# Face-Nest, Facial Recognition Attendance System with Timestamp Logs: An Information System Security Approach

Luthfi Jaka Satria*, Intan Farahana Kamsin, and Nur Khairunnisha Zainal

***Abstract*—In the ever-expanding world of technological advancement and development, many new concepts and technologies are being presented to the world that aim to streamline current processes or innovate an approach to an existing problem. The pandemic has brought forward new operating conditions that have forced many to make the leap to go fully digital, including the education sector. Therefore, this conducted study aims to develop facial recognition attendance system that promotes convenience and accurate attendance marking. This is crucial to ensure time taken to record students' attendance could be minimize without any sacrifice in accuracy, and theoretically limit the occurrence of proxy attendance within the education setting. Quantitative research was conducted in Malaysia, which involved 82 students from private university. This is crucial to ensure students are able to engage in the teaching and learning process, and at the same time develop a meaningful learning environment. Data were analyzed using the Statistical Package for the Social Sciences (SPSS) software. Research findings show that the facial recognition attendance system contribute to improve the quality of education within online settings by limiting the occurrence of attendance proxying among students. Therefore, this finding contributes by providing a research direction for improving attendance in education setting by utilizing facial recognition attendance system.**

***Index Terms*—Facial recognition, computer vision, attendance system, education**

## I. Introduction

### A. Background to the Study

Recent technological advancements have the power to transform and dictate how society operates through complex integrations that show no signs of slowing down. The education sector is among the largest businesses that exist in modern society, where technological adoption is usually absorbed faster among young adults in comparison to the older generation [1]. Attendance plays an integral part in maintaining integrity and keeping track of elapsed time. Among other things, one of the main benefits of attendance is that it saves money, increase productivity, yield in the workspace while among students and young adults; it demonstrates a track record of reliability, responsibility, and overall shows one's general ability to take instructions and perseverance. That being said, there are many things that factor into the record of overall attendance [2].

One of the major factors in education is students' engagement in class, which is influenced by enriching educational experiences, active involvement, and collaboration. However, the pandemic has brought challenges that have hindered progress in these aspects of education, leading to lower student engagement. The barrier that exists between students and institutions is the mode of study; concerns regarding the effects of the pandemic on the quality of graduates surfaced, thus leading to institutions finding alternatives and ways to ensure student engagement and attendance [3]. One of the mandatory requirements for students to participate in examinations is attendance; students whose attendance drops below an acceptable level would be barred from the examinations as they are deemed unfit to attend the examinations. This study presents the potential implementation of a facial recognition attendance system in educational settings. The study explores key aspects of facial recognition that both students and institutions would benefit from.

### B. Problem Context

As the online class attendance system is heavily reliant on students marking their attendance using quick response (QR) codes, it is susceptible to students asking their friends to send them the code or mark attendance for their friends.

Ensuring student engagement also plays a pivotal part in making sure overall student attendance does not fall below the minimum limit. This is because attendance acts as a ticket to attending an exam, and having a system that gives students leverage to mark each other's attendance may cause a reduction in the credibility of the institution. As a result, students would technically attend fewer classes and may not be able to perform as well as they should.

However, time zones may be at the root of a student's ability to learn, especially when the time difference is not exactly favourable. This may lead to problems such as disrupted sleep schedules which leads to sleep deprivation, shifted active times, and not enough resting times [4], which would then translate to the students not attending the classes properly. Additionally, this study aims to assess how the recent changes in ways to conduct education impact the unexplored relationship between attendance and students' performance during the pandemic.

The general assumption for this study is that students tend to neglect the importance of their attendance due to an online mode of study. The aim of this project is to limit the amount of attendance proxying through the current methods of attendance taking, ranging from QR code to roll call. The system is projected to allow for better attendance records by students, which implies better-quality graduates. Limitations to this study include coding best practices, standard security implementation, and hardware constraints. Coding best practices stem from the developer's experience and

Manuscript received July 5, 2022; revised August 4, 2022; accepted February 16, 2023.

The authors are with the School of Technology, Asia Pacific University of Technology and Innovation (APU), Malaysia

*Correspondence: jkstria@gmail.com (L.J.S.)

knowledge in the field of programming, which can be said to be very limited to only a few programming languages. The standard security implementation refers to the ISO standard of mitigation measures to ensure the safe usage of the program and its data, whereas the hardware constraints refer to the optimisation of the hardware used to host the actual program which requires fully fledged research and development.

### C. Rationale

According to the problems stated above, the facial recognition attendance system aims to improve class credibility and boost students' engagement in class to improve knowledge absorption among the students. The proposed solution hopes to improve the class's overall engagement as a random attendance record can be quickly initiated mid-class to make sure that no one is AFK (or away from keyboard) for long periods of time during sessions. An important aspect of learning is having enough attendance. For the majority, it is a no-brainer that low attendance usually correlates to the student not doing as well as they should or failing the class, hence why there is a minimum amount of class the student needs to attend. Therefore, with this proposed system, the goal is to ensure that students pay more attention to what is being displayed in class and to limit human error caused by manual tracking of attendance.

## II. Literature Review

Scientific breakthroughs and technological advancements of the recent decade have contributed to the current state of modern society. The increasing demand for better and more efficient technology has driven many industry specialists to keep innovating in their fields to meet the demands of the masses. The implementation of automated facial recognition attendance systems in education and businesses would help reduce attendance costs and time. In the presented setting, the high-accuracy face recognition algorithms that are currently available would make it harder for students to proxy their classmates onto the attendance lists. The main purpose of this study is to explore the correlation between attendance and overall performance among people in a select age category. The correlation would then be studied and reflected on in terms of how the usage of facial recognition may be able to improve overall attendance consistency and provide a substantial boost to performance in educational settings. Furthermore, this study will provide an overview of how well facial recognition systems are accepted among the populace of different backgrounds, which will allow for a better understanding of the value proposition that the system brings when implemented in educational settings.

### A. Domain Research

Recent applications of facial recognition can be found in airports and healthcare services. This was done to replace the commonly used finger biometric fingerprint scanners, which was the standard solution before the pandemic. Biometric fingerprint scanners have become almost obsolete in public services due to the invasive nature of the system that requires touching surfaces. Social distancing and COVID-19 measures made this point of identification obsolete, as constant sterilisation is needed, which would still be a liability and inefficient [5].

According to market research conducted by Markets and Markets [6] citing various bodies, the global forecast for facial recognition statistics is projected to grow from 3.2 billion USD in 2019 to 7.0 billion USD in 2024. Currently, the most common applications and usage of facial recognition can be found in the media and entertainment, BFSI (banking), and retail industries. The usage of facial recognition in education may fall short compared to more mature alternatives such as biometrics scanner. This is because the education sector adopts innovation at a slower rate compared to the other sectors due to the barriers to innovation in education being more apparent than elsewhere [7].

There is no denying that attendance plays a crucial role in a student's ability to learn [8]. In higher education, many institutions impose a rule where students must maintain a cumulative attendance of at least 80% to be eligible for exams. This is because low attendance and engagement often lead to poor overall performance, except for a few within a batch. Taking that into consideration, the current system in place for tracking attendance does not accommodate the transition from a traditional platform to a digital platform. To ensure that students stay in class for a minimum duration to help both attendance integrity and students' performance, two scans are carried out with an interval of 30 minutes for an hour class and one hour for a two-hour class.

This investigation report proposes an attendance marking system that uses facial recognition algorithms to improve the speed and integrity of the system. To extract features from an image or data, the proposed system employs the concept of histogram-oriented gradient (HOG) [9]. The facial recognition package incorporates machine learning with deep learning that allows for high face detection accuracy, which will be used in developing the "Face-Nest".

### B. Similar Systems

Among several other concepts that an attendance system is built around, QR-code web-based attendance systems may be the way to go, as they do not require any deep learning or complex algorithms to work [10]. The concept is well accepted among students and lecturers, while the learning curve is very low. Overall, it is simple in nature and gets the job done. Mass attendance taking can be painstakingly difficult if done manually, but with QR-based attendance, a code can be displayed, and students can scan the code.

On the other hand, the biometric fingerprint scanner has become the gold standard in the modern world. The technology can be found in all ranges of devices and applications, which makes it a versatile solution that can be integrated into almost any system [11]. A fingerprint scanner takes a fingerprint profile and stores it in a database. When a user scans their fingerprint, the system will match the print with an existing database and identify the user. Everyone is born with a unique fingerprint, so misidentification chances are almost nonexistent unless alteration has been done or the fingerprint could not be identified due to skin degradation.

To put it into perspective, when comparing the two, it is

hard to justify the use of facial recognition in some cases as fingerprint scanners are much more mature and are a low-cost solution to implement in many use case scenarios. Facial recognition, on the other hand, is reliant on input feed resolution to ensure that the correct identification is performed and, overall, is a more costly solution to implement in public places. However, the current times require a non-invasive solution both offline and during online sessions, which a fingerprint solution is not able to provide. The transmission of pathogens and harmful viruses through direct and indirect contact has made fingerprinting devices obsolete in public spaces [12].

### C. Research Gaps and Previous Studies

There are always problems associated with progress and innovation; in the end, it only comes down to who favours them and who is against them. Problems associated with facial recognition are no different; the question is, "must you give up user privacy in the name of efficiency and security?" [13]. Although uncommon, facial augmentation to impersonate a person can be done with the help of 3D technology and a custom silicone mask, which can be used to spoof a commercial facial recognition system [13].

That being said, there is not enough research being conducted on the rate at which a facial recognition algorithm identifies a fake silicone mask worn by an individual as the structure of the face could be very similar. In such an adverse environment and with a technology that has yet to reach maturity, there are still many unknowns that could potentially offset the benefits of the said technology. Furthermore, risk does not always stem from an external force; limitation may stem from the very concept of the technology, which do not always have a workable solution; for instance, facial recognition's ability to correctly identify a person degrades with identical twins in which among one of the solutions is to detect other facial features such as moles and scars. This solution, however, only works with two identical twins with scars and moles; the absence of such features will render the workaround useless [14].

Additionally, there are other known risks that one might want to consider before storing a face profile in a database somewhere with little to no oversight. Such risks include predatory marketing, which may be used to prey on selected groups of vulnerable customers based on facial expression; stalking, which can be carried out on a leaked face profile by conducting reverse image searches that may expose the victims to more data breaches; and lastly, identity fraud, which could significantly affect the victim's personal life, such as finance fraud and criminal charges.

To note, many of the previous studies [13] addresses the improvements made within the field of computer vision; however, very little study [12] is conducted on the potential benefits that facial recognition systems may have during the pandemic. Globally, the change in standard operating procedures has forced many students to adopt online learning. Even though the pandemic is still quite fresh, its effects can be seen across many sectors, from the economy to education. Although much of the previous research adds value by improving an existing algorithm or a combination of algorithms, it lacks the real-world aspect and application of the system. While this paper concerns and presents itself in a real-world scenario, it lacks an in-depth exploration of the field of computer vision and what enhancements can be made to further improve the performance of the system.

With the growth of the community and very little progress, many are debating the reliability and viability of facial recognition as a whole. Slow progress is being made in this technology, which is considered a contentious issue, with many concerned about what it could do to personal privacy and ways to regulate it. However, in recent decades, people have seen huge jumps in the detection rate and accuracy of facial recognition algorithms, which have brought more eyes to the subject.

Nonetheless, it does not change the fact that many are still skeptical about the potential that it may be misused or leaked into the wrong hands. This remains true even if the application is only implemented in educational settings such as universities or schools. Massive pools of facial profiles and personal data are a perfect target that could be used by cybercriminals to reverse search an image to obtain more information about their target, which could have a devastating impact on an individual if they fall victim to an attack. Additionally, companies can leverage this opportunity to buy data from hackers and tailor their ads and marketing strategies to those who are emotionally vulnerable.

Furthermore, there is very little solid grounds on which to base the findings on students' performance during the pandemic, as the sample size is huge, but the span is still fairly short, considering that the outbreak is fairly recent. Thus, only assumptions based on the operating conditions can be made.

## III. Methodology

System development methodology refers to the standards and framework that serve as the baseline criteria to ensure proper structure, planning, and control over the course of any system development. With that in mind, there are various methodologies that have been developed and refined throughout the years that suit certain project scales and applications. The aim of this section is to identify the preferred methodology to be used for system development and provide justification for choosing said method [15]. After thorough research and consideration, the methodology to be used for the development of the face recognition attendance system has been narrowed down to Waterfall. This is because the project's aims and goals have been clearly outlined beforehand, with little to no changes expected, as the project expectation has been clearly defined ahead of time, so the end user will know what is exactly going to be delivered [16].

The waterfall model adopts a linear or sequential approach to project development and asset management to be completed against a given timeframe with predefined end product quality, which suits the development of "Face-Nest". Throughout the system development life cycle (SDLC), cost is fixed, requirements are outlined, and time is well defined. The tasks that needed to be completed in each stage are well documented along with the materials, needs, and constraints that are expected to result from the development.

The waterfall methodology is designed to follow projects

that have clearly defined project requirements at the start of development. Face-nest has clear and defined goals that are expected from the end product. As there is a low risk of changing the features in this project, this makes the waterfall model a suitable methodology to use for the development as it follows a strict document as a guideline to aid development; this includes the possible constraints that may come along the way. The dataset used in this project is called "Faces in the wild Dataset", which is a database of face photographs purposely designed for machine learning in the fields of facial recognition. Fig. 1 below shows the stages of the research methodology.

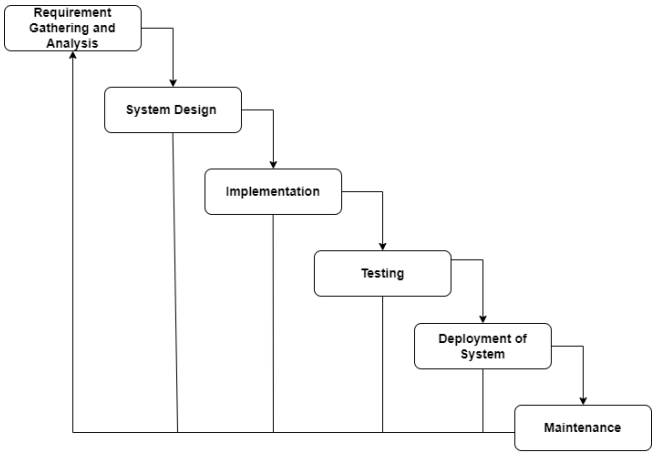


Fig. 1. Waterfall model flowchart.

**Phase 1: Requirements**. In this phase of the system development, a literature review is conducted as a preliminary research method to provide a reference guideline on how a similar system is built. Key functionality and features of the system are decided based on the data gathered from the literature review and the best practices that have been adopted from other attendance systems.

**Phase 2: Design**. The second phase includes designing the system schematics and how it works in detail. The descriptions of the technical requirements of Face-Nest are clearly defined in this phase. The features will be coded in separate files, while a modular coding approach is taken, where everything will be integrated together as the features are finished being developed. The feature and the backbone of the program will be developed separately to avoid confusion and will follow a priority order of development. This phase also includes the necessary charts to illustrate how the basic system works logically.

**Phase 3: Implementation**. In this phase of the SDLC (software development life cycle), the team building Face-Nest will set up the necessary environment to aid the development of the system. Some key functionalities will be developed first based on the priority of the development order. Constraints are addressed and appropriate workarounds from preliminary research are implemented by following the system flow and design with the help of the document compiled early in the development phase.

**Phase 4: Testing and deployment**. This phase of the development tests the system using various methods. Integration testing is particularly important as the units are coded separately. Integration testing allows the measurement of how well and how badly the two units work together, and some necessary changes may have to be made if the system speed is lacking or certain components do not work as intended. Upon completion of testing, the system will be deployed.

**Phase 5: Maintenance**. In this phase, as the system functionality and operation are fairly simple, the system could theoretically run for long periods of time without having any notable downtimes; however, the system may have performance issues encoding the faces in the database in real time as the library of faces grows, so it is important to have a capable CPU to handle such operations and ensure all the mechanisms protecting sensitive information is updated regularly.

## IV. Analysis and Findings

The demographic profiles of the respondents will be explained in this section. This will be useful in determining if certain religious practices or teachings may affect the acceptance of a facial recognition attendance system. To replace and encode facial features found in the target image, this facial recognition module employs HOG or histogram-oriented gradients by Adam Geitgey's technique. The encoded version of the image obtains the facial landmarks of the person, which can then be compared with a database of known individuals that has been prepared beforehand. The process is simple; the lower the variance, the higher the similarity between the two encoded faces. Therefore, this indicates that the two face profiles being compared are more likely to be the same person. Additionally, within the module is embedded another algorithm known as the face landmark estimation, invented by [17]. The concept works by marking 68 specific facial landmarks, which would then be rotated, scaled, and sheared to preserve parallel lines. This technique is called "affine transformation", which would allow the eyes to be centred even if the source feed is placed at a different angle. This mechanism would allow the feature positions to be approximated even if two different angles of the same image were to be compared.

The HOG+SVM (histogram-oriented gradients and support vector machine) module sports an accuracy of 99.38% in the labelled faces in the wild benchmark, which is a public benchmark for face verification, which is also known as pair matching. The accuracy for true positives of this algorithm is about as good as a human can be with identification.

### *A. System Overview*

The system user-interface (UI) is developed using the PyQT5 developer tools and Pyuic5. Upon launching the application, the user will be presented with the landing page shown in Fig. 2. This landing page serves as the gateway between the two login windows that take the user to either the student login page or the lecturer login page. The landing page also includes the logo of Face-Nest which can be found all throughout the application. Upon selecting which user class to log in as, the UI for the landing page will be hidden by default, as pre-set in the code.

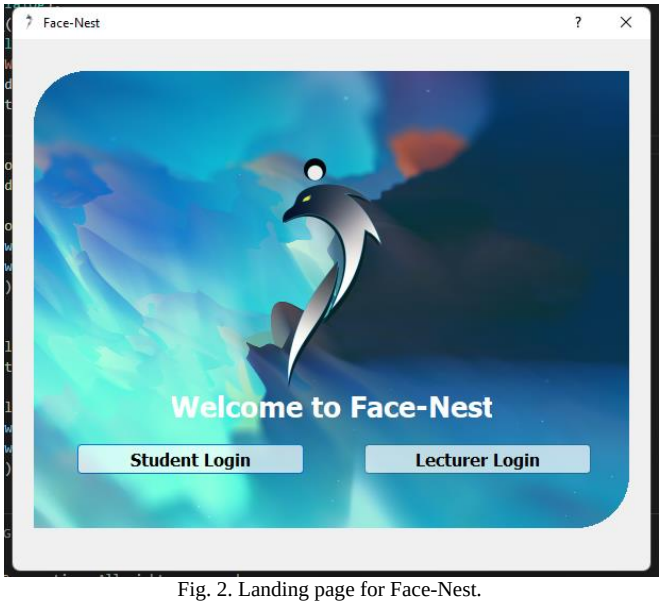


Fig. 2. Landing page for Face-Nest.

Fig. 3 shows the student login page for Face-Nest, where the student is required to input their credentials in order to gain access to the attendance application. Furthermore, to control access to the student page, the student login page incorporates strong password policy and credentials validation. A unique username and password are designated for each individual belonging to a user class.

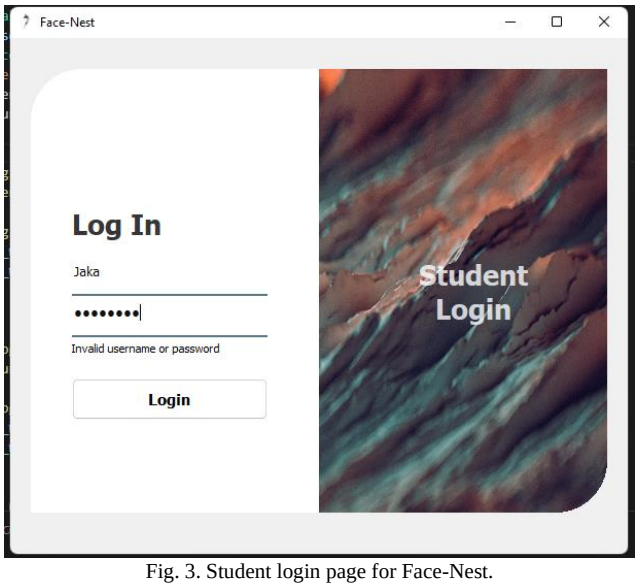


Fig. 3. Student login page for Face-Nest.

Similarly, in this section, the login mechanism incorporates the necessary validation and password policy in order to designate proper access to the defined user class.

As shown in Fig. 4, upon adding "Luthfi Jaka Satria" into the encoding list, the system is now able to detect the person in frame by comparing the encoding of the face in the folder with the live feed from the camera. Upon successful detection of the user in frame, a blue box with the word "verified" and the name of the image returned as a string from the folder is shown. The following screenshot shows the selection of classes that can be chosen and can be edited in the system depending on how many classes want to be added. The administrator has access to the source code, which enables the maintenance and editing of the classes. Once a class has been selected, upon clicking "enter", the selected class will be returned and displayed on the student details page next to the current class bar.

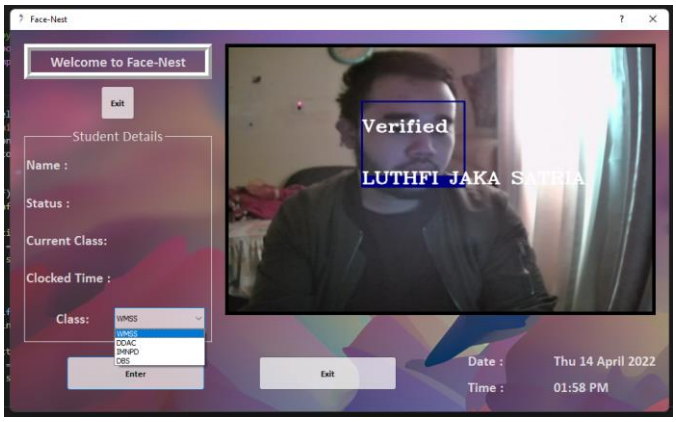


Fig. 4. Face classifier.

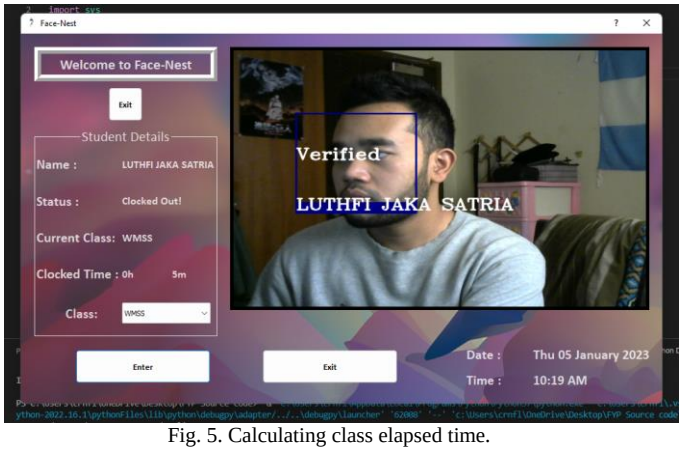


Fig. 5. Calculating class elapsed time.

Fig. 5 shows upon successfully clocking into the system, the name of the student is returned in the student details section, which records the current class the student is currently clocked into, their name, as well as the status of clocking in/out. This allows for easy cross-checking in the event the system detects a different person. Upon successful clocking in, the details of the clocked-in student are displayed on the window on the left. When prompting an exit from class, Face-Nest takes the name of the person in frame and returns it in a pop-up display to ensure the correct person is being clocked out, which corresponds to the student details currently displayed.

### *B. Demographic*

This section presents the demographics of the study. This study had a sample size of 50 people from various age categories, with the focus being on those between the ages 18 and 25. The questionnaire was distributed among people who are currently studying and those who graduated within the past five years. The purpose of the data is to gain insights from the respondents in various aspects of attendance systems currently being utilised. Although the data might not be entirely accurate, it was enough to provide an overview from the perspective of the selected age category.

Fig. 6 shows the demographic profile of the respondents. From the data, it is indicated that most of the respondents are males between the ages of 18 and 22 years old, which would make sense, considering the questionnaire was filled mostly by APU level 3 students with a small fraction coming from

people working in the service industry. The majority of respondents also practise Islam, with the remaining divided evenly between Buddhist, Christianity, and Hinduism. The data also indicates that the majority of the respondents are non-Malaysians, with a big fraction of the respondents currently attending university or having attained a degree. Considering the spread of the data indicating that the younger-adult generation took part in the survey, it is safe to assume that going forward, the data representation would point towards the adoption of facial recognition software as the younger generation is more accepting of new technology due to its lower technological boundaries and adaptability.

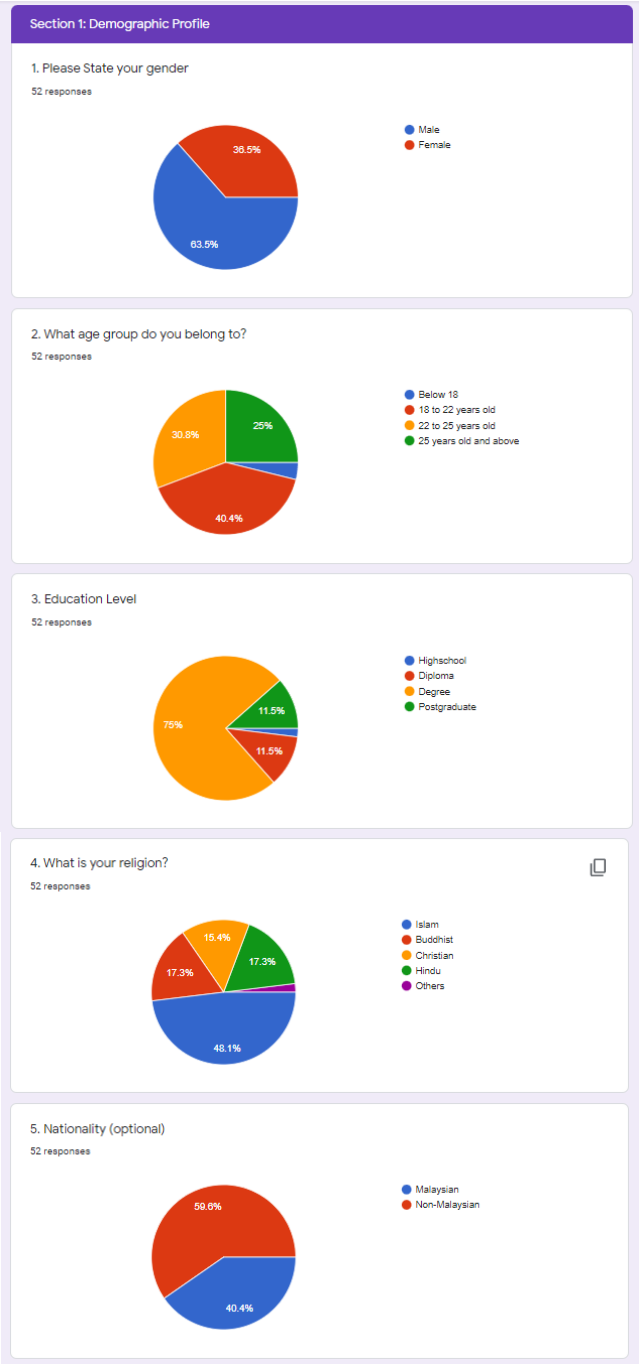


Fig. 6. Demographic profiles of respondents.

## C. Current Attendance Methods Used

According to the Fig. 7, when presented with a scale from 1 to 5 with from not accurate to highly accurate respectively, most respondents chose 4, which can be considered moderately accurate and accounts for 73.5% out of the 49 respondents. There are no ratings at 1 or 2 which means that the existing attendance system is satisfactory at the very least. Although they work, even if the surface is constantly sanitized, methods such as a fingerprint scanner, which was used by 15% of the respondents, may make them skeptical in using the system due to risk of COVID-19 contraction. Additionally, as 25% of the respondents still use roll calling as a method to take attendance, there is a high chance for error if the group were to scale up (increase the number of workers/students).

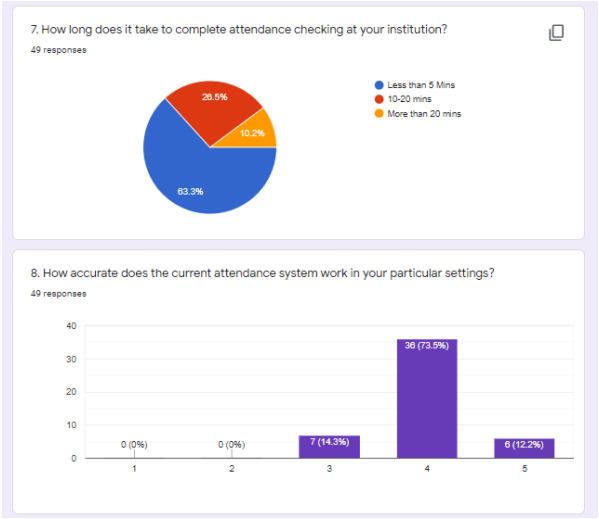


Fig. 7. Current methods used by respondents.

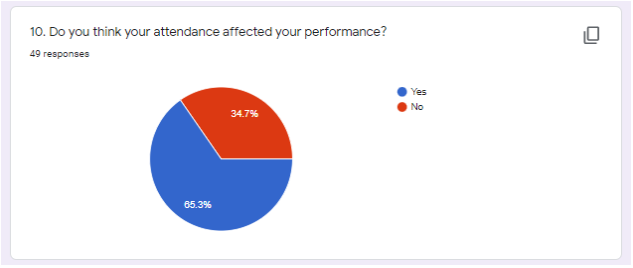


Fig. 8. Survey on the respondent's stance on whether attendance affected their performance.

Based on Fig. 8 above, the majority of the respondents' view attendance as a criterion that may affect their performance at work or school. Engagement may play a bigger role, but ultimately, it is the attendance that is being recorded, as there is no definitive way to measure engagement. Therefore, there is a direct correlation between attendance and engagement.

## D. View on Proposed System

Based on the data gathered from the three questions shown in Fig. 9, 87% of the respondents showed interest in using facial recognition software to mark their attendance. However, despite the high interest percentage, a considerable amount of those respondents still think that the risks outweigh the benefits, which could be due to the emergence of social engineering utilising deepfakes and predatory marketing. Only a few countries make use of facial recognition technologies; therefore, laws and regulations might be less refined in countries new to the technology. This may pose some risk to individual organisations employing

the technology, which may be up for abuse with little to no oversight from the government.

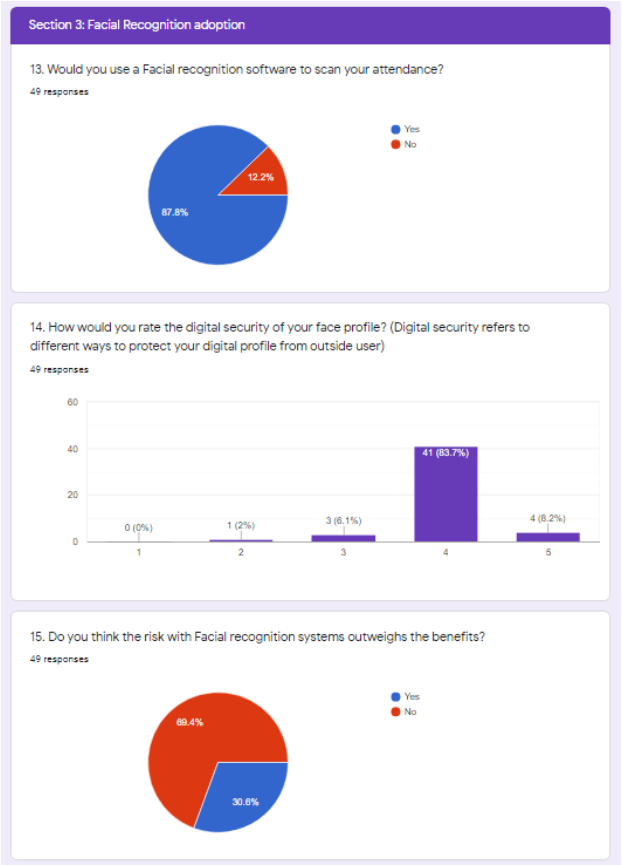


Fig. 9. Respondents' views on the proposed system.

Fig. 10 shows some of the common reasons why the respondents may think that the risks associated with using facial recognition software may outweigh the benefit. The introduction of deepfakes presents a great threat to those who have fallen victims to social engineering. The damage incurred when an impersonation of a victim happens can affect the personal and financial stability of the victim. Additionally, predatory marketing targeting those who present a particular facial expression or are emotionally vulnerable may have tailored sets of advertisements being sent over or displayed around their social platforms (outlining the fact that companies like Google and Facebook are constantly tracking their users' activities through their mobile devices).

According to the data gathered in Fig. 11 on whether facial recognition could be the solution in offline and online settings, the majority voted for agree, which means that despite the risks associated with facial recognition outlined in the previous question, many still view facial recognition as the future of identification in the mainstream market.

The high risk associated with the use of facial recognition software and what it could mean if the facial data fell into the wrong hands if mismanaged, many think there are adequate regulations and precautions in place to ensure the safekeeping of user data. This is because the risks are known, and it would better prepare system designers and data centers to design countermeasures to mitigate such attacks. On a scale from 1 to 5 rating the regulations in place to protect users against misuse of data, with 1 being worst and 5 being the best, majority voted with enough confidence in the protection of their data.


Fig. 10. Respondents' views on the risks associated with facial recognition.

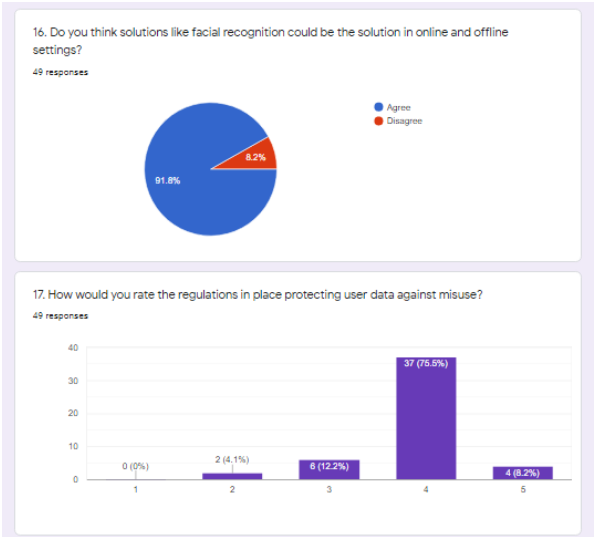


Fig. 11. Respondents' views on implementing face recognition system.

### E. Summary

The idea of a facial recognition attendance system with timestamp logs is widely accepted among the respondents. The proposed system could serve as a huge leap to roll-calling and biometric fingerprint scanners (in offline scenarios), which would provide both the accuracy and time efficiency many desperately need. Despite time being something, that QR-code-based attendance system is not lacking; it is highly vulnerable to proxying or attendance fraud. Based on the data gathered, despite the presumed risk associated with fingerprinting technology, the respondents would still choose to use the system, as the majority believed that with the right regulations and oversight, their facial data was well protected against malicious activities.

## V. Conclusion

The research and development conducted contributes to the natural progression of modern society as the digitalization rate continues to increase, the adoption of technology in education continues to progress, and eventually online learning will reach the mainstream audience with or without the pandemic. Education sector also no exception, which the

major challenges in education sector was face to face learning, which was not possible due to Covid-19 as the result. Many turned their sights straight to the internet where online learning platforms starts to emerge with various offerings due to the projected increase in demand in the service sector. The face-to-face learning quickly called off and digital alternatives was set up to replace the traditional means of learning. This process affected the attendance procedure, where the online class attendance system is heavily reliant on students marking their attendance using QR codes, it is susceptible to students asking their friends to send them the code or mark attendance for their friends. Therefore, students tend to neglect the importance of their attendance due to an online mode of study. With that the idea of the project is to limit the amount of attendance proxying through the current methods of attendance taking, ranging from QR code to roll call. Thus, this study aims to develop facial recognition attendance system that promotes convenience and accurate attendance marking, which contribute to a research direction for improving attendance in education setting by utilizing facial recognition attendance system.

## VI. Research Direction and Recommendation:

Several additions and recommendations from the user base can be considered to further improve the prospect and future proof Face-Nest. The accuracy of facial recognition algorithms has been increasing exponentially and is considered one of the more innovative solutions out there, but until a few years ago it would not have been possible to implement the technology in a real-life application as the baseline performance and face identification were not impressive. However, with today's algorithm, the accuracy of facial recognition algorithm can rival even some of the more high-end fingerprint scanners available in the market despite being an older and more refined technology out there.

Python's versatility and wide range of support from both the community and the developer were deemed suitable to be used for Face-Nest development. Lastly, the waterfall model was chosen as the system development methodology of choice, namely because of the low chance of changing the functional features of the system. That being said, it would be easier to compile a document that would provide adequate guidance throughout the development. This document discussed all aspects of development in order to provide as much as information as possible to aid development.

The importance of documentation is expressed throughout this investigation report as it provides guidelines for those who follow and outlines project constraints that may be crucial for future research. Ensuring that this document is written clearly and neatly is important to avoid confusion for readers as it may affect their understanding of certain concepts.

Further research can be conducted in the direction of the use of multiple cameras set up to execute an aspect of the program. For instance, the current system operates on a single webcam that processes both the facial detection and movement detection; should the processes be delegated to separate cameras working together, it would allow for faster processing, thus improving the overall latency of the detection.

Additionally, hardware development to accommodate the program opens up the possibility for deployment of a standalone system that would work in offline settings, which could be targeted towards smaller institutions looking for an affordable solution to minimise points of contact with the pandemic. Lastly, due to coding best practices and experience and the limitations of the developer, only minimal security measures are implemented. In terms of data privacy and data security, ensuring that security measures implemented adhere to industry best practices is critical to the system's long-term viability.

The future scope of this project is to conduct further research on hardware optimization and experiment with multiple setups to see how each affects the performance of the system. The current project is implemented with minimal hardware set up, resulting in overall low latency of the detection; however, accuracy is maintained.

## Conflict of Interest

The authors declare no conflict of interest.

## Author Contributions

Luthfi Jaka Satria conducted the research, run the development and data analysis, while Intan Farahana Kamsin and Nur Khairunnisha Zainal compile the analysis and wrote the paper. All authors had approved the final version.

## Acknowledgment

I would like to take this opportunity to thank my family, especially my late mother, who believed in me when no one did, not even myself. I would also like to thank my friends, who assisted me and provided me with much-needed support throughout the whole journey, which gave me the push to complete the project. I would also like to express my utmost appreciation to my supervisor, Dr. Intan Farahana Kamsin for her assistance and guidance throughout the entirety of the project. Credit to Asia Pacific University of Technology and Innovation (APU) for the opportunity given to publish the article.

## References

[1] A. Mehra, J. Paul, and R. P. S. Kauraz. (Feb. 3, 2022). Determinants of mobile apps adoption among young adults: Theoretical extension and analysis. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/13527266.2020.1725780?journalCode=rjmc20

[2] Smitha, P. S. Hedge, and Afshin, "Face recognition based attendance management system," *Internatinal Journal Of engineering Research & Technology (IJERT)*, vol. 9, no. 5, pp. 1190–1192, May 2020.

[3] H. E. Jackson and S. L. Schwarcz, *Protecting Financial Stability: Lessons from the Coronavirus Pandemic*, 2022.

[4] M. Hassan, "Online teaching challenges during COVID-19 pandemic," *International Journal of Information and Education Technology (IJERT)*, vol. 11, no. 1, pp. 41–46, January 2021.

[5] J. N. Rosenthal, D. J. Oberly, and A. H. Schrag, *Biometric Privacy in the Era of COVID-19: Facial Recognition Compliance for Airports and Airlines*, 2022.

[6] Marketsandmarkets Inc., *Facial Recognition Market*, Feb. 20, 2022.

[7] D. Morin, "Transition from face-to-face teaching to online teaching," *International Journal of Information and Education Technology (IJET)*, vol. 12, no. 3, pp. 246–251, March 2022.

[8] N. Li, J. Wang, and R. Sherwoord, "Investigation of face-to-face class attendance, virtual," *International Journal of Information and Education Technology (IJET)*, vol. 11, no. 3, pp. 112–118, March 2021.
[9] A. Singh, *Feature Engineering for Images: A Valuable Introduction to the HOG Feature Descript*or, Feb. 20, 2022.
[10] A. Talib, B. Ahmed, K. A. Al Saidi, and J. Rajasekaran, *Effect of Implementing 'QR Code Attendance System' during Examination in SHCT-Limits and Possibilities* Feb. 2022.
[11] M. Alhothaily, M. Alradaey, M. Oqbah, and A. M. El-Kustaban, *Fingerprint Attendance System for Educational Institutes*, Feb. 20, 2022.
[12] K. Okereafor, I. Ekong, I. O.Markson, and K. Enwere, *Fingerprint Biometric System Hygiene and the Risk of COVID-19 Transmission*, Feb. 20, 2022.
[13] R. Ramachandra *et al*., "Custom silicone Face Masks: Vulnerability of commercial face recognition systems & presentation attack detection," in *Proc. 2019 7th International Workshop on Biometrics and Forensics (IWBF)*, 2019, pp. 1–6, doi: 10.1109/IWBF.2019.8739236.
[14] S. Biswas, K. W. Bowyer, and P. J. Flynn, "A study of face recognition of identical twins by humans," presented at 2011 IEEE International Workshop on Information Forensics and Security, 2011, pp. 1-6, doi: 10.1109/WIFS.2011.6123126.
[15] K. Khan, *System Development Methodologies*, Feb. 20, 2022.
[16] A. Gallagher, J. Dunleavy, and P. Reeves, *The Waterfall Model: Advantages, Disadvantages, and When You Should Use It*, March 20, 2022.
[17] R. Valle, J. M. Buenaposada, A. Valdés, and L. Baumela, *Face Alignment Using a 3D Deeply-initialized Ensemble of Regression Trees*, March 20, 2022.

Copyright © 2023 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (CC BY 4.0).