Home Intruder Detection System using Machine Learning and IoT

Fadhluddin Sahlan, Faeez Zimam Feizal, Hafizah Mansor
Department of Computer Science, Kulliyyah of Information and Communication Technology
International Islamic University Malaysia, Selangor, Malaysia
fadhluddinsahlan@gmail.com

Abstract— Home surveillance requires human effort, time and cost. Many tragedies such as robbery and vandalism occurred at home while the owners were negligent or not at home. Some residential areas hire guards to monitor their homes but hiring workers is not considered a cost-efficient option. Home Intruder Detection System (HIDES) is an Internet of Things (IoT) system with a mobile application to help homeowners in house surveillance by alerting users for any potential threats remotely. The main objectives of HIDES are to create a reliable home security system with the implementation of IoT, to implement the object detection algorithm to determine the presence of humans, and to develop a smart mobile application for users to monitor their houses from anywhere in the world and be alerted if any threats are detected. HIDES is developed using the System Development Life Cycle (SDLC) approach. HIDES implements an object detection algorithm; Single-Shot Multibox Detection (SSD) in NVIDIA Jetson Nano to detect intruders through a camera connected to the system. HIDES successfully achieves its objective in detecting persons precisely and alerting the detection to users through mobile application remotely. The system can capture video at an average of 20 frames per second (FPS) while detecting intruders and sending detection video to the server. The mobile application achieves good performance where the loading time takes 2.3 seconds while only requiring about 0.99MB of memory to run and 66.87MB of space.

Keywords— home surveillance, object detection, IoT, SSD, mobile application.

I. INTRODUCTION

Many home tragedies such as robbery and vandalism occurred at home while the owners were unaware, negligent, or not at home. Some residential areas hire guards to monitor their homes but hiring workers is not considered a cost-efficient option.

With the use of Internet of Things (IoT), home intrusion detection systems are available where sensors such as cameras are used to detect the presence of intruders. However, without real-live data, these systems may deem less useful. The live data would be able to give alert to homeowners at the time the intrusion happens, instead of just having recorded video of the occurred events.

II. RELATED WORK

There are several systems available in the market that are similar to this project. Smart home security system developed by ADT Security provides multiple house monitoring plans such as live video monitoring and home automation that are integrated with the mobile application [4]. The strength of the product is the implementation of Internet of Things (IoT) and a mobile application that allows users to monitor their house wherever they are. The weakness of the system is the plans offered are quite expensive and there is no implementation of smart human detection or anomaly detection in their system.

Another similar system from GTC is a Malaysia-based security system that offers great deals on security solutions [5]. The system consists of devices such as alarms, security cameras and recorders. The system is good at capturing video but there is no implementation of intruder detection, and mobile applications that allow users to monitor their house remotely.

Research and development work on home surveillance systems is a recent in-demand area. In 2019, a group of researchers developed a system to capture video and send it to the server and identify the person in the video by their faces [1]. They use Raspberry PI to capture the video and send it to the server over the internet and the server will process the video frame-by-frame to detect the face in the frame by using OpenCV in Python. The project is quite simple and cost-effective. However, the frame rate transferred from Raspberry PI is very low and identifying a person that moves in a quick manner might be hard.

In 2019, another group of researchers also conducted a study on detecting intrusion and threats by using Convolutional Neural Network (CNN) and computer vision [2]. The main objective of the research is to recognise intrusions and detail down the threat's information. The

research uses a 3-stage Smart Intruder Detection and Surveillance System (SIDSS). The first layer is threat and intrusion detections using optimised CNN. Then, it uses cascading classifiers to refine and correct the undetected threats in the previous stage. Finally, the system uses Principal Component Analysis (PCA) to efficiently train the facial recogniser and further refine the result of the previous two stages. The algorithm proposed in this paper is thorough, but there is no implementation of IoT and mobile applications.

Other than that, a research work on Smart Home systems using Global System for Mobile communication (GSM) technology was implemented using IoT [3]. It uses Arduino Uno (acting as a mini-computer), ESP266 Wifi Module (to send data to the internet), and Reed Sensor (to detect opened doors). Despite it being easy to develop and the devices used are cheap, the Reed Sensor has the downside of being too slow due to its mechanical build, thus not suitable for applications that need high-speed detection [8].

Papers / Existing Systems	Human / anomaly detection	Good video quality	Mobile app integration	Notify users on detection	Save detection video	Quick emergency call
Rambabu, Haritha, Srinivas and Reddy (2019)	✓	✗	✗	✗	✗	✗
Zhang, Yi and Sanlie (2019)	✓	✓	✗	✗	✗	✗
Anitha (2017)	✓	✗	✓	✗	✗	✗
CTC Security Camera	✗	✓	✗	✗	✗	✗
ADT Automated Security	✗	✓	✓	✗	✗	✓
HIDES	✓	✓	✓	✓	✓	✓

Fig. 1 Existing Systems Comparison

III. METHODOLOGY

A. *Design*

From the literature review, we designed the Home Intruder Detection System (HIDES) system. HIDES architecture consists of a detection system using machine learning and a mobile application. The role of the detection system is to capture live videos, and the captured frames will later be processed by the NVIDIA Jetson Nano to detect any intrusions. Any intrusions detected will be updated to the server, in which later the information will be retrieved by the mobile application to be displayed to users. The whole architecture of HIDES is portrayed in Figure 2.

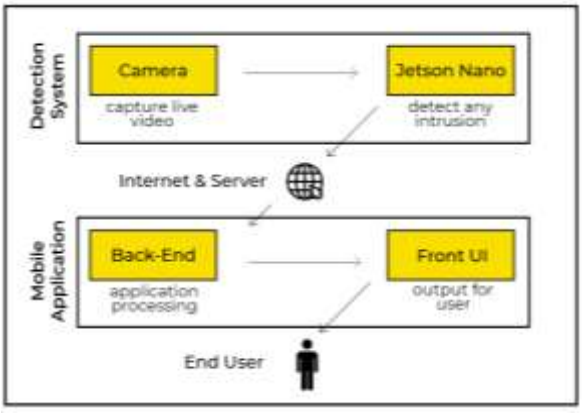

Fig. 2 HIDES Architecture

The HIDES mobile application is designed minimalistic in terms of design and code structure. The minimalist User Interface (UI) design gives a fresh and easy look to the user to navigate through the app. The UI is designed based on Human-Computer Interaction (HCI) studies to produce a product that is accessible and convenient to use by any human despite complications such as colour blindness, low-level vision and dyslexia. Furthermore, the User Experience (UX) design also is structured thoroughly using diagrams such as Use-Case Diagram and Flowchart Diagram to make sure no unintended event will happen when using the app. Relatively to the minimalist UI and UX design, a neat code structure also is considered when developing the app. This is useful in the production and testing phase where bugs or faulty can easily be noticed and fixed.

Since HIDES is a security system, security aspects of the system need to be measured and contingency plans need to be taken in case any threats occur. For that, threat modelling is performed to identify threats that might occur in the system and their countermeasures. The threat modelling diagrams for the HIDES system are illustrated in Figure 3 and Figure 4.

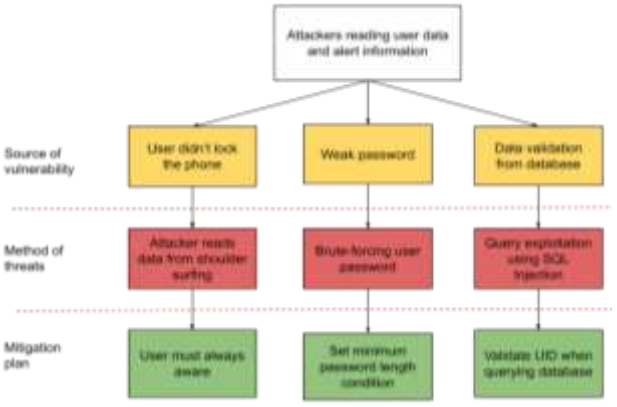

Fig. 3 Threat Case for HIDES Mobile App

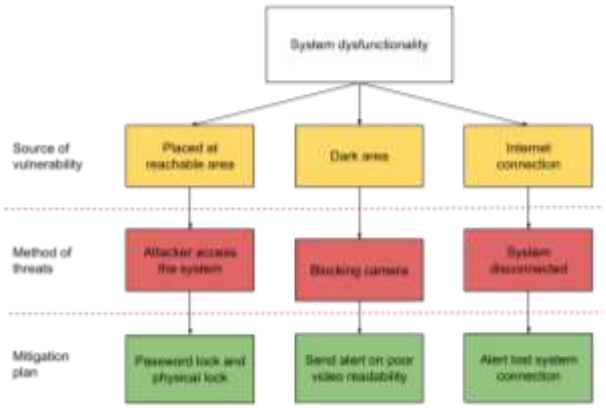

Fig. 4 Threat Case for HIDES Detection System

The focus of threat possibility for HIDES mobile application is the security of unapproved people to read user data and intrusion alerts as in Figure 3. First and foremost, the carelessness of the user by leaving his/her phone left open is dangerous as social engineering threats such as shoulder surfing could happen easily. Furthermore, the choice of weak passwords by users can threaten the security of users' accounts as the attacker can easily guess or brute-force the password to log in. Hence, we provide a minimum password length restriction upon sign-up and password reset page because a long password will provide better security. Other than that, database validation could be a threat as methods like SQL injection can be used by the attackers to get high-threat data such as other users' data. Hence, we write a rule using the Firebase Security Rules where User ID (UID) will be validated before querying any data so only data owned by a user can be accessed. The most critical vulnerability of the application should be the failed authorisation when navigating through the application. Some pages that are meant for private users (paid users) only should not be accessed by public users who signed up through the app. To mitigate this vulnerability, we use Fire Angular Guard where the route of pages will be guarded based on user role access and any disallowed role will be redirected to another page. Data spoofing is crucial too as any text or data sent over the internet to the database has the potential of being spoofed by a man-in-the-middle attack. An encrypted Hypertext Transfer Protocol Secure (HTTPS) connection over Secure Sockets Layer (SSL) is the best option to use to counter this vulnerability.

The HIDES detection system also is not free from any threat vulnerability as in Figure 4. Firstly, placing the system or mini-computer in an open reachable area is harmful as people can easily access or break the system. We should avoid this by hiding the system and locking it physically using a bracket lock. Secondly, the camera limitation such as low-lighting and blocked lens is risky as the system could not process any human detection. An alert will be sent to the user if the camera detects any poor video readability. Then, loss of connection to the internet is a crucial threat to the system as HIDES is an IoT product hence requires a functioning and good internet connection to operate at the fullest. Disconnected systems from the internet will result in failure to send alert and intruder video to the user. As the solution, HIDES will always monitor the internet connection and will alert the user if any loss of connection is detected. Other than that, the power source is really important and the loss of electricity is the biggest threat as the system could not operate at all. Having a backup power source such as a power bank will help in avoiding this environmental threat. Last but not least, the threat of data spoofing when uploading alerts or videos to the internet will always be a concern for the users. Using an HTTP(S) connection along with the security check by the Cloud Firebase will ensure the security of transferring data to the database.

B. Implementation

System Development Life Cycle (SDLC) approach was used in building the system. The cycle includes the planning and analysis phase, design phase, prototyping and testing phase, and implementation phase in which the detailed steps for all the phases are illustrated in Figure 5.

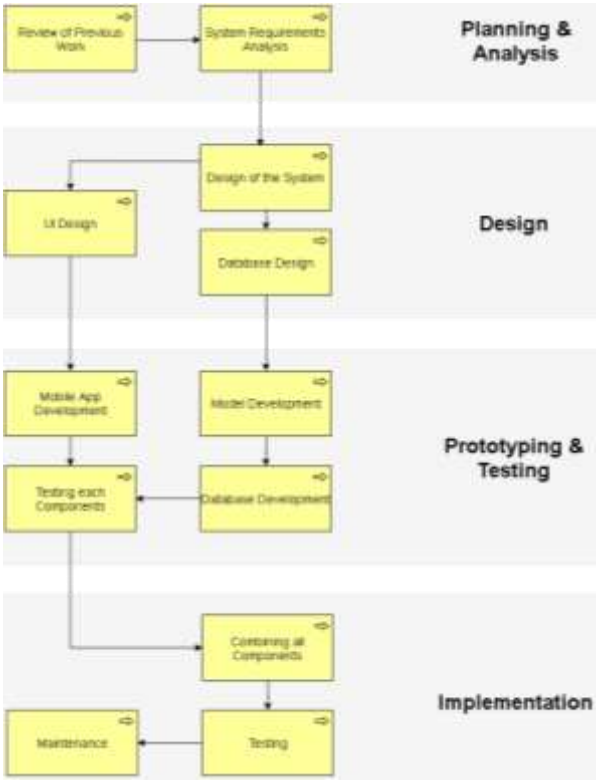

Fig. 5 SDLC Approach

The detection system consistd of several hardware which are the NVIDIA Jetson Nano, WiFi Module and IMX219

Camera. The camera is connected to Jetson Nano through Camera Serial Interface on Jetson Nano's board while the WiFi Module with M.2 key is connected to Jetson Nano through the Peripheral Component Interconnect Express (PCIe) port on the board. Jetson Nano powered using 5V 4A DC power adapter to maximise the power usage of the mini-computer. The model used to perform object detection is a pretrained model (Single-Shot Multibox Detection (SSD)) available online in Github and it appears to achieve good accuracy in detecting person with different light settings. SSD Mobilenet V2 is used to train the detection model [9]. The system is capable of detecting persons and the detection videos are saved to the cloud storage and the metadata of the videos are updated to the database to be retrieved by the mobile application.

Meanwhile, the mobile application was built by using the Ionic Framework (AngularJS) that offers robust cross-platform app development like Progressive Web App (PWA), Android and iOS. Hence, HIDES is always ready for users from any platform. Ionic also is proven to have the best web performance compared to other SDKs such as Flutter and React Native [7]. For the app interface (front-end), basic web development languages such as HTML, CSS and Javascript are used as these elements are easy to maintain and can be optimised to reduce app size. Furthermore, the UI was brushed with Tailwind CSS for an immersive clean and modern look that keeps up with the current market trend. Ionic Capacitor is chosen as the app runtime and the integration of Ionic with AngularJS has eased the hassle of writing the back end. In addition, an optimised version of the code was built at the production phase where the code is compressed to improve the app performance. In Table 1, we can see that the optimised version offers a smaller app size, compared to a normal build. The performance is increased as the app becomes more lightweight, and the time taken to load content is shorter.

TABLE I

HIDES CODE BUILD

Type of Build	Size of Build (MB)	Time Taken to Load (seconds)
Normal	11.42	2.56
Minified	5.02	2.30

C. *Evaluation*

The HIDES can capture live frames while detecting people in the frames, saving the frames, and uploading the saved videos and their metadata on cloud storage and database. These processes are successfully executed at an average performance of 20 Frames Per Second (FPS).

Furthermore, the mobile application (Android) can be executed even in old devices with Android 8.0. Videos can be played quickly since the videos are loaded directly from the database using HTTP(S) link and web player. Authorities also can be called immediately as there is always a button for that when an intruder is detected.

IV. DISCUSSION

From the previous evaluation section, the system is capable of executing all the main features at an average of 20 FPS in Jetson Nano using SSD Mobilenet V2 object detection algorithm. However, it appears that there are some competitions in terms of the hardware and the algorithm that were used.

Other than using Jetson Nano for the detection system, Raspberry PI is also capable of replacing Jetson Nano to run the detection. A test was done to run object detection inference in the Raspberry PI environment and the system can run object detection but at only 1 FPS excluding video saving and uploading which this performance was 20 times lower than Jetson Nano. Lower FPS will result in low frames caught which could be a threat to a security system in capturing clear faces of people. This comparison is illustrated in Figure 6 below.

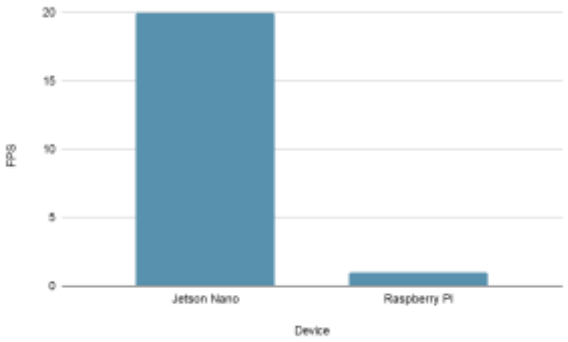

Fig. 6 Jetson Nano vs Raspberry PI

Besides, the SSD object detection algorithm can be replaced with the You Only Look Once (YOLO) algorithm. However, in Jetson Nano environment, it appeared that YOLO could perform inference in Jetson Nano environment but only achieve an average of 10 FPS without performing video saving and uploading which is lower than what SSD achieved. In addition, it appeared that the YOLO algorithm was quite less sensitive in detecting people. This might be because performing YOLO inference is not compatible in CUDA GPU as compared to SSD inference. This comparison is illustrated in Figure 7 below.

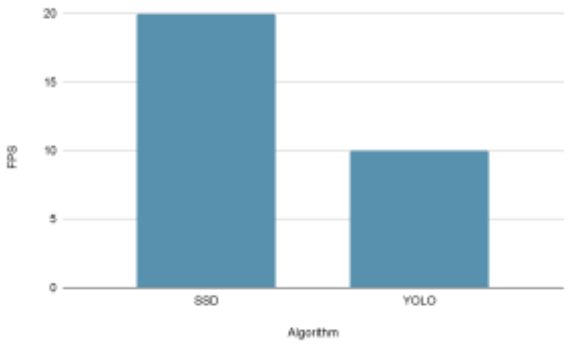

Fig. 7 SSD vs YOLO

An Android app comparison was tested between HIDES and other security solution apps in the market such as ADT Interactive and MI Home. The comparisons were conducted using the built-in Android App Manager by running the login page and homepage only since ADT and MI Home require buying their actual product to explore more. In Table 2, HIDES has the lowest app size which means it's more lightweight compared to the others. The system memory usage also is not large as ADT Interactive considering the comparison test does not involve any heavy workload. However, the ADT and MI Home offer other features as well in their apps such as a smart home and a smart lock that might be the reason the apps' sizes are big. In HIDES App, the only processing needed is fetching and loading data from the database. This is because human detection, video processing and capture are performed by the HIDES Detection System. Hence, the app does not require intense mobile phone processing power, resulting in low memory usage and battery-saving.

TABLE II

APP COMPARISON

App Name	App Size (MB)	Memory Usage (MB)
ADT Interactive	158.00	6.00
MI Home	214.00	0.44
HIDES	66.87	0.99

V. CONCLUSIONS

In conclusion, it is proven that HIDES has the potential to be the best home security solution in the market, as proper and neat preparation such as researching existing solutions, planning system flow, sketching system architecture, using SDLC approach and evaluating a threat modelling are performed before developing the system. All the IoT technology, framework and algorithm are chosen properly to create a perfect system.

Based on a detailed experiment, SSD is the best object detection algorithm to use as it can steadily maintain a 20 FPS video while running object detection and capturing video. Similarly, Ionic Framework is, without doubt, the most suitable app SDK to produce a lightweight app that loads within 2.3 seconds, and only uses 0.99MB memory and 66.87MB space. Due to that, HIDES is always ready for the current market trend and welcomes users from any background and condition. In the future, HIDES aims to offer more amazing features that could help homeowners secure their houses safely such as face detection and live feed detection.

REFERENCES

[1] Rambabu, K., Haritha, V., Srinivas, S. N., & Reddy, P. S. (2019). IoT-based human intrusion detection system using lab view. International Journal of Advanced Science and Technology 127, (1), 162-166.

[2] Zhang, X., Yi, W. J., & Saniie, J. (2019, May). Home surveillance system using computer vision and convolutional neural network. In 2019 IEEE International Conference on Electro Information Technology (EIT) (pp. 266-270). IEEE.

[3] Anitha, A. (2017). Home security system using Internet of Things. IOP Conference Series: Materials Science and Engineering, 263, 042026. https://doi.org/10.1088/1757-899x/263/4/042026

[4] Home Security System: 24/7 Alarm System Monitoring: ADT Security. ADT Services Malaysia. (n.d.). https://www.adt.my/smart-home-security/.

[5] Product – GTC. (2021). Retrieved 20 June 2021, from http://www.gtc.my/product/

[6] Ananthan, R. (2019). Crime Trends and Patterns in Malaysia | Kyoto Review of Southeast Asia. Retrieved 20 June 2021, from https://kyotoreview.org/trendsetters/crime-trends-and-patterns-in-malaysia

[7] Netkow, M. (2021). Ionic vs Flutter: Best Platform for Hybrid App Development. Ionic Forum. https://ionic.io/resources/articles/ionic-vs-flutter-comparison-guide

[8] Moermond, J. (2017, February 1). The Pros and Cons of End-of-Stroke Detection with Reed Switches. AUTOMATION INSIGHTS. https://automation-insights.blog/2010/05/24/the-pros-and-cons-of-end-of-stroke-detection-with-reed-switches/

[9] Franklin, D. (2022). Locating Objects in DetectNet. https://github.com/dusty-nv/jetson-inference/blob/master/docs/detectnet-console-2.md#pre-trained-detection-models-available