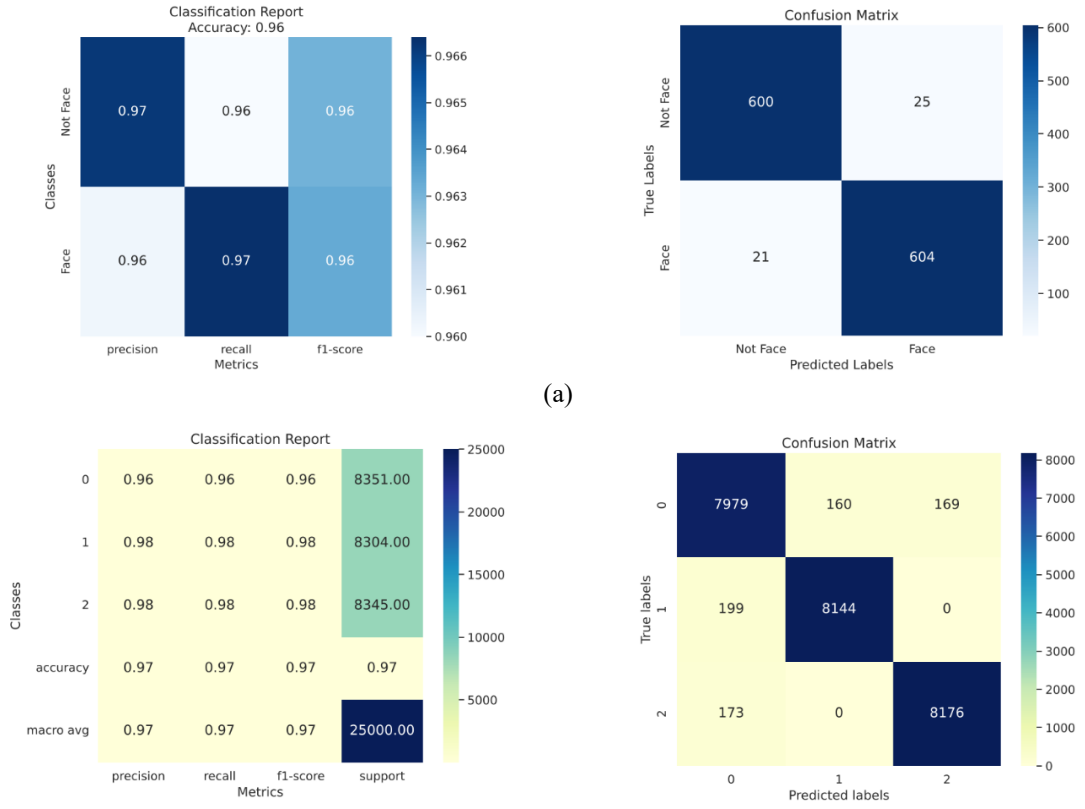


Figure 7. Confusion matrix and classification metrics of the (a) SSD and (b) RF models

As stated by Ritharson *et al.* [25] in their study, machine learning algorithms like DNNs and YOLOv3 enhance school safety by enabling facial recognition, weapon detection, and an alert system, thus preventing school shootings effectively. Also, machine learning algorithms such as RF in fire detection provide accurate fire potential assessment and timely alerts to emergency services, enhancing safety and reducing false alarms, as discussed by Deepa *et al.* [26]. Furthermore, the integration of the SSD algorithm model enhances surveillance capabilities and threat identification within school premises, particularly in the context of gate access control. Simultaneously, integration of the RF model empowers schools to effectively

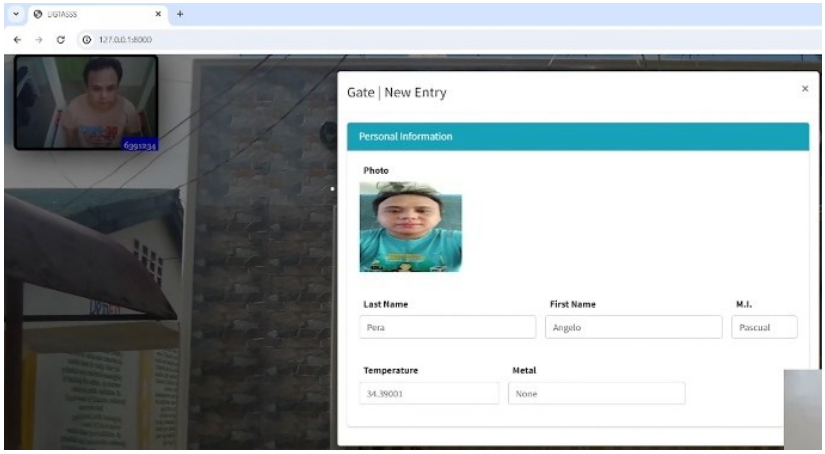
detect and respond to fire emergencies. With its high accuracy and precision, the model facilitates timely activation of fire alarms and initiation of evacuation procedures, thereby minimizing potential risks to students, staff, and infrastructure.

3.2. Functionality testing

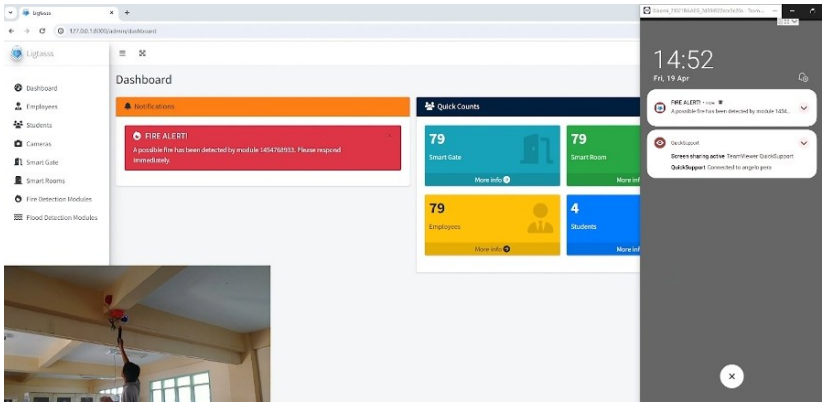
The system was tested and passed different test cases to ensure all functions worked properly. There are 11 test cases as shown in Table 2 for thorough evaluation of whether the system triggers an alert and sends a notification to each corresponding person involved. During testing, the researchers simulated different conditions from normal to unusual events such as increasing temperature and decreasing humidity levels where fire detection was installed to check its ability to trigger fire alerts and alarms, as shown in Figure 8. Upon testing, the smart gate successfully detected metal and measured body temperature, as shown in Figure 8(a), and when temperature and humidity reached values needed to trigger, the system was able to send alerts to ECR and the mobile application, send SMS notifications to BFP, and trigger an alarm inside the cooking laboratory as depicted in Figure 8(b).

Table 2. Test cases of functionality testing

#	Test scenario ID	Test scenario name	Result
1	TS_FD_001	Normal event handling of fire detection device	Passed
2	TS_FD_002	Fire detection functionality of the fire detection device	Passed
3	TS_EFD_001	Normal event handling of the flood detection device	Passed
4	TS_EFD_002	Early flood detection of the flood detection device	Passed
5	TS_SD_001	RFID card access functionality of the smart door	Passed
6	TS_SD_002	Manual door opening alert of the smart door	Passed
7	TS_SG_001	Normal condition of the smart gate	Passed
8	TS_SG_002	Unrecognized face entry on smart gate	Passed
9	TS_SG_003	Recognized face with metal detection entry on smart gate	Passed
10	TS_SG_004	Face recognition with high body temperature on smart gate	Passed
11	TS_SC_001	Video monitoring and recording	Passed



(a)



(b)

Figure 8. Machine learning models simulation (a) face recognition and (b) fire detection

Meanwhile, Figure 9 illustrated how the researchers exposed the ultrasonic distance sensor module connected to flood detection device of the system to verify whether it can trigger flood alerts to ECR, mobile application and send SMS notification to the MDRRMO when certain level was detected by the sensor. For smart door, it was tested to verify if it can classify valid and invalid RFID cards. If the door is opened manually, without tapping an RFID card, it indicates that door is opened by force of possible intruders.

Therefore, it automatically triggers an alert to ECR and send SMS notification to PNP shown on Figure 10. The smart gate feature of the system was tested in accordance with various conditions. While testing, the system can identify known and unknown faces passing on smart gate. Upon testing, all IoT cameras successfully sent live feeds to the central hub, and recorded videos could be viewed from the IoT cameras.

According to Cristea *et al*. [27], functionality testing of IoT devices is crucial for identifying bugs across diverse devices and interactions. The successful completion of all test scenarios indicates the robustness and effectiveness of the IoT project in delivering the intended functionalities. The system demonstrated reliable performance across various scenarios, including fire and flood detection, access control, and surveillance. In the context of surveillance, Figure 11 shows that all IoT cameras were tested for their ability to capture and record video streams.

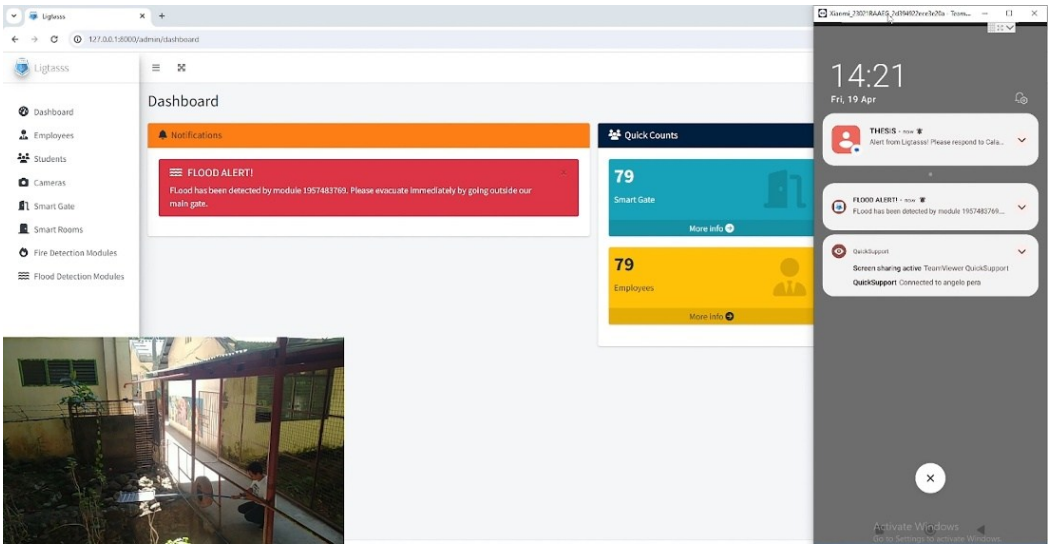


Figure 9. Flood testing

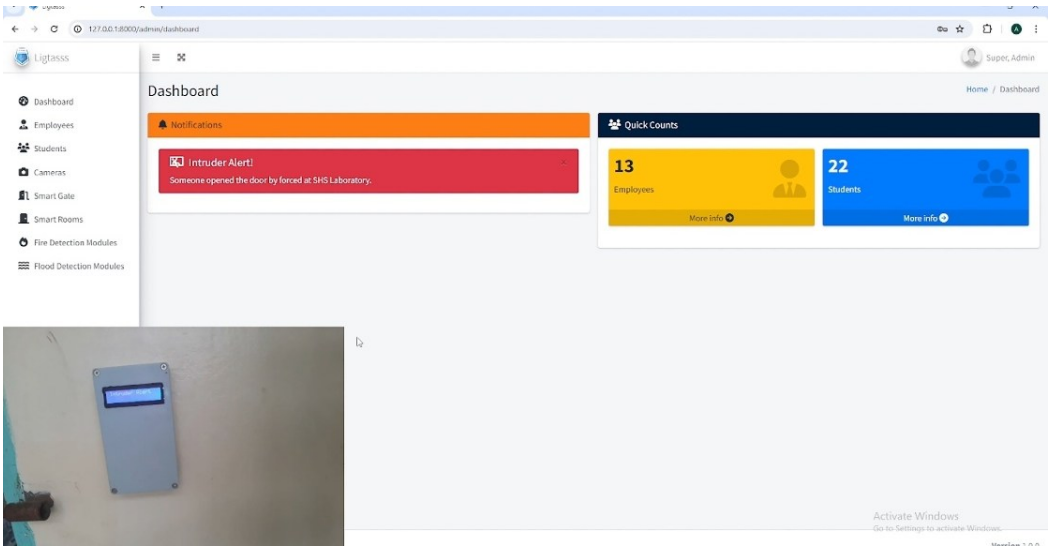


Figure 10. Smart door testing

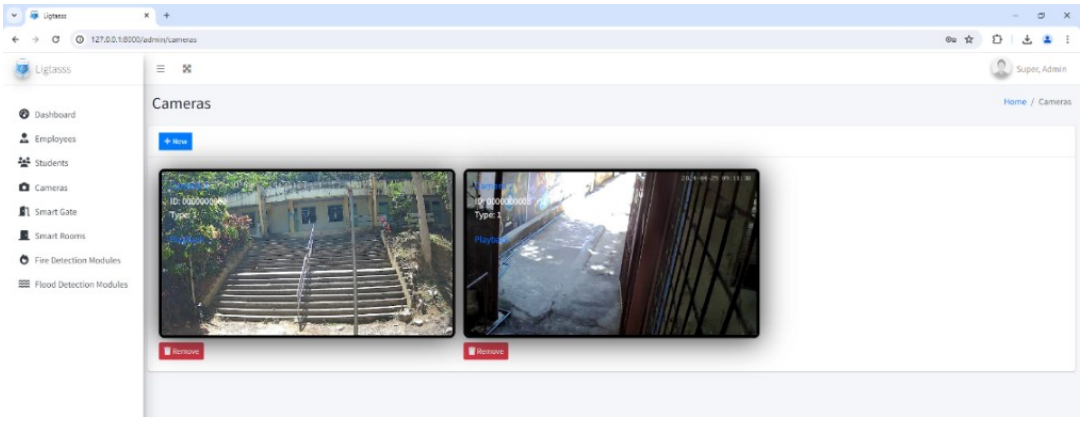


Figure 11. IoT cameras

3.3. Acceptability testing

The TAM–based questionnaire utilized in this study has 6 constructs stated in Table 3 in accordance with the TAM framework shown in Figure 1, each has four indicators. The instrument undergoes pilot testing with 30 participants to ensure its clarity and internal consistency among indicators of each construct. The results revealed high levels of internal consistency, better than the recommended threshold of 0.70 for reliability [28].

Among the 161 respondents who completed the TAM-based questionnaire, the results presented in Table 4 indicate a strong intention to use the system, as reflected by the mean rating of 4.49 (SD = 0.63) for BI. This suggests a high level of willingness among participants to adopt the system to enhance school safety measures. Further, attitude towards using (ATU) and system trust (ST) received mean ratings of 4.48 and 4.50, respectively, with standard deviations of 0.59 and 0.60, indicating consistency in positive perceptions among participants regarding the system's functionality and reliability. The mean rating for the IoT construct was 4.52 (SD = 0.63), indicating a high level of satisfaction with the system's features among participants. PU received a mean rating of 4.46 (SD = 0.61), suggesting that participants found the system is valuable in improving school safety. Similarly, PEOU got a mean rating of 4.34 (SD = 0.63), participants perceived the system was easy to use and navigate.

Table 3. Reliability testing results

Construct	Cronbach's alpha	Interpretation
IoT	0.81	Acceptable
PU	0.71	Acceptable
PEOU	0.71	Acceptable
BI	0.76	Acceptable
ATU	0.73	Acceptable
ST	0.74	Acceptable

Table 4. Descriptive statistics results

Constructs	Mean	Standard deviation
IoT	4.52	0.63
PU	4.46	0.61
PEOU	4.34	0.63
BI	4.49	0.63
ATU	4.48	0.59
ST	4.50	0.60

The researchers utilized SEM using statistical package for the social sciences (SPSS) to examine the relationships among latent constructs in the TAM framework [13]. Findings provide valuable insights into the interplay between variables under investigation and contribute to understanding of factors influencing individuals' acceptance of IoT systems. Confirmatory factor analysis (CFA) was conducted to evaluate the underlying factor structure of survey items measuring users' perceptions regarding adoption of IoT systems [29]. All factors have strong factor loadings exceeding the recommended threshold of 0.50 shown in Figure 12, this indicates strong relations between survey items and their respective constructs [30].

Meanwhile, SEM results shown in Table 5 validate the appropriateness of the factor model in representing users' perceptions toward the adoption of an IoT system, having a CMIN/DF value of 1.569 and root mean square error of approximation (RMSEA) value of 0.077 were considered a good fit. Hence, the comparative fit index (CFI) and Tucker-Lewis index (TLI) resulted in 0.842 and 0.801 respectively, indicating marginal fit accounting for 90% of the total variance. Findings enhance the reliability and validity of survey instruments, providing valuable insights into the factors influencing the acceptance and adoption of IoT systems across diverse respondents. According to Giasi *et al.* [31], a structural model having a value of CMIN/DF ≤ 3 indicates a good fit index, including the CFI, TLI, and RMSEA, demonstrating excellent fit

between observed data and proposed model, with values of CFI and TLI close to or above 0.90, and RMSEA close to or under 0.08. While these findings validate the reliability of the survey instruments, the marginal fit indices necessitate caution regarding causal interpretation. Such values imply that while the model captures significant variance, the underlying path relationships should be viewed as preliminary rather than definitive, as omitted variables or measurement errors may still influence the structural paths [32].

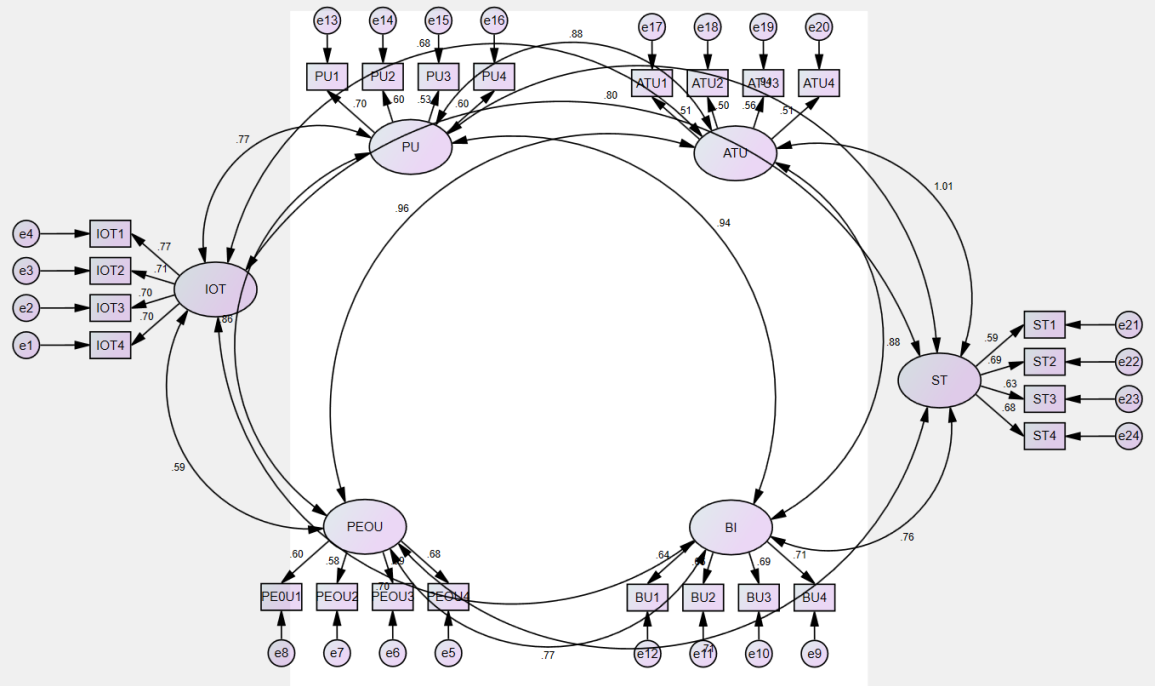


Figure 12. SEM

Table 5. SEM metrics

Model fit indices	Criteria	Result	Description
CMIN/DF	≤3	1.569	Good fit
RMSEA	≤0.08	0.077	Good fit
CFI	≤0.9; ≥0.8	0.842	Marginal fit
TLI	≤0.9; ≥0.8	0.801	Marginal fit

Lastly, hypothesis testing was performed to examine relationships of the utilized TAM framework and assess their implication in predicting users' intentions to adopt the system. Results of hypothesis tests deliver strong evidence for the assumed relationships between IoT, PU, PEOU, BI, ATU, and ST on the system shown in Table 6. Results reveal significant relationships between examined constructs based on the proposed TAM framework. Particularly, there is a positive association between PU and ATU (H1), indicating that respondents tend to engage with systems they observe as useful. Similarly, the study found a positive correlation between PEOU and ATU (H2), suggesting that the system is user-friendly and more likely to be accepted. Further, the results demonstrate that higher PU leads to stronger intentions to use the system, as specified by the positive relationship between PU and BI (H3). Additionally, attitude towards the system is positively associated with stronger intentions to use it further (H4), highlighting the importance of user experience in determining BI.

Moreover, analysis reveals that high ST is related to increased system usage (H5), indicating the importance of trust in driving user adoption. This study also found that features associated with the IoT positively influence both PU and PEOU (H6 and H7), highlighting the role of technological features in determining user perceptions. Lastly, analysis found a significant relationship between ST and BI (H8), suggesting that trust in the system proportionally impacts users' intentions to use it. Overall, findings contribute to the understanding of factors influencing users' perceptions and behaviors regarding technology adoption.

Table 6. Hypotheses testing results

H	Relationship	Estimate	S.E.	C.R.	P-value	Result
H1	PU–ATU	.119	.032	3.737	<0.001	Supported
H2	PEOU–ATU	.118	.031	3.785	<0.001	Supported
H3	PU–BI	.184	.040	4.585	<0.001	Supported
H4	ATU–BI	.133	.035	3.754	<0.001	Supported
H5	ST–ATU	.106	.029	3.657	<0.001	Supported
H6	ST–BI	.116	.031	3.803	<0.001	Supported
H7	IOT–PU	.156	.038	4.109	<0.001	Supported
H8	IOT–PEOU	.111	.032	3.479	<0.001	Supported

4. CONCLUSION

The study sets out to develop, implement, and measure the acceptability of the IoT and machine learning-enabled system, producing significant perceptions and results. This study has argued that integration of machine learning techniques such as SSD, RF, various sensors, and microcontrollers combined to develop a system infrastructure including a smart gate, smart door, flood and fire detectors, surveillance camera, central hub, ECR, mobile application, and web application presents a comprehensive solution for addressing security challenges in educational settings. The testing conducted on the system's functionality validated its reliability and effectiveness. The system demonstrated robust performance by meeting specified requirements. The evaluation of SSD and RF models demonstrated high accuracy and efficiency in their respective applications. These models are integrated into smart gate and fire detector functionalities, contributing to the system's ability to enhance security face screening and detect potential fire incidents. Furthermore, the adaptation of the TAM framework for evaluating the system's acceptance provided valuable insights into stakeholders' perceptions and intentions to use the system. Statistical analysis using SPSS and SEM revealed positive acceptance and indicated the system's potential for widespread adoption and implementation. Overall, the study found that the developed system demonstrates a robust, reliable, and effective solution for enhancing safety and security measures in educational environments. The integration of machine learning algorithms and IoT devices combined with comprehensive testing and evaluation underscores the system's capability to address security challenges and safeguard the well-being of students and staff. Future studies may enhance the system by integrating advanced analytics for real–time processing, predictive analysis, and further refinement by adding machine learning models. A possible expansion to other schools may be explored to evaluate the scalability and effectiveness across different environments. Lastly, regular user training and continuous stakeholder awareness are recommended to support ethical system use.

ACKNOWLEDGMENTS

The authors thank the administration, faculty, staff, and students of Calauag National High School (CNHS), and the PNP, MDRRMO, and BFP of Calauag, Quezon, for their cooperation and support during this study.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Angelo Pera	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
Marco Jr. Del Rosario				✓		✓				✓				

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

The data that support the findings of this study are available on request from the corresponding author, [AP]. The data, which contain information that could compromise the privacy of research participants, are not publicly available due to certain restrictions.

REFERENCES

[1] J. DePaoli and J. McCombs, *Safe Schools, Thriving Students: What We Know About Creating Safe and Supportive Schools*. Palo Alto, CA, USA: Learning Policy Institute, Aug. 2023, doi: 10.54300/701.445.

[2] L. Spector and A. Malyutin, "Schoolshooting as a modern form of terrorism in the educational environment," in *East–West: Practical Approaches to Countering Terrorism and Preventing Violent Extremism*, Laragh, County Wicklow, Republic of Ireland: Dela Press Publishing House, no. 23, 2022, doi: 10.56199/dpcshss.vtwp9624.

[3] K. M. Waryoba and H. Mung'ong'o, "Enhancing fire emergency response readiness in Butiama District secondary schools in Tanzania: an in-depth investigation," *Asian Journal of Education and Social Studies*, vol. 48, no. 4, pp. 129–141, Sep. 2023, doi: 10.9734/ajess/2023/v48i41092.

[4] M. William V. Puna, "Assessment of learning delivery in the new normal: an input to school intervention plan," *EPRA International Journal of Multidisciplinary Research*, pp. 555–560, Jan. 2024, doi: 10.36713/epra15649.

[5] J. Nieuwenhuis, "Editorial," *Perspectives in Education*, vol. 42, no. 4, pp. 1–3, Dec. 2024, doi: 10.38140/pie.v42i4.8894.

[6] C. Viana, "Innovative protection in education: employing IoT, AI, and cloud computing for enhanced detection and supportive response systems in schools," in *Computer Science & Information Technology (CS & IT)*, vol. 14, pp. 73–92, 2024, doi: 10.5121/csit.2024.140105.

[7] V. Jain and S. K. Tiwari, "Overview: machine learning," in *Machine Learning: an Art of Computer Thinking*, vol. 3, May 2024, pp. 130–144, doi: 10.58532/nbennurch183.

[8] A. Kasthurirengan, "Technology acceptance model in understanding consumers' adoption of emerging technologies in retail," *Journal of Advances in Developmental Research*, vol. 16, no. 1, 2025, doi: 10.71097/IJAIDR.v16.i1.1451.

[9] J.-E. Baños, C. Orefice, F. Bianchi, and S. Costantini, Eds., *Good Health, Quality Education, Sustainable Communities, Human Rights: The Scientific Contribution of Italian UNESCO Chairs and Partners to SDGs 2030*, ser. *Strumenti per la didattica e la ricerca*, vol. 209. Florence, Italy: Firenze University Press, 2019, doi: 10.36253/978-88-6453-896-9.

[10] Norliyana Md. Aris, "Design and development research (DDR) approach in designing design thinking chemistry module to empower students' innovation competencies," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 44, no. 1, pp. 55–68, Apr. 2024, doi: 10.37934/araset.44.1.5568.

[11] E. Ozsaker, Z. Aykut, N. C. Doruker, B. S. Koze, and S. Gecit, "The relationship between the academic self-efficacy and perceived stressors among nursing students in clinical settings: a cross-sectional study," *BMC Nursing*, vol. 4, no. 216, 2025, doi: 10.1186/s12912-025-02836-0.

[12] M. O'Dea, "Editorial: 'are technology acceptance models still fit for purpose?" *Journal of University Teaching and Learning Practice*, vol. 21, no. 8, Jan. 2025, doi: 10.53761/1bdbms32.

[13] W. C. J. Tan and H. C. Koh, "Applying structural equation modelling in education research," in *2023 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)*, 2023, pp. 1–8, doi: 10.1109/TALE56641.2023.10398315.

[14] X. Wang *et al.*, "Single shot multibox detector object detection based on attention mechanism and feature fusion," *Journal of Electronic Imaging*, vol. 32, no. 02, pp. 1–12, 2023, doi: 10.1117/1.JEI.32.2.023032.

[15] H. A. Salman, A. Kalakech, and A. Steiti, "Random forest algorithm overview," *Babylonian Journal of Machine Learning*, vol. 2024, pp. 69–79, Jun. 2024, doi: 10.58496/BJML/2024/007.

[16] A. I. Awad, A. Babu, E. Barka, and K. Shuaib, "AI-powered biometrics for internet of things security: a review and future vision," *Journal of Information Security and Applications*, vol. 82, May 2024, doi: 10.1016/j.jisa.2024.103748.

[17] S. V. S. Prasad, "Integration of fire detection and personnel accountability system," *International Journal of Scientific Research in Engineering and Management*, vol. 8, no. 5, pp. 1–5, May 2024, doi: 10.55041/IJSREM32162.

[18] M. Khan, P. Mishra, R. Khan, and V. Maurya, "ESP32-based intelligent fire detection system utilizing machine learning and computer vision for enhanced safety in Indian micro and small enterprises," *Research Square*, 2025, doi: 10.21203/rs.3.rs-6734116/v1.

[19] P. P. Pillai and K. Chellappan, "Face recognition using deep learning for real-time intruder detection," *Jurnal Kejuruteraan*, vol. 37, no. 4, pp. 2035–2045, Jul. 2025, doi: 10.17576/jkukm-2025-37(4)-40.

[20] S. Dey and T. Bera, "Design and development of a smart and multipurpose IoT embedded system device using ESP32 microcontroller," in *2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM)*, Aug. 2023, pp. 1–6, doi: 10.1109/ELEXCOM58812.2023.10370327.

[21] K. Namee, T. Prempranee, W. Phonngam, R. K.-On and A. Meny, "Enhancing hospital bed management through chatbots: integrating dialogflow and firebase cloud messaging for real-time bed availability and reservation system," *22nd International Conference on ICT and Knowledge Engineering (ICT&KE)*, 2024, pp. 1-6, doi: 10.1109/ICTKE62841.2024.10787179.

[22] G. P. Adam *et al*., "Machine learning tools to (semi-) automate evidence synthesis: a rapid review and evidence map," *Agency for Healthcare Research and Quality*, Research White Paper 25-EHC006, Rockville, MD, USA, Dec. 2024, doi: 10.23970/AHRQEPCWHITEPAPERMACHINE.

[23] Q. Luo and Z. Liu, "Research on face local attribute detection method based on improved SSD network structure," *Advances in Multimedia*, vol. 2022, pp. 1–11, Jan. 2022, doi: 10.1155/2022/3730529.

[24] F. F. Faky, M. H. Baswaid, N. A. Z. B. M. Yusri, and N. Ul Amin, "Enhancing fire alarm systems with machine learning: a data-driven approach to early fire detection," *Preprints.org*, 2025, doi: 10.20944/preprints202504.0733.v1.
[25] P. I. Ritharson, G. Madhavan, M. Rajeswari, and D. Brindha, "Prevention of school shooting using neural networks and computer vision," in *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*, Aug. 2022, pp. 1703–1709, doi: 10.1109/ICICICT54557.2022.9917656.
[26] K. R. Deepa, A. S. Chaitra, K. Jhansi, D. A. K. R, P. A. Kumari, and M. M. Kodabagi, "Development of fire detection surveillance using machine learning and IoT," in *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, Oct. 2022, pp. 1–6, doi: 10.1109/MysuruCon55714.2022.9972725.
[27] R. Cristea, M. Feraru, and C. Paduraru, "Building blocks for IoT testing: a benchmark of IoT apps and a functional testing framework," in *Proceedings of the 4th IEEE/ACM International Workshop on Software Engineering Research and Practices for the IoT (SERP4IoT)*, May 2022, pp. 25–32, doi: 10.1145/3528227.3528568.
[28] J. F. Hair, M. Celsi, A. H. Money, P. Samouel, and M. J. Page, *Essentials of Business Research Methods*, 3rd ed. New York, NY, USA: Routledge, 2016.
[29] C. E. Pacewicz, C. R. Hill, H. Chun, and N. D. Myers, "Confirmatory factor analysis in kinesiology journals with explicit measurement focus," *Measurement in Physical Education and Exercise Science*, vol. 28, no. 2, pp. 146–171, Apr. 2024, doi: 10.1080/1091367X.2023.2270466.
[30] W. Wilnio, M. S. Haramain, F. A. Nasution, and A. Mailangkay, "Measuring the impact of perceived risk and trust on the acceptance of IoT technology," in *2024 International Conference on Digital Business and Technology Management (ICONDBTM)*, Oct. 2024, pp. 1–6, doi: 10.1109/ICONDBTM64135.2024.11122858.
[31] W. R. Giasi, C. Rahardja, and D. Anandya, "Factors affecting fashion product customer satisfaction: a case study of Indonesian e-commerce users," in *Proceedings of the 19th International Symposium on Management (INSYMA 2022)*, *Advances in Economics, Business and Management Research*, vol. 223, 2022, pp. 856–863, doi: 10.2991/978-94-6463-008-4_107.
[32] R. B. Kline, "Structural equation modeling," in *The Cambridge Handbook of Research Methods and Statistics for the Social and Behavioral Sciences*, vol. 1, A. L. Nichols and J. Edlund, Eds. Cambridge, U.K.: Cambridge University Press, 2023, pp. 535–558, doi: 10.1017/9781009010054.026.

BIOGRAPHIES OF AUTHORS



Angelo Pera is a dedicated educator and researcher with a master of science in information technology (MSIT). Currently teaching IT-related subjects, he specializes in web and mobile application development, networking, and the integration of the technology acceptance model (TAM) and ISO 25010 standards to evaluate both user acceptance and software quality. His research interests include educational technology, software development methodologies, IoT-based solutions, machine learning, network design and optimization. He is currently employed as an Instructor at Polytechnic University of the Philippines–Unisan Campus. He can be contacted at email: angeloppera@gmail.com.



Marco Jr. Del Rosario received his bachelor's degree in Information Technology from the Laguna State Polytechnic University and a master of information technology degree from the Technological University of the Philippines. He is currently a member of the Faculty of the College of Computer Studies at Laguna State Polytechnic University, Philippines. He has published papers related to improving local government processes and using string matching algorithms in computer software to detect plagiarism. His research interests include web systems development, performance and reliability analysis of computer software, e-government, IT education, and eLearning. He can be contacted at email: macky.delrosario@lspu.edu.ph.