ISSN: 2773-7055
Proceedings of 3rd International Research Conference
Institute of Technology, University of Moratuwa
December 18, 2024

A MOBILE APPLICATION FOR ENHANCED ATM SECURITY AND EFFICIENCY: COMBINING HELMET DETECTION, FRAUD PREVENTION, AND REAL-TIME CASH MANAGEMENT

D.S. Kuruppu[1*], K. Galappaththi [2], G.M.C. Prabhashwara[3], M.G. Nayanajith[4], W.L. Gimhan[5], and N.S. Madanayaka[6]
[2, 3,4,5,6] Institute of Technology University of Moratuwa, Sri Lanka
[1]Sri Lanka Institute of Information Technology, Sri Lanka
dushanthi.k@sliit.lk[1*],kgalappaththi@itum.mrt.ac.lk[2],20it0491@itum.mrt.ac.lk[3],
20it0487@itum.mrt.ac.lk [4], 20it478@itum.mrt.ac.lk [5],20it0465@itum.mrt.ac.lk [6]

ABSTRACT: Automated Teller Machines (ATMs) are essential for financial transactions but often lack robust security measures, especially in developing nations. In Sri Lanka, it is illegal to access ATMs while wearing helmets as it hinders identification in case of robbery or fraud. Additionally, customers are required to notify their banks if an ATM runs out of cash before the scheduled refill. To address these two issues a mobile application was developed by leveraging the Internet of Things (IoT) and Machine Learning (ML). A suite of technologies including Python, OpenCV, PyTorch, Firebase, and Flutter were incorporated to develop the application. The mobile application employs image processing and ML to detect individuals wearing helmets, triggering alerts for both customers and bank officials. OpenCV, a Python library for computer vision, is used for image processing and face detection to identify unauthorized wearers and alert bank officials in real-time. This feature enhances security by discouraging fraudulent activities and ensuring proper identification of users from fraudsters. The ML model trained for helmet detection reached a higher accuracy level of 99.94%. For efficient cash level monitoring, an IoT system integrates Infrared sensors with Arduino and is programmed with C++ to monitor ATM cash levels, providing proactive notifications to bank authorities before cash runs out, and minimizing service disruptions. The research contributes to improving ATM security and operational efficiency by combining advanced technologies with a user-centric design.

Keywords: ATM security, efficient ATM, IoT, Machine Learning, real-time cash monitoring

1. INTRODUCTION

ATM robberies are occurring all around the world. Fig. 1 shows the growth of ATM robberies from the year 2005 to 2020. However, the 2020 and 2021 statistical analysis shows a sharp increase in crime incidents at ATMs. ATM crimes in America increased by 600% from 2019 to 2020. These numbers were likely significantly influenced by the 2020 pandemic (Pinkerton. n.d.).

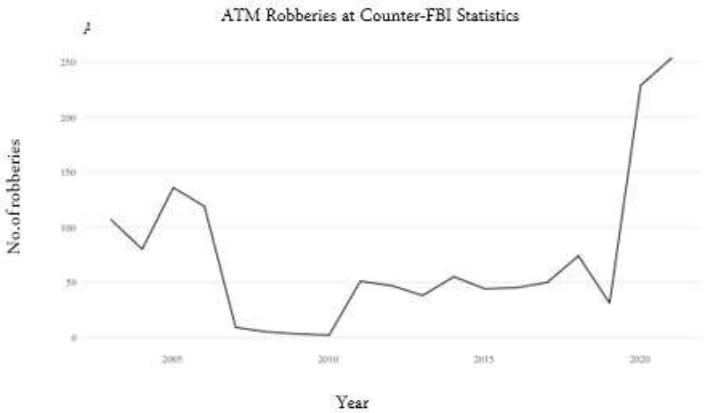

Fig. 1. Global ATM robberies

Although it is illegal to access Automated Teller Machines (ATMs) while wearing helmets in Sri Lanka, sometimes some users violate the rule as there is no specific person or procedure to monitor whether an ATM user is wearing a helmet or not. Even robbers and fraudsters can enter wearing helmets. Also, if an ATM is out of cash before the regular checkout from the bank, customers must inform the relevant bank, and then only bank officials visit the relevant ATM and refills. To address these two issues a mobile application was developed by leveraging a combination of sensors,

cameras, and Artificial intelligence (AI) algorithms to detect unauthorized wearers, monitor cash availability, and alert bank officials in real time. The system utilizes an IR sensor to track the thickness of the cash stack, and an ML model to identify unauthorized helmet wearers, by analysing the CCTV footage. Upon detecting unauthorized access, the system triggers an alarm, blocks transactions, and provides detailed information to bank officials via a mobile application. This proactive approach not only enhances security by deterring fraudulent activities but also improves operational efficiency by enabling timely replenishment of cash and minimizing downtime. By addressing these concerns, Mobile applications foster greater customer trust and ensure seamless ATM transactions.

Several approaches have been implemented to enhance security and efficiency in ATM functionality. This section similar studies are discussed on addressing vulnerabilities and improving ATM efficiency. Similar approaches are discussed under three sub-categories; “unauthorized access prevention”, “transaction security and efficiency”, and “accessibility and user experience”.

Smart ATM security system using False Positive Rate (FPR), Global System for Mobile Communication (GSM), and Global Positioning System (GPS) proposes a multi-layered security approach. It has been integrating Radio Frequency Identification (RFID) cards, Infrared (IR) sensors, GSM, and GPS technology. The system aims to detect tampering, track ATM locations in case of theft, and verify authorized bank personnel (Saranraj et al.,2020). The safety helmet detection for ATM’s surveillance system via the modified Hough transform utilizes DL techniques to identify individuals wearing helmets to hide their identity to prevent unauthorized access (Bharati et al.,2017). DL Helmets-Enhancing Security at ATMs investigates helmet detection using Convolutional Neural Network (CNN) suspicious behaviour within the ATM environment. (Jacintha et al.,2017)

An IoT-based ATM Surveillance System aims to identify theft attempts by sending alerts through social media platforms and dispensing chloroform to incapacitate potential intruders (Wen et al.,2003). ATM security system using Arduino proposes a solution which is a combination of fingerprint authentication and One-Time Password (OTP). (Jacintha et al, 2017). The design of the Embedded Based Dual Identification ATM Card Security System uses both fingerprint recognition and OTP generation. This replaces traditional ATM cards with secure biometric authentication, minimizing the risk. (Chumuang et al., 2020).

A money detector module has been developed based on Light Dependent Resistor (LDR) sensors to help blind people identify bank notes. This system uses voice output to communicate the detected value. (Devi at al.,2019)

2. METHODOLOGY

The proposed mobile application consists of two modules: “Unauthorized Wear Detection” module and the “Run-out-of-Money Detection” module. The “Unauthorized Wear Detection” module employs image processing technology to identify users wearing helmets before they initiate a transaction. If a helmet is detected, the ATM triggers a warning alert for both the customer and bank officials. The second module monitors cash levels within the ATM, notifying the bank when the cash before cash runs out, allowing for proactive replenishment.

Collaboration with bank officials was crucial for gathering requirements and detailed information about ATMs, transactions and the internal structure of the machines. The agile development methodology was followed during the mobile application development process. Figma was utilized for designing and prototyping the user interface, while the front-end user interfaces were built using the Flutter framework, providing a visually appealing and responsive experience across multiple devices. Google Colab was used as the development environment using libraries such as TensorFlow

and Keras to build and train the model. The “OpenCV” library was used for image pre-processing and face detection. An open data set was downloaded to create the training dataset.

In the first stage, data loading and pre-processing were conducted. It included image loading, resizing, and converting to arrays. Techniques such as rotation, zoom, shift, shear, and flip were applied to increase dataset diversity. For helmet detection, ResNet50 was used as the base model, with a custom head model added. The base layers were frozen, and only the head was trained. The model was trained using the Adam optimizer, with performance evaluated on a test set and visualized using Matplotlib. Face Detection was performed using OpenCV’s cv2.dnn module with a pre-trained SSD model to detect faces in images. The trained model predicts helmet usage, and results are displayed with bounding boxes and labels on images.

The development environment utilized Visual Studio Code as the IDE and Firebase for cloud-based services and data storage. Version control was managed through Git and GitHub. Furthermore, Arduino was integrated for basic Internet of Things (IoT) device that is ATM cassette development within the project. IoT components, powered by “C++” programming with an Arduino Uno board, acquire real-time data from an IR sharp distance sensor to monitor cash levels, transmitting data to the Firebase database via an ESP8266 Wi-Fi module. Firebase's real-time database capabilities ensured timely communication between the system and bank officials regarding alerts and notifications. The combination of these technologies has created a comprehensive mobile application that enhances ATM security, operational efficiency, and user experience.

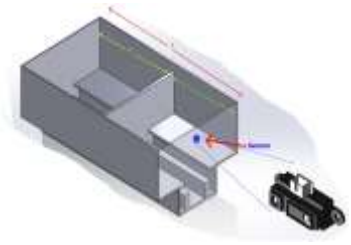

Fig. 2. Structure of the cash-cassette of the ATM designed to monitor cash level

Equation 1 was used to calculate the cash level in the ATM cassette. When the remaining cash level (d) reaches 30%, a notification is sent to the bank official to remind them to refill. This notification level can be customized according to the requirements of bank officials.

$$d = \left(\frac{b}{a}\right) 100\% \; ; \quad (b = a - c) \qquad \text{…….. Equation 1}$$

a=Total length of the cash cassette b= Length of the note bundle

c=IR Sharp distance sensor reading length d=% of the remaining currency note

Challenges encountered during implementation included high cost of physical components, the need for custom datasets for helmet detection, and the complex integration of diverse technologies. Despite these hurdles, the chosen technologies have facilitated the development of a robust system that enhances ATM security, operational efficiency, and user experience.

3. RESULTS

The training loss and accuracy of the ML model as the number of epochs increases are shown in Fig. 3. It is evident that the training loss decreases up to epoch 1.0 and remains constant while the validation loss (val_loss) remains constant without being affected by the number of epochs. Fig. 4 shows the output of the model identifying an image of a person wearing a helmet. The model achieved a high accuracy level of 99.94%.

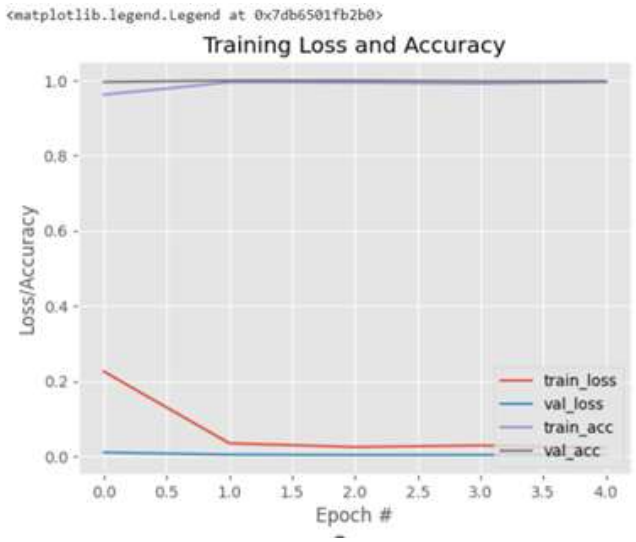

Fig. 3. Accuracy of the machine learning model for helmet detection

Fig. 4. Model identifies wearing helmet image with 99.94% rate of accuracy

4. CONCLUSIONS

The system developed in this study addresses security and efficiency concerns in ATM operations through a mobile application that leverages deep learning and image processing. The system detects unauthorized helmet and jacket wearers, triggering alerts for both customers and bank staff, while also providing real-time notifications about cash availability, ensuring proactive replenishment. Utilizing Python, OpenCV, PyTorch, Flutter, and Firebase, the solution aims to enhance security, improve operational efficiency, and promote customer satisfaction, ultimately fostering a seamless and secure ATM experience for all users.

To design an ATM system covering all problems in operation, this paper suggests implementing an alert system for bank officials when the receipt paper roll runs out and an ML model to detect ATM customers wearing jackets during the transaction.

5. REFERENCES

ATMs and crime. (n.d.). Pinkerton. Retrieved from https://pinkerton.com/our-insights/blog/atms-and-crime

Bharati, M. N., Reddy, N. V. U., & Awasti, N. (2017). SMART ATM security system using FPR. *Proceedings of the IEEE*, Coimbatore, India.

Chumuang, N., Hiranchan, S., Ketcham, M., Yimyam, W., Pramkeaw, P., & Tangwannawit, S. (2020, November 1). Developed credit card fraud detection alert systems via notification of LINE application. *2020 International Conference on Information Science and Artificial Intelligence (ISAI-NLP)*, IEEE Xplore. https://doi.org/10.1109/iSAI-NLP51646.2020.9376829

Devi, K. B., Room, S. M. M., Meena, M., & Meghana, S. (2019). Deep learn helmets enhancing security at ATMs. *Proceedings of the IEEE*, Coimbatore, India.

Jacintha, V., Nagarajan, J., Yogesh, K. T., Tamilarasu, S., & Yuvaraj, S. (2017). An IoT-based ATM surveillance system. *Proceedings of the IEEE*, Coimbatore, India.

Nurfadilah, H. I., Fatmawati, N. N., One, R. D., Pambudi, O. I., Oktafaina, D. D. R., Adiati, R. F., & Irawati, N. (2019). Money detector based on LDR sensor. *Proceedings of SPIE*, Surabaya, Indonesia.

Wen, C.-Y., Chiu, S.-H., Liaw, J.-J., & Lu, C.-P. (2003). The safety helmet detection for ATM's surveillance. *Proceedings of the IEEE*, Taipei, Taiwan.