INTI JOURNAL | eISSN:2600-7320
Vol.2022:26

# Virtual On-Premise Shopping System with Face Recognition Authentication

Yap Choi Sen[1*] and Cheng Chee Chen Dandy[2]

[1]Faculty of Data Science and Information Technology, INTI International University, Persiaran Perdana BBN, Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia

[*]**Emails:** choisen.yap@newinti.edu.my

## Abstract

This project aims to develop a modern, convenient, and secure virtual on-premise shopping system to promote efficient shopping with minimal waste. The system provides users with the ability to shop and pick up purchased items with minimal effort, which is particularly helpful for elders who are unable to carry heavy items for long periods. This system consists of an E-catalogue to enable product browsing, as well as a mobile app to enable the shopping process. With the proposed system, consumers are only required to sign up for an account to begin the process. After a top-up, consumers can simply start adding items to their virtual shopping cart by scanning any QR code on the E-catalogue. To ensure account and data security, consumers can simply opt-in face recognition upon signing up to enable two-factor authentication (2FA) to ensure that account security is not compromised. With the admin panel in place, the relevant staff will be able to easily modify item prices, and categories, manage stock and create purchase orders. Furthermore, the packaging department will be able to take advantage of the system to keep track of consumers' purchased items and notify consumers upon the completion of the packaging process.

## Keywords

Artificial Intelligence, Face Recognition, Virtual Shopping System

## Introduction

The advancement of leading-edge security and research has led to new challenges in cyber security, in which security experts and researchers are inevitably required to devise new algorithms or methodologies to improve data security. As cyber security plays an important role in securing payments, security infrastructures must always be up to date. In 2020, ESET - a renowned antivirus internet security company, discovered a backdoor known as *ModPipe* in Point-of-Sale (POS) systems which provides unauthorized access to user data (ESET, 2021). Furthermore, creative security exploits are constantly devised by malicious attackers. For instance, attackers have found ways to inject malicious commands into mobile phones when users scan QR codes found in public by replacing existing QR codes. In addition, the existence of credit and debit cards have provided another gateway for fraud through social engineering and other methodologies. In 2020, the US

**Submission**: 11 July 2022; **Acceptance:** 27 September 2022

Federal Trade Commission has reported that there are approximately 4.72 million credit card frauds with reported losses up to 3.3 billion USD, almost twofold compared to losses in 2019. As modern credit or debit cards support payWave using RFID, this allows attackers to perform various attacks, such as cloning attacks.

To address this security issue, the author proposes a virtual on-premise shopping system that integrates two-factor authentication by utilizing face recognition. Besides improving payment security, the author aims to make shopping a more efficient process by enabling users to add items to their shopping cart virtually. This also allows the merchant to reduce labor costs while promoting the LEAN methodology by adopting automation. As this system consists of a user interface to allow packaging departments to simplify the packaging process, this enables the packaging department to work together as a team and improve team chemistry; rather than requiring multiple cashiers who work at a different pace, not to mention being prone to burnouts.

## Methodology

As visualized in figure 1. The system consists of three major components - mobile application, admin panel, and E-catalogue. With the mobile application, customers can add items to their virtual shopping cart by simply scanning a QR code on the E-catalogue. As the E-catalogue may be located in the shopping mall, customers are only required to walk to the respective store for item pick up. In addition to this, the E-catalogue is updated real-time, hence only one of two different customers will be able to add an item with one unit remaining into their virtual cart. With enough credits in the customer's account, the user is only required to enter their PIN, along with an optional face recognition two-factor authentication to authenticate and process the payment. The packaging department will be notified upon payment, which allows relevant staff to initiate the packaging process. The staff can notify the customer regarding the packaging progress with the system. Upon completion, customers will be able to pick up purchased items at their respective locations. With this infrastructure in place, both consumers, business owners, and staff can benefit from the automation process. Moreover, this reduces physical contact for all parties, which contributes to a circuit breaker for the pandemic.

The author has implemented the system with careful consideration of essential user's requirement. To make the E-catalogue available to the public, relevant staff are required to utilize the admin panel to create and update relevant information for products and categories. In addition to this, the admin panel acts as a platform to provide stock and purchase order management, which further extends to produce a summary of important statistics through a dashboard.

Figure 2 shows a sequence diagram of the payment process. To start shopping, customers are required to install a mobile application and register for an account. For extra security, customers can optionally opt-in for two-factor authentication using face recognition. By scanning the QR code using the mobile application, customers can simply add products to the virtual shopping cart and checkout upon completion. The packaging department will receive the customer's shopping list after payment, thus allowing the staff to initiate the packaging process. During the packaging process, respective staff members can notify respective customers regarding the current packaging process by sending a push notification via a dedicated user interface that

will be utilized by the packaging department. The process ends upon the receipt of the final push notification regarding the completion of the packaging process, which prompts the customer to pick up the packed items by presenting the generated serial number to allow the respective staff to identify customers easily. Besides updating customers regarding the packaging process, it also allows customers and the relevant staff to resolve any potential confusion regarding the purchased items.

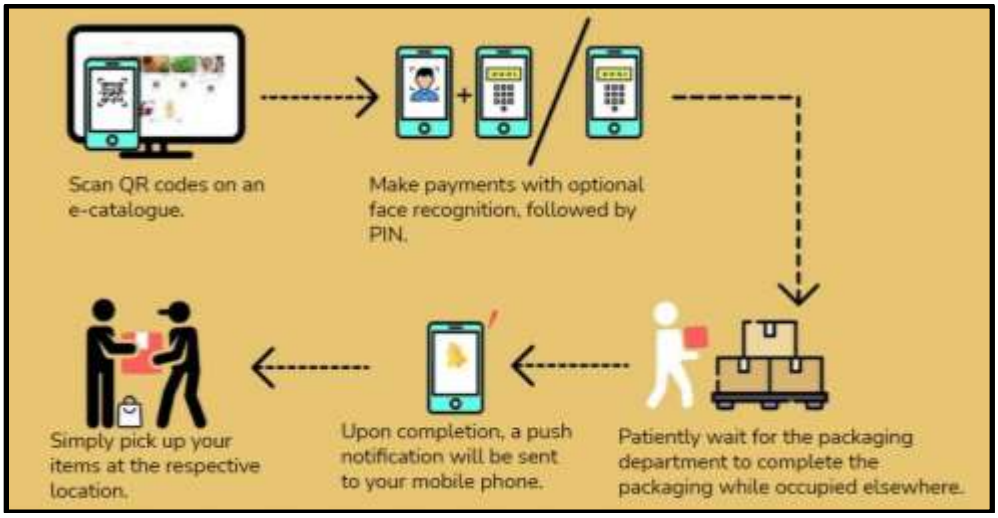


Figure 1. System process flow

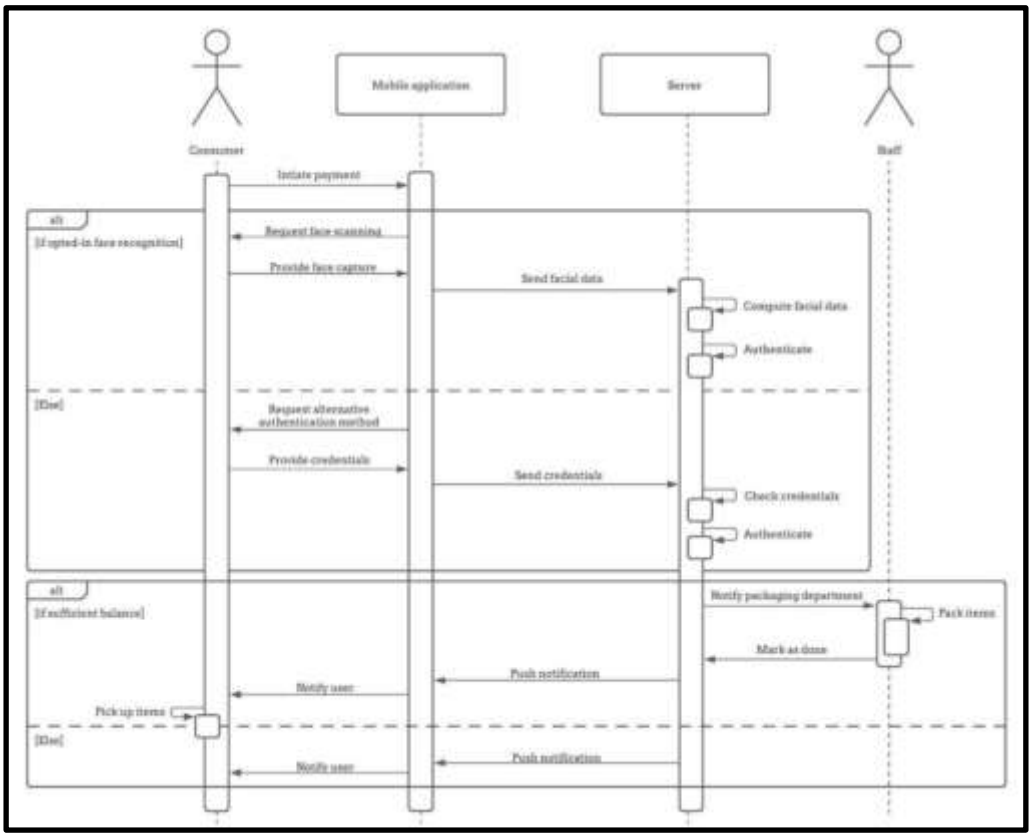


Figure 2. Sequence diagram of the payment process

The Siamese network architecture is used to train the face recognition model, which consists of two Convolutional Neural Networks (ConvNet) of the same architecture and parameters as seen in figure 3. This is used as an embedder, such that feature vectors (or embeddings) can be created to train a classifier in a later phase. To reduce the number of mathematical operations, the input image is reshaped into a smaller image with the shape of 220 by 220.

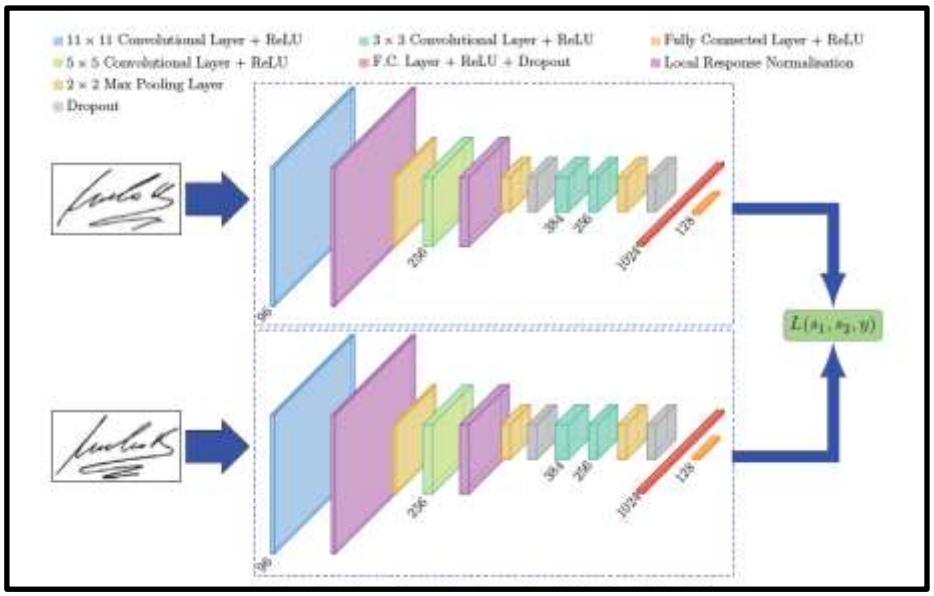


Figure 3. Siamese network SigNet architecture (Dey et al. 2017)

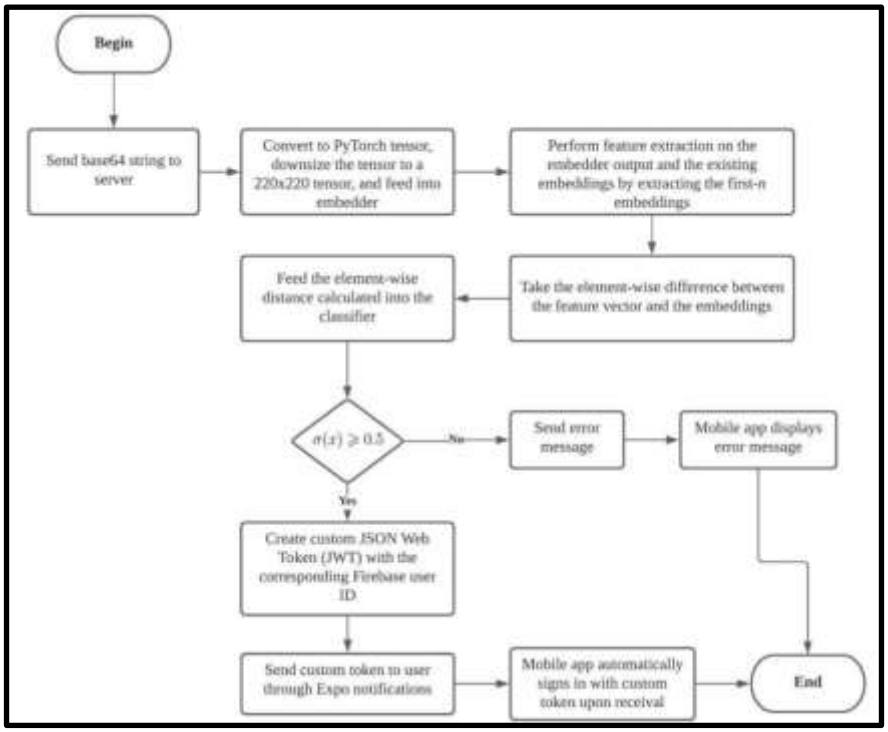


Figure 4. Face recognition authentication process flow

The process flow of facial recognition authentication is shown in figure 4. The facial image is captured from the mobile application during authentication processes such as login and payment verification, which is converted into a base64 string and uploaded to the server. The server will decode and convert the sent encoding into a PyTorch tensor with a shape of 220 by 220. This tensor is fed into the ConvNet, which produces a feature vector of 2048. The element-wise differences between the input image and the stored embeddings are calculated and fed into the classifier to determine the similarity between the two embeddings. The highest similarity is used to determine the identity of the user. A custom JSON Web Token (JWT) will be created and sent to the user's mobile application via Expo Notifications API if the similarity score is at least 0.5. Otherwise, an error message will be sent to the mobile application indicating authentication failure. The user will be notified upon successful or failed authentication. To further optimize the authentication process, the author has pre-computed the embeddings, which are stored in a CSV file.

Figure 5. Examples of the types of datasets used

The dataset comprises cropped faces with different identities, which also includes facial images with simulated masks to enable facial recognition despite the obstruction of a face mask (figure 5). This plays a significant importance in times when individuals are more concerned about personal health and safety due to an ongoing pandemic. In each iteration of the training phase, three facial images are used to create a sample - two images of the same identity (anchor and positive), and one contrasting identity (negative). This is fed into the Siamese network to decrease the euclidean distance between the anchor and positive image, and increase the distance between the anchor and negative image. Principal Component Analysis (PCA) is conducted on the output feature vector to perform dimensionality reduction to reduce the number of mathematical operations. In this implementation, the author has reduced the feature vector's size from 2048 to 55 with 99.99% of variance maintained.

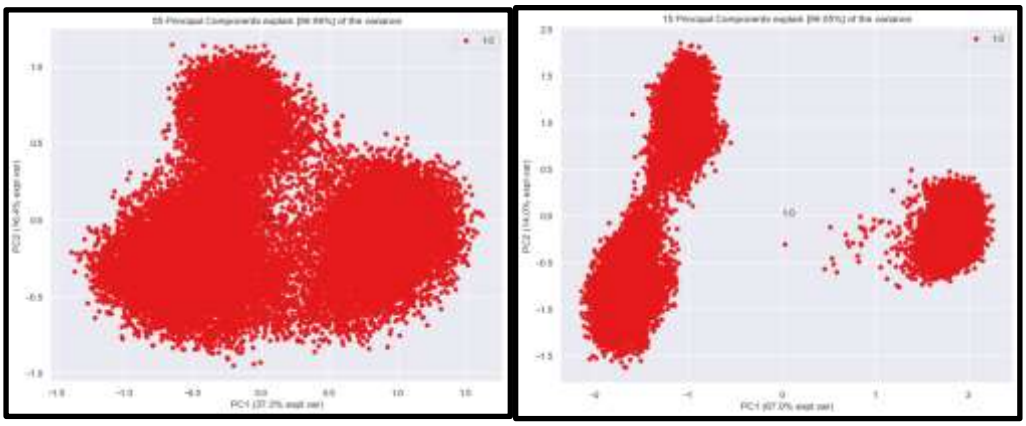

Figure 6. Clustering of principle components before (left) and after (right) batch hard triplet mining

As different facial images may look similar despite having different identities, batch hard triplet mining is utilized to mitigate this issue. Figure 6 shows the before and after the result of batch hard triplet mining, in which the negative image with the shortest Euclidean distance is selected such that it forces the neural network to push these images further away to allow better clustering. With this, the author can achieve significant improvements with smaller feature vectors.

## Results and Discussion

Figure 7 shows the classifier's performance before and after batch hard mining. Before batch hard triplet mining, the classifier had a training accuracy of 91.86%, and test accuracy of 92.2%. By reducing the batch size and implementing batch hard triplet mining, the accuracy of the model has increased its training accuracy to 92.16%, and test accuracy to 93.12% due to smaller gradient descent incremental steps, which increases the probability of converging into a better local or global minima.

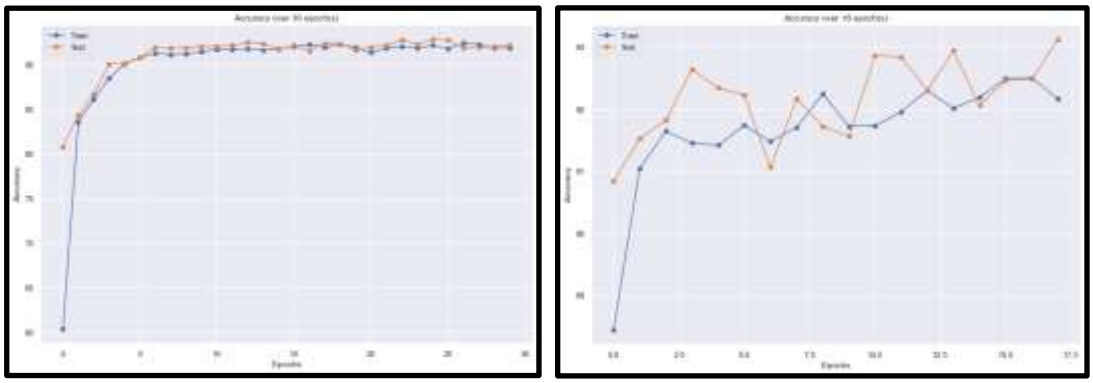

Figure 7. Classifier accuracy before (left) and after (right) batch hard triplet mining

Several images of different identities are used to compare with an anchor image. As seen in figure 8, the classifier is capable of recognizing the author despite obstructions of the existence of a face mask and face shield.


Figure 8. Similarity results produced by the classifier

Table 1. User evaluation results

| Attributes | Tester 1 | Tester 2 | Tester 3 | Mean Score |
|---|---|---|---|---|
| Intuitive (Admin panel) | 5 | 5 | 5 | 5 |
| Intuitive (Mobile app) | 4 | 4 | 5 | 4.33 |
| User friendliness | 4 | 4 | 5 | 4.33 |
| Security assurance | 5 | 4 | 5 | 4.67 |
| | | | **Total** | 18.33 / 20 |

User evaluation is conducted to ensure that users can understand and properly operate the system. Three different testers with different technical knowledge are requested to operate the system by providing a series of tasks and provide feedback based on a maximum scale of 5. As seen in table 1, three testers provided relatively high scores in terms of factors such as intuition, user-friendliness, and security assurance.

## Conclusion

Based on user feedback, it can be concluded that the system is capable of providing satisfactory usability, high efficiency, and security assurance while shopping. Besides improving the user experience for customers, stakeholders such as managers and employees benefit from the implementation of this system. As this system enables automated data collection and analysis using a dashboard, it allows managers to make data-driven decisions by identifying relevant correlations. Moreover, it promotes an eco-friendly shopping ecosystem as less resource wastage is required to maintain the integrity of the environment while achieving economies of scale by adopting automation.

**Acknowledgment**

This study is supported by to the Faculty of Data Science and Information Technology at INTI International University in Nilai, Malaysia.

**References**

Ali, M. A., Azad, M. A., Parreno Centeno, M., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems, 100*, 408–427. https://doi.org/10.1016/j.future.2019.05.012

Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N., & Arthi, S. (2020). Why is phishing still successful? *Computer Fraud & Security, 2020*(9), 15–19. https://doi.org/10.1016/S1361-3723(20)30092-0

Cho, J.-S., Jeong, Y.-S., & Park, S. O. (2015). Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. *Computers & Mathematics with Applications, 69*(1), 58–65. https://doi.org/10.1016/j.camwa.2014.10.015

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L. F., & Christin, N. (2018). "It's not actually that horrible": Exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)* (Paper No. 456). Association for Computing Machinery. https://doi.org/10.1145/3173574.3174030

Dey, S., Dutta, A., Toledo, J. I., Ghosh, S. K., Lladós, J., & Pal, U. (2017). SigNet: Convolutional Siamese network for writer-independent offline signature verification. *arXiv preprint*. https://arxiv.org/abs/1707.02131

ESET. (2021, June 3). *Threat report Q4 2020: ESET Threat Report T1 2021*. https://www.eset.com/int/about/newsroom/press-releases/research/eset-threat-report-q4-2020/

Federal Trade Commission. (2021, February 4). *New data shows FTC received 2.2 million fraud reports from consumers in 2020* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2021/02/new-data-shows-ftc-received-22-million-fraud-reports-consumers-2020

Iliyasu, A. M. (2019). Cellular-automated protocol to safeguard confidentiality of QR codes. *IEEE Access, 7*, 144451–144471. https://doi.org/10.1109/ACCESS.2019.2945224

Mugalu, B. W., Kiwumulo, E., & Angiro, D. (2021). Face recognition as a method of authentication in a web-based system. *International Journal of Computer Applications, 183*(19), 5–9. https://doi.org/10.5120/ijca2021921531

Wahsheh, H. A., & Luccio, F. L. (2020). Security and privacy of QR code applications: A comprehensive study, general guidelines and solutions. *Information, 11*(4), 217. https://doi.org/10.3390/info11040217