International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 10, pp. 4161-4182
doi: 10.25147/ijcsr.2017.001.1.264
https://stepacademic.net

Long Paper

Convergence of Descriptive and Clustering Analysis of Awareness and Practices towards Uncovering Cyber Behavior Profiles of Senior High School Students

Christian Michael M. Mansueto
christianmichael.mansueto@umak.edu.ph
College of Computing and Information Sciences, University of Makati, Philippines
(corresponding author)

Mary Ellaine R. Cervantes
maryellaine.cervantes@umak.edu.ph
College of Computing and Information Sciences, University of Makati, Philippines

Jomariss B. Plan
jomariss.plan@umak.edu.ph
College of Computing and Information Sciences, University of Makati, Philippines

Roel C. Traballo
roel.traballo@umak.edu.ph
College of Computing and Information Sciences, University of Makati, Philippines
ORCID: 0009-0007-3470-1437

Date received: July 24, 2025
Date received in revised form: December 29, 2025
Date accepted: March 8, 2026

Recommended citation:

Mansueto, C. M. M., Cervantes, M. E. R., Plan, J. B., & Traballo, R. C. (2026). Convergence of descriptive and clustering analysis of awareness and practices towards uncovering cyber behavior profiles of senior high school students. *International Journal of Computing Sciences Research*, *10*, 4161-4182 https://doi.org/10.25147/ijcsr.2017.001.1.264

Abstract

Purpose – The study aims to identify the cyber behavior profiles and online habits of senior high school students by examining their awareness of cyber threats, digital practices, and

responses to online risks. The results serve as a basis for developing targeted cybersecurity education programs.

Method – A quantitative and descriptive research design was employed involving 206 senior high school students selected through convenience sampling. Data were collected using an online survey that measured cybersecurity knowledge, digital behavior, and online safety practices. To identify hidden behavior patterns beyond descriptive results, the DBSCAN clustering algorithm was applied.

Result – Findings indicated that students possess a moderate level of cybersecurity awareness, but their online safety practices vary. Many can identify common cyber threats and understand the importance of cybersecurity, yet exhibit risky behaviors. DBSCAN analysis revealed three behavior profiles: students with low awareness and high-risk behaviors, those with moderate awareness and inconsistent practices, and highly aware students who engage in proactive online safety.

Conclusion – The study concludes that cybersecurity awareness and safe online practices among senior high school students are unevenly distributed. Some students demonstrate strong awareness and responsible behavior, while others remain vulnerable due to limited knowledge and unsafe practices. DBSCAN clustering effectively revealed behavior patterns that would not be evident through descriptive analysis alone.

Recommendation – The study recommends implementing targeted, cluster-based cybersecurity education programs, especially for students with low to moderate awareness. Integrating cybersecurity topics into the curriculum and providing regular digital safety training can improve online behavior and reduce cyber risks.

Practical Implications – The findings provide guidance for educators and school administrators in designing data-driven cybersecurity initiatives. Identifying student groups based on risk and awareness allows schools to tailor interventions, promote responsible digital citizenship, and enhance overall online safety.

Keywords – Cybersecurity, digital safety practices, cyber behavior profile, DBSCAN clustering, descriptive clustering analysis

INTRODUCTION

The increasing integration of digital technologies into everyday life has reshaped how individuals communicate, learn, and access information. Senior high school students are among the most active users of digital platforms, relying heavily on the internet for academic activities, social interaction, and entertainment. This heightened digital engagement has led to increased exposure to online environments where cybersecurity threats, such as phishing, malware, identity theft, and online fraud, are prevalent. As digital

participation continues to expand, cybersecurity awareness and online safety practices have become essential components of responsible digital citizenship among students.

The digital invasion significantly changed global connectivity beyond recognition, leading to the facilitation of endless communication, access to information, and economic growth. The internet penetration in the Philippines saw a steep boom to about 83.8% in the first quarter of 2025. However, urban centers like Pagadian City have also been major beneficiaries of the robust digital infrastructure, such as mobile network coverage that is more than adequate (3G, 4G, 5G), 17 free Wi-Fi sites for educational and governmental services, and so on. This digital expansion was, nevertheless, trailed by a vice-like grip of cybercrime that witnessed the Philippine National Police declaring that 19,472 cases were reported in 2023, which is an increase of 68.98% or 11,523 cases higher than 2022, and the average number of cases being reported is 53 per day. The main issues with online scams, hacking, identity theft, sextortion, and cyberbullying are that they threaten to take over the vulnerable groups like women, youth, and vulnerable elders' safety and security (O'Malley, 2023; Ahmad & Smith, 2024). Accordingly, the enactment of Republic Act No. 10175 (R.A. 10175), the Cybercrime Prevention Act of 2012 in the Philippines, was the creation of the legal provisions to combat cybercrime and provide for online safety. Although the government has made some legislative efforts, the success of R.A. 10175 depends on public awareness and people practicing cybersecurity. Research also shows that there is a high awareness of common cyber threats among people. However, the understanding of specific legal regulations and advanced protection methods changes a lot among different groups of people. Notably, there are significant differences in the knowledge between older adults and less-educated individuals (Mahinay & Mamasalagat, 2025). As Pagadian City is the center of the region in Zamboanga Peninsula, it can be used as a perfect example to examine these conditions due to the new and fast development of its digital infrastructure and the still-limited research studies on cybercrime awareness in that area (Barican, 2024).

This study focuses on understanding how senior high school students perceive and practice cybersecurity in their everyday digital lives. Using a quantitative research approach, this study explores students' awareness of cyber threats, their online safety habits, and how they utilize various digital platforms. In particular, the study has three main objectives. First, it aims to describe the overall level of cybersecurity awareness, online safety practices, and digital platform usage among senior high school students. This is done using descriptive statistical tools such as frequency, mean, median, and mode to present a clear picture of students' digital behaviors. Second, the study seeks to identify distinct cybersecurity behavior profiles by applying the DBSCAN clustering algorithm. By grouping students based on similarities in their awareness, safety practices, and platform usage, the analysis goes beyond surface-level trends and uncovers meaningful behavior patterns. Finally, the study aims to interpret the identified clusters alongside the descriptive statistical results. This combined analysis helps explain differences in students' levels of cybersecurity awareness, common online behaviors, and degrees of vulnerability to cyber threats. Overall, the findings are intended to provide a deeper understanding of how students engage with digital technologies and where targeted cybersecurity interventions may be most needed.

The paper at hand explores the practices and awareness of cybersecurity among the digital citizens of high school students. The focus is on the students' knowledge that is related to the cybercrime menace, their experience of the digital dangers, and their cybersecurity awareness and online practices, as an efficient way to tackle these problems. In general, the authors chose a type of research called descriptive research design with a population of 206 internet users between the ages of 18 and 60. Data for the study were collected using a structured questionnaire that measured students' cybersecurity awareness, experiences of victimization, and online security behaviors. To better understand patterns within the survey responses, the DBSCAN clustering technique was applied to group students according to similar cybersecurity profiles. The analysis revealed three distinct clusters. Cluster 0 represents students with high cybersecurity awareness who consistently practice safe online behaviors and feel confident in recognizing potential threats. Cluster 1 includes students with a moderate level of awareness whose security practices are applied inconsistently. Cluster 2 consists of students with low awareness, limited use of security measures, and uncertainty when dealing with cyber threats, placing them at higher risk online.

By combining descriptive statistical analysis with DBSCAN clustering, this study adds depth to existing research on cybersecurity education. Rather than relying solely on overall averages, it highlights meaningful behavior patterns and identifies student groups with varying levels of risk and preparedness. These insights offer practical value for educators, school administrators, and policymakers, as they can be used to design targeted cybersecurity awareness programs and learning interventions. Ultimately, the findings support the goal of fostering safer, more informed, and more responsible digital behavior among senior high school students.

LITERATURE REVIEW

Cybercrime Trends and Impacts

The Philippines saw a big rise in cybercrime. Online scams were the main problem, going from 7,208 cases in 2022 to 14,030 in 2023. This shows a 94.64 % increase. Other computer crimes, like hacking, taking someone's identity, sextortion, and online bullying, also went up. Sextortion cases increased by 10 % in that time. These crimes use the hidden, widespread, as well as open nature of digital places. This makes finding and stopping them hard. Online scams often use phishing tricks, which fool users into showing private facts. Sextortion targets people who are easily hurt, especially young people, using social media plus dating apps - this leads to bad mental and financial problems. Women and young people face more danger. Online bullying and digital violence make them more open to harm. That shows a quick need for specific ways to stop these acts, which help groups such as Cluster 1. The economy and people's lives suffer much from cybercrime - it touches individuals, companies, and public faith in computer systems. Stealing identities plus computer fraud cause much money to disappear. Businesses in the Philippines say they lose millions each year. The mental effect is also a worry. People who suffer from sextortion and cyberbullying often feel

long-term hurt, like worry and sadness; they need good help. In Pagadian City, more internet access from free Wi-Fi and phone networks exposes people to these dangers. This is true especially for Cluster 1 users. They do not know much about scams, nor do they feel sure they can spot them. Local facts on cybercrime effects are few. Studies for specific areas are important - they help us understand how different groups feel and act when these dangers appear.

Advanced analytical methods increase knowledge of cybercrime trends across the clusters identified. K-means clustering defines Clusters 0 and 1, along with 2. It sorts incidents by type and severity. This allows law enforcement to put resources towards high-impact crimes that affect groups prone to harm, such as Cluster 1. Hierarchical clustering shows how crime types relate to demographic factors. As an example, it shows how age or gender affects how often people in the Unaware or Vulnerable cluster become victims. Principal component analysis identifies important reasons for victimization, like a lack of security or frequent internet use - these reasons affect Cluster 1 users more, as they seldom change privacy settings (Blancaflor et al., 2024). These methods offer a way to fit interventions to particular clusters using data; they help to direct resources to the specific needs of Pagadian City's digital citizens. The number of reported cybercrime cases grew. This growth likely shows that Cluster 0 users, who are informed and proactive, recognized threats and reported events more often. Cluster 1 users, however, often did not know if someone attacked them - this likely led to fewer reports, which made it harder to manage cybercrime well. (Barican, 2024). This study looked at how often cybercrime happened, plus what it did across different user groups - it sought to explain how people in Pagadian City dealt with online dangers. The results will help create specific actions - these actions include awareness campaigns for Cluster 1 users; they also include support for Cluster 2 users, who are average users. These actions reduce the financial and mental problems cybercrime causes. They also make R.A. 10175 better at keeping people safe online.

Cybersecurity Awareness and Education

Cybersecurity awareness plays an important role in protecting people from the growing range of online threats, yet clear differences can be seen among user groups in Pagadian City. Using k-means clustering, respondents were grouped into three distinct profiles. Cluster 0, described as *informed and proactive*, includes individuals with strong cybersecurity knowledge, confidence in spotting threats, and consistent protective behaviors such as regularly updating privacy settings. Cluster 1, labeled *unaware and vulnerable*, is largely made up of older or less-educated users who have limited awareness of online risks, making them more susceptible to phishing, malware, and similar attacks. Cluster 2 represents *average users* who have a basic understanding of cybersecurity but do not always apply safe practices consistently (Mahinay & Mamasalagat, 2025; Blancaflor et al., 2024). Survey results show that schools and universities are the primary source of cybersecurity awareness for 35.7% of respondents, followed by social media at 31.3%. In contrast, government-led campaigns reach only 8.9% of users, suggesting that the most vulnerable groups may not be effectively reached (Ahmad & Smith, 2024; Blancaflor et al., 2024). These gaps become even

more concerning as people engage with newer digital spaces, such as the metaverse, where limited awareness increases the risk of financial fraud and privacy violations (Jaipong et al., 2023).

Studies from Thailand further highlight that higher cybersecurity knowledge is closely linked to safer online behavior, especially in mobile banking. They also point to the value of integrating accredited cybersecurity lessons into existing programs as a practical model for Pagadian City (Limna et al., 2023; Juneam & Greenlaw, 2024). By using advanced analytical methods such as hierarchical clustering and PCA, key factors like age, education, and access to information can be identified, allowing for targeted interventions—basic training for Cluster 1, behavior strengthening for Cluster 2, and peer-led education roles for Cluster 0 (Blancaflor et al., 2024). In line with the Philippines' National Cybersecurity Plan 2023–2028 and local DICT initiatives, a mix of community workshops, accessible social media content, and school-based cyber hygiene programs can help close these gaps. Focusing on vulnerable users while engaging informed individuals as advocates can support the development of a safer and more resilient digital community in Pagadian City.

Legal Frameworks and Public Perception

R.A. 10175 establishes a very elaborate system to iron out the issues of cybercrimes that include online scams, hacking, and cyber libel, but also the preventive education part of it (Respicio, 2024). In Pagadian City, people's views on the law's effectiveness in different areas are still in flux, with a majority of 58% expressing confidence, 23.3% neutrality, and 18.6% skepticism, citing problems in enforcement and fear of possible overreach as the main reasons (Mahinay & Mamasalagat, 2025). Cluster 0 (Informed and Proactive) users, those highly aware, are more likely to see the law in a favorable light, whereas Cluster 1 (Unaware or Vulnerable) users, among whom a quarter do not know about the law, have low confidence as they do not understand it. Cluster 2 (Average User) users show mixed perceptions, reflecting their moderate awareness and inconsistent engagement with legal provisions (Tamdang & Borreros, 2024). Enforcement problems, such as insufficient resources and a lack of technical skills for local police that are not effective in the law's enforcement, especially for users of Cluster 1 who are often indecisive about going to report the incidents, are just a few examples of the law's impact that is limited by enforcement challenges. Only 21.1% of cybercrime victims in Pagadian City have reported incidents, saying that they found distrust or have not been made aware of the reporting mechanisms, a situation that is more evident among Cluster 1 (Mahinay & Mamasalagat, 2025). Cluster 0 users who can identify threats confidently will most likely report the incidents, whereas those in Cluster 2 may be unsure due to ambiguity in practices. Improving reporting procedures, for example, by installing a cybercrime hotline or developing an online portal, might not only bring about a change in reporting frequency among all clusters but also help in further enforcing.

Perceptions can be better understood through analytical methods. The study's clusters were defined by k-means clustering, which can further subdivide those respondents who are

most aware and confident in R.A. 10175 into groups, and then they can come up with solutions for each of the groups. Through hierarchical clustering, we can get an idea of how demographic aspects such as age or education affect the perceptions of individuals, and at the same time, PCA will tell which variables are most important, for example, trust in authorities or getting a legal education, which will be the main source of public sentiment (Blancaflor et al., 2024). These instruments can help policymakers to decide whom to target in driving outreach. If it is Cluster 1 users, they will need to work on raising awareness; Cluster 2 users will have to be convinced of the trust in law, and Cluster 0's confidence will be the vehicle that promotes peer education. By addressing barriers to legal awareness and reporting, this study aims to improve the implementation of R.A. 10175 in Pagadian City. Community-based legal education programs might be suitable for Cluster 1. On the other hand, a simplified reporting system can be the motivating factor for Cluster 2 and Cluster 0 users to come forward and report incidents. The transparent communication about the law's scope can be a way to eliminate the doubts of the overreach, particularly among the skeptical Cluster 2 users, thus the law R.A. 10175 will be recognized as the protection of all the clusters (Tamdang & Borreros, 2024).

Cybersecurity Practices and Victim Responses

The use of cybersecurity practices amongst different clusters is inconsistent to a great extent. The users of Cluster 0 (Informed and Proactive) are those who frequently change their privacy settings, do not click on suspicious links, and have a high confidence in recognizing threats; hence, they are the ones utilizing cybersecurity practices at a high level. The users of Cluster 1 (Unaware or Vulnerable) are those who rarely use privacy settings and have low confidence in recognizing scams; therefore, they become easily vulnerable. The users of Cluster 2 (Average User) are those who adopt moderate practices, but they are still inconsistent as they sometimes exhibit secure behavior and at other times become risky (Mahinay & Mamasalagat, 2025). In Pagadian City, 80% of respondents avoid suspicious links, and 73.3% use strong passwords, but only 56.7% use two-factor authentication, and 60% perform regular software updates, with Cluster 1 lagging in advanced practices (Blancaflor et al., 2024). Victim responses to cybercrime, however, are also different among clusters, with 31.6% of victims in Pagadian City implementing stricter security measures after an incident, 23.2% deciding not to react to incidents, and only 21.1% reporting to the police. Cluster 0 users are more likely to strengthen measures and report incidents, while Cluster 1 users, who are mostly unsure if they have been attacked, are the main reason for underreporting due to distrust or lack of knowledge. Cluster 2 users show mixed responses, reflecting their inconsistent practices (Mahinay & Mamasalagat, 2025). Underreporting obstructs law enforcement's capacity to fight cybercrime; there is a need for reporting systems that are easily accessible and support services for victims to prompt them to act, especially among Cluster 1 (Sikra & Renaud, 2023). Analytical methods can reveal in-depth information about these behaviors. K-means segmentation can categorize respondents by the level of security practice adoption, thus making differences more visible. For example, Cluster 0's proactive measures and Cluster 1's minimal engagement. A hierarchical clustering may also disclose the connections between practices and demographic factors. Thus,

showing how age is the driving factor of Cluster 2's inconsistent behaviors. Meanwhile, PCA can detect the main factors (e.g., trust in technology or access to resources) that influence each cluster (Blancaflor et al., 2024). These methods are a pointer to the direction of the possible targeted interventions. For instance, workshops for Cluster 1 can be designed to help that group catch up with the basic practices. These methods can guide targeted interventions, such as workshops for Cluster 1 to promote basic practices or campaigns for Cluster 2 to encourage consistency.

This study seeks to reveal habits in security methods and responses to victim reactions that will assist in planning ways to improve cybersecurity in Pagadian City. Educational programs may step up the Cluster 2 good practices, and Cluster 1 could only need basic awareness, whilst a reporting portal that is easy to use would probably facilitate the reporting of the incidents by the various clusters. Turning Cluster 0's behavior into a source of peer education and thus multiplying the impact will result in the creation of a stronger digital environment (Tamdang & Borreros, 2024).

Effectiveness of DBSCAN in Cybersecurity Clustering

From 2023 to 2025, the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) has continued to stand out as a reliable unsupervised learning technique in cybersecurity research. Its main strength lies in its ability to detect clusters of varying shapes while naturally identifying low-density data points as noise. This makes DBSCAN particularly well-suited for anomaly and intrusion detection, where abnormal activities often appear as scattered or irregular patterns rather than clearly defined groups (Artioli et al., 2024; Chamkar et al., 2025). Unlike K-means, which assumes evenly shaped clusters and forces all data into predefined groups, DBSCAN adapts more effectively to the complexity of real-world cybersecurity data such as network traffic, system logs, IoT communications, and graph-based structures (Retiti Diop Emane et al., 2024).

Recent studies highlight DBSCAN's practical value in operational settings. For instance, Chamkar et al. (2025) reported high detection accuracy with minimal false positives when applying DBSCAN to real-time security log analysis, while Mutha et al. (2024) achieved strong results in identifying threats to sensitive medical data. Its performance has been further enhanced through hybrid approaches, including adaptive parameter optimization for IoT botnet detection (Mustafa & Husien, 2023), integration with deep learning models for wireless sensor network attacks (Li et al., 2023), and gradient diffusion improvements in advanced frameworks (Wang et al., 2024).

Comparative research during this period generally favors DBSCAN over K-means in environments characterized by noise, imbalanced data, and irregular attack patterns—common features of intrusion detection systems, graph-based threats, and user behavior analytics (Artioli et al., 2024; Imran, 2025). However, some studies note that K-means can perform better when data patterns are well structured and clearly separable (Kumarasinghe et al., 2025). Overall, recent literature suggests that DBSCAN remains a flexible and effective

tool for modern cybersecurity challenges, particularly in contexts where threats are complex, evolving, and difficult to model using traditional clustering assumptions.

METHODOLOGY

Research Design

This work takes a quantitative- descriptive research approach to dig into the cyber character traits of senior high school students and to identify their profiles from the point of their awareness and good practices regarding cybersecurity and online safety. To guarantee that there was no bias in the selection of the sample and every student had an equal chance of being included in the study, respondents in senior high school were chosen using a convenience sampling technique. The researchers selected participants who were easily accessible to them throughout this process.

Data Gathering Procedures and Instruments of the Study

The researchers circulated the link to an online survey via official school communication channels that students frequently use. They also explained the study's aim, their role as participants, including their rights such as free will involvement, confidentiality, and anonymity of responses, and ensured that no one would lose their status for giving information before students gave their informed consent. The gathering of data proceeded until the targeted number of respondents, which was 206, was obtained. This research utilized descriptive statistics using Microsoft Excel to summarize data on the students' understanding and behavior in cybersecurity and online safety. It included core demographic variables such as age and gender. The great majority of the respondents' ages fall between 13 and 20 years, and there was approximately a balanced distribution of male and female students. The essential variables, namely the cybersecurity awareness, safety of the online world practices, digital platform usage, and basic demographic information, were captured by means of a structured, self-administered survey questionnaire. The questionnaire included multiple-choice and Likert-scale items, and the responses were converted into numbers for the analysis. The items were classified into three categories: Digital platform used, cybersecurity awareness, and online safety practices.

Questions that were relevant to the category, along with the justifications as shown in Table 1, were picked. This table is a representation of how the various survey questions are grouped and conceptualized for detailed analysis within this study. This classification is the basis of understanding the next descriptive statistics presentation, and more importantly, it is the input for the clustering analysis that is intended to discover the existence of distinguishable cyber behavior profiles among senior high school students.

Table 1. Categorization of Survey Questions for Detailed Analysis

Category	Questions to Analyze	Justification
Digital Platform Use	Q1, Q19, Q20	Usage Pattern
Cybersecurity Awareness	Q2, Q4, Q23, Q24, Q25, Q29	Knowledge/ confidence
Online Safety Practices	Q6, Q8, Q10, Q11, Q22, Q26	Actual Behaviors

Statistical Analysis

Frequency and percentage were the major ways that were applied to identify the number and proportion of respondents who selected particular responses. These measures are very important for presenting categorical data such as demographic profiles, internet usage, and selected online behaviors, which make it possible to compare and interpret the data easily. At the same time, the mean was the main way that was used to find out the average responses in scaled items, that is to say, the levels of confidence, knowledge, and the perceived importance of cybersecurity. It gave a broad look at the students' combined tendencies. The mode was carried out to find the most frequent response, which enabled the understanding of the most common perspectives or behaviors among the respondents. On top of that, the standard deviation was figured out as a means for determining the extent of consistency of response situations around the mean. A low standard deviation represented that the students agreed, while a high value signified different opinions or experiences. In combination, these various statistics provided a clear and comprehensive picture of the students' cybersecurity awareness and their online safety practices.

DBSCAN Clustering Technique

To move beyond simple descriptive results and gain deeper insight into student behavior, the study applied the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm. Before clustering was performed, the data were carefully prepared through cleaning, encoding of categorical responses, and normalization to ensure that all variables could be fairly compared. DBSCAN was then used to group students based on shared patterns in cybersecurity awareness, online safety practices, and digital platform use, while also identifying outliers that may reflect unusual or high-risk behaviors. The clusters that emerged were analyzed alongside the descriptive statistics, allowing the researchers to clearly define and interpret distinct cybersecurity behavior profiles among the students.

RESULTS

This part of the paper details the results of a survey that was completed by 206 senior high school student respondents. The data are arranged in tables. At first, descriptive statistics, including frequencies, percentages, means, standard deviations, and modes are shown in order that the demographic profile of the respondents, their digital platform usage patterns, levels of cybersecurity awareness, and reported online safety practices are summarized. After these preliminary resumés, the results of the K-means clustering analysis will be given to demonstrate the cyber behavior profiles that were identified among the population that was sampled. This structured presentation is intended to give a

comprehensive empirical basis for understanding senior high school students' cyber behaviors and for the further discussion of these findings.

Descriptive Statistics Analysis

The survey of students comprised 206 students in total, out of which 111 (53.88%) were females, while 95 (46.12%) were males. Table 2 illustrates this distribution, which implies a slight predominance of female students in the sample. The digital platform usage patterns of the senior high school student respondents are presented in Table 3. This part of the paper describes the frequency of internet use, common online activities, and the amount of time spent on the web each day. The key focus of this section is on the results of a survey of the cybersecurity awareness levels of a group of senior high school students, who are presented in Table 4. It also discusses their basic awareness of some dangers, their own estimation of the knowledge that they have, their confidence in detecting threats, the importance they give to cybersecurity, and their confidence in protecting themselves.

Table 2. Gender Distribution

Gender	Frequency	Percentage
Male	95	46.12%
Female	111	53.88%
TOTAL	206	100.00%

Table 3. Digital Platform Usage

Item Number	Relevant Question	Options	Frequency	Percentage
1	How often do you use the Internet in a typical week?	A few times a week	3	1.46%
		Once a day	15	7.28%
		Once a week	2	0.97%
		Rarely	1	0.49%
		Several times a day	185	89.81%
19	What do you usually do online when you browse the web?	Information Seeking	93	45.15%
		Online Shopping	108	52.43%
		Online Financial	75	36.41%
		Research	147	71.36%
		Social Media	191	92.72%
		Communication	156	75.73%
		Watching Videos	174	84.47%
		Gaming	107	51.94%
		1 hour - 3 hours	42	20.39%
20	How much time do you spend surfing the web in a day?	4 hours- 6 hours	41	19.90%
		7 hours- 9 hours	48	23.30%
		Less than 1 hour	17	8.25%
		More than 9 hours	58	28.16%

The section of the text outlines the online safety measures that have been reported among the senior high school students. The information is visually represented in Table 5. The discussion explores the students' behavioral characteristics towards the above-mentioned areas of online safety, such as updating software, password management, suspicious links, backing up data, and privacy settings.

Table 4. Cybersecurity Awareness

Item Number	Relevant Question	Options	Frequency	Percentage
2	Are you aware of phishing/malware/ etc.?	Yes	189	91.75%
		No	8	3.88%
		Maybe	9	4.37%
Item Number	**Relevant Question**	**Mean**	**Standard Deviation**	**Mode**
4	Rate your knowledge on protecting personal info	3.310679612	0.69182158	3
23	How knowledgeable do you consider yourself?	3.04368932	0.6499786	3
24	Confidence in identifying threats	3.689320388	0.91629292	4
25	Importance of cybersecurity	4.436893204	0.87979934	5
29	Confidence in self-protection	3.140776699	0.6204541	3

Table 5. Online Safety Practices

Item Number	Relevant Question	Options	Frequency	Percentage
6	Update software regularly	Always	83	40.29%
		Often	78	37.86%
		Sometimes	34	16.50%
		Rarely	8	3.88%
		Never	3	1.46%
8	How often change passwords	Every month	62	30.10%
		Every week	9	4.37%
		Every year	85	41.26%
		Never	50	24.27%
10	Click on suspicious links	Yes, often	12	5.83%
		Yes, occasionally	35	16.99%
		Not sure	7	3.40%
		No, never	152	73.79%
11	Backup important data	Regularly	84	40.78%
		Occasionally	80	38.83%
		Rarely	38	18.45%
		Never	4	1.94%
22	Examine suspicious links/websites	Yes	179	86.89%
		No	27	13.11%
26	Review and adjust privacy settings	Always	65	31.55%
		Often	69	33.50%
		Sometimes	60	29.13%
		Rarely	9	4.37%
		Never	3	1.46%

DBScan Clustering Analysis

Figure 1 shows the sorted distances of each observation to its 5th nearest neighbor. A pronounced elbow appears around distances of approximately 1.09–1.14, marking the transition from dense regions to sparse observations. Based on this elbow, an eps value of

1.10 was selected to balance cluster separation while minimizing noise. Distances beyond this range (≈2.19) correspond to outliers identified as noise by DBSCAN.

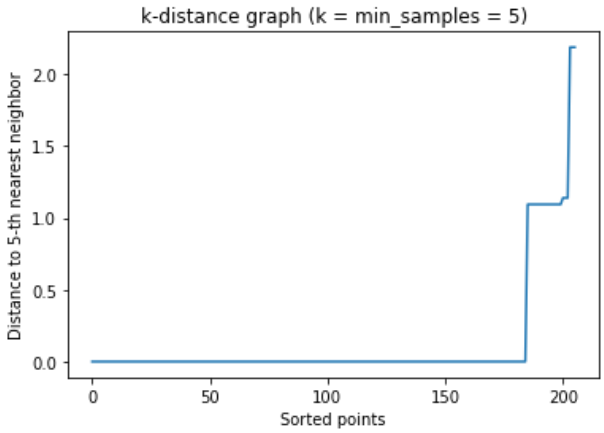

Figure 1. k-distance graph for DBSCAN parameter tuning (k = min_samples = 5)

Table 6. DBSCAN parameter sweep (eps grid)

Item Number	eps	min_samples	n_clusters	noise_ratio	silhouette_non_noise
1	0.3	5	8	0.101942	1
2	0.325	5	8	0.101942	1
3	0.35	5	8	0.101942	1
4	0.375	5	8	0.101942	1
5	0.4	5	8	0.101942	1
6	0.425	5	8	0.101942	1
7	0.45	5	8	0.101942	1
8	0.475	5	8	0.101942	1
9	0.5	5	8	0.101942	1
10	0.525	5	8	0.101942	1
11	0.55	5	8	0.101942	1
12	0.575	5	8	0.101942	1
13	0.6	5	8	0.101942	1
14	0.625	5	8	0.101942	1
15	0.65	5	8	0.101942	1

The DBSCAN parameter tuning results show that when the *eps* value falls between 0.30 and 0.65, the clustering outcome remains the same. Within this range, the algorithm consistently identifies eight clusters, maintains a noise level of about 10.2%, and produces a perfect silhouette score of 1.0 when calculated on non-noise data points. This level of stability suggests that the data naturally form very tight and clearly separated groups, a pattern that aligns with the discrete response structure of Likert-scale survey data. However, despite these strong statistical indicators, using such small *eps* values leads to over-segmentation. The resulting clusters are too fine-grained, making them difficult to interpret in a meaningful way. To address this issue and achieve clearer, more practical groupings, larger *eps* values were therefore examined to produce a clustering solution that better balances statistical quality with interpretability.

Table 7. Cluster profiling (means per cluster)

DBSCAN_Cluster	24. On a scale of 1 to 5 (1 being not confident and 5 being very confident) how confident are you in your ability to identify and protect yourself from online threats?	25. On a scale of 1 to 5 (1 being lowest and 5 being highest) how would you rate the importance of cyber security in your daily life?
0	3.886364	5
1	3.634146	4
2	3.185185	3

The DBSCAN results revealed three clear groups of respondents, along with a small number of outliers. Cluster 0, which included most participants, was characterized by a strong belief in the importance of cybersecurity and a high level of confidence in recognizing and responding to online threats. Cluster 1 reflected a more moderate stance, with average levels of confidence and perceived importance. In contrast, Cluster 2 showed the lowest confidence in handling cyber risks, even though members still rated cybersecurity as moderately important.

The relatively small number of outliers suggests that most respondents follow recognizable and consistent behavior patterns. Taken together, the clusters point to a gradual decline in cybersecurity awareness and self-efficacy from one group to the next, highlighting clear differences in users' engagement with and readiness for online security challenges.

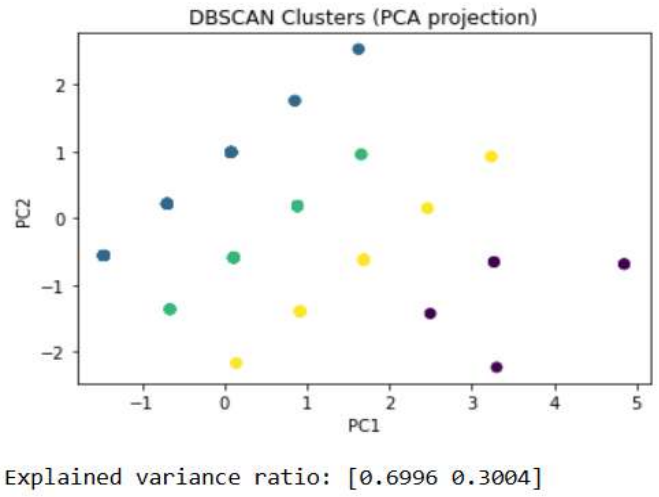

Figure 2. PCA-based visualization of the DBSCAN clustering results

Figure 2 illustrates that the first principal component captures about 69.96% of the total variance in the data, while the second accounts for the remaining 30.04%. Together, these two components fully represent the variation present in the original feature set. The visualization shows that the three identified clusters are clearly separated in space, with very little overlap, which supports the reliability of the density-based clustering results. The diagonal pattern formed by the data points suggests a strong relationship between

respondents' confidence in cybersecurity and how important they perceive it to be, indicating that these two factors tend to increase or decrease together.

DISCUSSION

Data on digital platform usage (Table 2) reflects senior high school students as individuals who are very active and deeply integrated into the digital world. A vast majority (almost 90%) of them who use the internet "Several times a day" is indicative of their continuous connectivity, which is a feature of the "digital native" generation. This high frequency of access constitutes the essential foundation for their exposure not only to the good but also to the bad of the online environment. The mentioned online activities again highlight their profound involvement in the digital world. The dominance of social media (92.72%), Watching Videos (84.47%), and Communication (75.73%) shows that their main online focus is targeting social interaction, entertainment, and interpersonal connections. This trend is typical for teenagers and is also consistent with the global youth internet usage pattern. The peak of engagement in Research (71.36%) points out their academic necessities as senior high school students; it also signifies that the internet is a tool of paramount importance for learning. The most outstanding result is the length of daily web surfing. A majority of those who answered stated (28.16% for "More than 9 hours" and 23.30% for "7-9 hours") that they were online for more than 7 hours a day, which indicates that they are exposed to online environments for a long time. This great amount of time online directly relates to a higher chance of coming across cybersecurity threats (for instance, malware, cyberbullying, misinformation, privacy breaches) and thus, it outlines the importance of implementing sound cybersecurity knowledge and practicing safe online behaviors. Students who are on the internet for a longer period are more likely to be exposed to several online risks, and this might be the basis for the formation of their cyber behavior profiles, according to the clustering analysis.

Table 4 clearly shows that a great majority of the respondents, 189 (91.75%), indicated that they are aware of phishing, malware, and other similar threats. A very small number of people reported that they do not ("No" - 3.88%) or are not sure ("Maybe" - 4.37%) about their awareness. The results also indicate that senior high school students have a high level of self-reported cybersecurity awareness. The fact that over 90% of them are aware of the common threats, which are phishing and malware, is a good sign. This means that the simple information about these cyber-risks that are going around has reached this group of young people, probably via several sources such as school programs, media exposure, or informal learning from peers and family. But when a closer look is taken at the self-assessed knowledge and confidence scores, it tells a different story. Students say they are aware, but their self-assessed knowledge (Q4: Mean 3.31; Q23: Mean 3.04) and confidence in self-protection (Q29: Mean 3.14) are still at the medium level. The difference between the reported general awareness of threats and the more moderate confidence in practical knowledge or self-protection is very big. It means that students probably know about phishing or malware, but they may not feel that they have enough knowledge of how they can protect themselves and use safe practices regularly. This could indeed point to a

"knowledge-practice gap," where people understand the theory, but this understanding doesn't always lead to them changing their security behaviors. Interestingly, the confidence for threat identification (Q24: Mean 3.69) was higher than for self-assessed knowledge on protecting personal info or general self-protection confidence. It could mean students are more comfortable recognizing danger signs (e.g., a suspicious email) than being able to list the steps to neutralize the danger or to secure their digital life. This difference might become the key target point for educational interventions to be more focused on practical skills than only threat identification. On the other hand, the highest level of perceived importance of cybersecurity (Q25: Mean 4.44; Mode 5) might be the most positive finding so far. It shows that senior high school students fundamentally understand that cybersecurity is indispensably important in their lives. The fact that the students' attitude towards cybersecurity is so positive is an implication that if the education provided is practical and effective, the students will be willing and interested in learning and implementing safe behaviors. Their understanding of the significance of cybersecurity can act as a powerful basis for further launching awareness campaigns and practical skills training.

In a nutshell, the data on online safety habits (table 5) shows a positive picture among senior high school students, though it is a little mixed. The signs of positive security behaviors are very evident, but there are also some areas of potential vulnerabilities. The high numbers mainly come from regular software updates (78.15% "Always" or "Often") and examining suspicious links/websites (86.89% "Yes"), which mean good security hygiene. Changing software regularly is highly important for fixing the vulnerabilities, and checking out the suspicious links is a very active approach of being threat-free, which fits very well with the fact that they have a high threat awareness. The same goes for the high percentages of setting privacy settings (more than 94% "Always," "Often," or "Sometimes"), which is a good indication that they realize the control of the data they give out, which is an extremely important point here in the digital world. The very fact that only a small percentage do not click on suspicious links at all (73.79% "No, never") shows that the majority are cautious, which is great.

The most obvious reason for it is definitely awareness campaigns that have been carried out, among others, in the case of phishing and malicious links. On the other hand, issues are still there, and they have to be addressed. Even though data backup is performed by a large percentage of users, the fact that nearly a quarter (24.27%) "Never" change their passwords is a major vulnerability that can be easily exploited. Very weak or unchanged passwords are the main reason for hacking of accounts. The fact that the majority of those surveyed would like to change their passwords only once a year does not reflect current cybersecurity threats and practices which are more persistent and require more frequent changes. This clearly shows that although people understand the importance of cybersecurity, their password management is not so good. Besides this, although a high rate states they would "never" click on suspicious links, the combined 22.82% who say "Yes, often," "Yes, occasionally," or are "Not sure" still constitute of a significant portion of the sample, who are very vulnerable to phishing and other social engineering attacks.

This signifies that even if they understand what a suspicious link is, they are still vulnerable to curiosity, urgency, deception, or even a lack of consistent vigilance. Such a group could be at a high risk of becoming the victims of cyber incidents. The descriptive analyses directly preceding have thoroughly outlined the demographic make-up of senior high school students, their typical digital platform usage patterns, their cybersecurity awareness levels, and the online safety practices they have reported. Although these analyses showed the general trends (such as high internet engagement and mixed safety behaviors), they also clearly revealed the student population's inherent diversity.

Based on the DBSCAN results, three clear cybersecurity behavior profiles emerged among the students, each reflecting different levels of awareness, confidence, and online safety practices.

Cluster 0: "High Cybersecurity Awareness and Proactive Safety Practices."

Students in this group demonstrated consistently high scores in cybersecurity awareness, confidence, and perceived importance, as reflected in Tables 4.0 and 5.0. Their responses indicate a strong understanding of cyber risks and a positive attitude toward online safety. Data on digital platform usage and safety practices further show that these students regularly engage in proactive behaviors, such as checking suspicious links, updating software, and managing privacy settings. Overall, Cluster 0 represents a highly informed and responsible group whose behaviors align with recommended cybersecurity practices.

Cluster 1: "Moderate Awareness and Inconsistent Safety Practices."

The descriptive results suggest that most respondents fall within a moderate range of cybersecurity awareness and online safety behavior, and this pattern is clearly reflected in Cluster 1. Students in this group possess basic knowledge of cybersecurity concepts but do not apply safe practices consistently. While they show moderate confidence in identifying threats, their actual behaviors—such as updating software or reviewing privacy settings—tend to be irregular. As a result, Cluster 1 closely represents the "typical" Grade 11 student identified in the descriptive analysis.

Cluster 2: "Low Cybersecurity Awareness and High-Risk Practices."

Cluster 2 includes students who scored below the overall averages in terms of awareness, confidence, and perceived importance of cybersecurity. Tables 4.0 and 5.0 indicate that these students are less familiar with common threats and more likely to engage in risky behaviors, such as clicking unverified links and rarely changing passwords. This cluster reflects a group that is particularly vulnerable to cyber threats due to limited knowledge and unsafe online habits.

Overall, the DBSCAN analysis successfully revealed meaningful patterns that would not be evident from descriptive statistics alone. Although smaller *eps* values initially produced stable but overly detailed clusters, selecting a larger value resulted in clearer and more interpretable groupings with minimal noise. PCA visualization further supported the validity of the clustering by showing clear separation among the three groups. These findings

highlight that cybersecurity awareness varies widely among students and emphasize the need for targeted education and interventions tailored to each profile.

CONCLUSIONS AND RECOMMENDATIONS

The study showed that DBSCAN is an effective tool for uncovering meaningful patterns in users' cybersecurity awareness and confidence. By carefully tuning the model parameters using the k-distance graph, the analysis was able to avoid overly fragmented results and instead produce clear, interpretable clusters with very little noise. Three distinct user groups emerged, each reflecting different levels of perceived importance of cybersecurity and confidence in protecting themselves online. This finding highlights that cybersecurity awareness and self-efficacy vary considerably among users rather than following a single, uniform pattern. The PCA visualization further supported these results by showing clear separation and strong internal consistency among the clusters.

In light of these findings, cybersecurity awareness initiatives would benefit from a more targeted approach. Users with lower awareness and confidence may need basic, introductory training that focuses on fundamental concepts and everyday safety practices. In contrast, users who already demonstrate higher confidence may benefit more from advanced or specialized guidance that builds on their existing knowledge. To strengthen future research, it is recommended that subsequent studies include additional variables, larger and more diverse samples, and longitudinal designs. These improvements would help validate and extend the use of density-based clustering for understanding user behavior in cybersecurity contexts.

RECOMMENDATION FOR FUTURE WORKS

Future research can build on these findings by including a wider range of demographic, behavioral, and contextual factors to gain a clearer understanding of what influences differences in cybersecurity awareness and confidence. Using longitudinal research designs would make it possible to track how user behaviors change over time and to assess how effective cybersecurity education or intervention programs really are. From a methodological standpoint, future studies could also examine hybrid or alternative density-based clustering methods and apply stronger validation techniques that are better suited to handling noisy or complex data. Extending this approach to larger and more diverse populations would further strengthen the results, improve their generalizability, and help inform the development of well-targeted, evidence-based cybersecurity awareness programs.

IMPLICATIONS

The results of this study carry important implications for education, policy, and everyday practice in strengthening cybersecurity awareness among senior high school students. The

presence of distinct cybersecurity behavior profiles shows that students differ widely in their level of awareness, online safety habits, and exposure to cyber risks. This finding highlights the need for targeted approaches rather than one-size-fits-all cybersecurity programs. For educators and school administrators, these insights provide a practical basis for developing data-driven interventions that focus on students who are most at risk, while at the same time reinforcing and sustaining positive behaviors among those who already demonstrate higher awareness. At the policy level, the findings support the inclusion of cybersecurity and online safety topics within the senior high school curriculum, helping ensure that such education is delivered consistently and sustainably. From a research perspective, the study also illustrates the value of combining descriptive statistical analysis with DBSCAN clustering to reveal meaningful behavior patterns, offering a useful methodological framework for future studies on digital safety and student online behavior.

ACKNOWLEDGEMENT

The researchers want to thank the senior high school students and their teachers for their cooperation and support during the study. Their readiness to share valuable insights into digital media usage made this research possible. The authors also appreciate the University of Makati for creating a supportive academic environment for research. This study did not receive any specific grant or funding from public, commercial, or nonprofit institutions.

FUNDING

The study was not funded, and no institution was asked for any funding.

DECLARATIONS

Conflict of Interest

The authors declare that they have no conflict of interest in the conduct and reporting of this study.

Informed Consent

Informed consent was obtained from all student participants before data collection. Participation was voluntary. Respondents were assured of confidentiality and the academic purpose of the research. Since the study involved senior high school students, consent was coordinated with the respective school administrators and teachers to ensure ethical compliance.

Ethics Approval

The authors declare that all applicable ethical standards were fully observed during the conduct, completion, and finalization of this research.

REFERENCES

Ahmad, D. N. F., & Smith, N. (2024). Digital safety for women and children: Legal and policy challenges in Indonesia, Philippines, and Thailand. *Journal of Law and Legal Reform,* 5(1), 123–140.

Artioli, P., Maci, A., & Magrì, A. (2024). A comprehensive investigation of clustering algorithms for User and Entity Behavior Analytics. *Frontiers in Big Data, 7*, Article 1375818. https://doi.org/10.3389/fdata.2024.1375818

Barican, A. (2024). Cybercrime awareness among senior high school students in Pagadian City. *Journal of Cybersecurity Studies, 3*(2), 45–60.

Blancaflor, E. B., Del Rosario, P. M., & Santos, J. R. (2024). Cybercrimes in online audiovisual content sharing services: A literature review of client-side caches and forensic techniques. *IEEE Transactions on Information Forensics and Security, 19*, 456–467. https://doi.org/10.1109/TIFS.2024.10698579

Chamkar, S. A., Zaydi, M., Maleh, Y., & Gherabi, N. (2025). *ML-driven log analysis for real-time cyber threat detection in security operation centers* [Preprint]. Preprints.org. https://doi.org/10.20944/preprints202504.2197.v1

Imran, I. I. (2025). Exploiting anomalies with data mining techniques to enhance cloud security. *Mathematical Modelling of Engineering Problems, 12*(2), 636–646. https://doi.org/10.18280/mmep.120227

Jaipong, P., Sritapan, C., & Kittipong, P. (2023). Security and privacy risks in the metaverse: Challenges for future digital environments. *Journal of Virtual Environments and Emerging Technologies,* 5(2), 77–91.

Juneam, P., & Greenlaw, R. (2024). Integrating cybersecurity education into university curricula: Lessons from Southeast Asia. *Education and Information Technologies, 29*(4), 4387–4405. https://doi.org/10.1007/s10639-023-11890-2

Kumarasinghe, K. G. K. I., Kumarsiri, I. P. M. P., Pussewalage, H. S. G., Kumarasinghe, K. A. G. T. V., Liyanage, K. S. K., Manawadu, Y. P., & Mamankaran, H. (2025). Efficient post-processing of intrusion detection alerts using data mining and clustering. In Proceedings of the 22nd International Conference on Security and Cryptography (SECRYPT 2025) (pp. 682–689). https://doi.org/10.5220/0013558700003979

Li, Q., Ma, Y., & Wu, Y. (2023). Utilize DBN and DBSCAN to detect selective forwarding attacks in event-driven wireless sensor networks. *Engineering Applications of Artificial Intelligence, 126*, Article 107122. https://doi.org/10.1016/j.engappai.2023.107122

Limna, P., Kraiwanit, T., & Jermsittiparsert, K. (2023). Cybersecurity awareness and safe online practices among mobile banking users in Thailand. *Journal of Asian Finance, Economics and Business, 10*(2), 281–289. https://doi.org/10.13106/jafeb.2023.vol10.no2.0281

Mahinay, C. J. D., & Mamasalagat, M. P. (2025). Assessing cybercrime awareness and experiences among netizens: A study on the impact of R.A. 10175 in Pagadian City. *International Journal of Research and Innovation in Social Science, 9*(5), 216–230. https://dx.doi.org/10.47772/IJRISS.2025.905000216

Mustafa, D. H., & Husien, I. M. (2023). Adaptive DBSCAN with Grey Wolf Optimizer for botnet detection. *International Journal of Intelligent Engineering and Systems, 16*(4). https://doi.org/10.22266/ijies2023.0831.33

Mutha, R., Barekar, S. S., Borhade, R. R., Raja Kumar, J. R., Dhage, P., & Gotmare, V. (2024). Cybersecurity technologies for protecting social medical data in public healthcare environments. *South Eastern European Journal of Public Health*. https://www.seejph.com/index.php/seejph/article/view/485

O'Malley, R. (2023). Short-term and long-term impacts of financial sextortion on victims' mental well-being. *Journal of Interpersonal Violence, 38*(9–10), 6789–6810. https://doi.org/10.1177/08862605221127123

Philippine National Police. (2023). *Annual cybercrime report 2023*. Philippine National Police Anti-Cybercrime Group. https://acg.pnp.gov.ph

Republic of the Philippines. (2012). *Republic Act No. 10175: Cybercrime Prevention Act of 2012*. Official Gazette of the Republic of the Philippines. https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/

Respicio, H. (2024). Understanding and navigating RA 10175: The Cybercrime Prevention Act of 2012. Lawyer Philippines. https://www.lawyer-philippines.com/articles/understanding-and-navigating-ra-10175-the-cybercrime-prevention-act-of-2012

Retiti Diop Emane, C., Song, S., Lee, H., Choi, D., Lim, J., Bok, K., & Yoo, J. (2024). Anomaly detection based on GCNs and DBSCAN in a large-scale graph. *Electronics, 13*(13), Article 2625. https://doi.org/10.3390/electronics13132625

Second Quarter Regional Economic Situationer. (2024). National Economic and Development Authority. https://nro9.neda.gov.ph/wp-content/uploads/2024/08/CY-2024-2QRES.pdf

Sikra, J., & Renaud, K. V. (2023). UK cybercrime, victims, and reporting: A systematic review. Crime Science, 12(1), 1–15. https://doi.org/10.1186/s40163-023-00198-6

Tamdang, D., & Borreros, A. J. (2024). Raising awareness of IT regulations and compliance through symposiums in Philippine public high schools. Journal of Physics, Mathematics, and Informatics, 2(1), 89–102.

Wang, H., Huang, X., & Wu, Y. (2024). GD3N: Adaptive clustering-based detection of selective forwarding attacks in WSNs under variable harsh environments. Information Sciences, 665, Article 120375. https://doi.org/10.1016/j.ins.2024.120375

Author Biography

Christian Michael Marquez Mansueto is a faculty member currently teaching at the University of Makati and Jose Rizal University, with over a decade of experience in academia. He holds advanced degrees in information technology, including a Doctorate in Information

Technology from De La Salle University-Dasmariñas (academically completed) and a Master's in Information Systems from the University of Makati. He is also recognized for his academic contributions, such as developing IT-based management systems and presenting papers at academic conferences. He has passed multiple certifications, including TESDA's National Certificate II in Computer Hardware Servicing and Java Information Technology Specialist. He is also a certified Microsoft Innovative Educator and has received accolades such as the Most Outstanding Educator for the academic year 2023-2024.

Mary Ellaine R. Cervantes is a college professor with extensive experience in the fields of education and information systems. She holds a Bachelor's degree in Computer Science from Adamson University, a Master's degree in Technology Education from the Technological University of the Philippines, and a Master's degree in Information Systems from the University of Makati. She has also academically completed her Doctor in Information Technology program at De La Salle University – Dasmariñas, Cavite. With nearly 25 years of teaching experience, Ms. Cervantes is deeply committed to fostering student engagement and enhancing learning outcomes.

Jomariss B. Plan is a graduate of Master of Science in Information Technology (MSIT) from Polytechnic University of the Philippines (PUP-QC) and Bachelor of Science in Computer Science (BSCS), a Cum Laude, from STI-College Fairview. She has academically completed her Doctor in Information Technology program at La Consolacion University Philippines. She is presently working as an Assistant Professor III at the University of Makati. Currently, she is one of the committee members of the University of Makati Research Ethics Committee (UMREC). Asst. Prof. Plan is certified in Microsoft Word (Microsoft Office Specialist (MOS)), Certified Microsoft Innovative Educator (MIE), and Blockchain Excellerator Expert Qualifier. She has certifications in Java Programming Information Technology Specialists (ITS), and Database ITS.

Roel C. Traballo is a seasoned information technology educator with extensive expertise in programming and computing education. He has been a permanent faculty member of the University of Makati – College of Computing and Information Sciences (CCIS) for nearly 18 years and previously served as the department chair of the former College of Computer Science (CCS) from 2015 to 2021 and as a part-time IT faculty member at Jose Rizal University for 23 years. He has completed all academic requirements for the Doctor of Information Technology (DIT) at De La Salle University–Dasmariñas and holds a Master of Science in Information Technology (MSIT) from the University of La Salette and a Bachelor of Science in Mathematics with a major in Computer Programming from the Polytechnic University of the Philippines. Assoc. Prof. Traballo also holds multiple professional certifications, including Python, Data Analytics, Java Programming, Databases, and Microsoft Excel, alongside TESDA NC-2 national certification and CodeChum Certified Programmer status in COMPROG1 for Java, C#, C++, and Python. He is an active member of the Philippine Society of Information Technology Educators (PSITE) - NCR chapter, contributing to the advancement of IT education in the Philippines.