

SISTEM KUNCI PINTU PENGECEMAN WAJAH MENGGUNAKAN RASPBERRY PI

Nuur Izzah Binti Munizar
Mohd Zamri Murah

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Setiap fungsi utama sistem automasi rumah adalah untuk mengesan orang yang masuk atau meninggalkan rumah. Daripada perlu mengingati kata laluan atau pin anda, wajah unik boleh digunakan kerana ia adalah ciri biometrik seseorang. Ini adalah semulajadi dan tidak boleh diubah atau dicuri. Tahap keselamatan boleh ditingkatkan dengan penggunaan pengesanan wajah. Sistem keselamatan kunci pintu pengecaman wajah yang dicadangkan, direka untuk mencegah rompakan di tempat yang selamat seperti di rumah yang mempunyai penggunaan tenaga yang lebih rendah dan sistem keselamatan sendiri yang cekap untuk pengesanan gangguan dan akses pintu. Sistem ini dibentuk oleh litar pi raspberi. Apabila seseorang itu berada di hadapan pintu, ia akan mengiktiraf muka berdaftar dan membuka pintu tetapi jika muka tidak didaftarkan, penggera akan berdering selama kira-kira 30 saat. Ini adalah cara sistem berfungsi.

1 PENGENALAN

Pada era globalisasi ini, teknologi telah menjadi bahagian yang sangat diperlukan dalam kehidupan manusia. Memandangkan teknologi semakin canggih, maka segelintir pengguna telah menjadikan teknologi lebih ke arah keselamatan. Dengan kewujudan sistem kunci pintu pengecaman wajah, tahap keselamatan dapat ditingkatkan. Sistem ini adalah untuk memastikan harta benda dan orang tersayang sentiasa selamat dan dilindungi. Bahagian penting dari setiap sistem keselamatan rumah adalah mengenal pasti orang yang memasuki dan meninggalkan rumah.

Penggunaan sistem kunci pintu secara tradisional yang bergantung kepada penggunaan perkara luaran seperti kunci, kata laluan dan kad pengenalan untuk mendapatkan akses merupakan salah satu sistem kunci pintu yang kerap digunakan sebelum ini. Walau bagaimanapun, insiden seperti kehilangan kunci telah menyebabkan berlakunya banyak kes membimbangkan seperti rompakan dan penipuan identiti. (G.Senthilkumar, K.

Goplakrishnan, V.S. Kumar, 2014) Untuk mengatasi masalah ini, sistem kunci pintu pengecaman wajah menggunakan teknologi pembelajaran mendalam telah diperkenalkan, dan Internet Of Thing (IOT) juga digunakan untuk menerapkan sistem kontrol akses yang efisien. Biometrik adalah satu-satunya parameter yang dapat dihitung yang digunakan untuk pengenalan individu jika dibandingkan dengan ciri biologi lain seperti cetakan cap jari. Pengecaman wajah adalah kaedah yang paling terkenal dalam teknologi pengecaman biometrik kerana wajah mengandungi lebih banyak ciri dan membawa kestabilan yang lebih tinggi. Selain itu, wajah dianggap sangat selamat kerana ia tidak dapat dicuri, dipinjam dan dipalsukan untuk memasuki rumah.

Internet Of Thing (IOT) adalah teknologi masa depan yang menghubungkan peranti dan internet. Ia berbeza dengan Internet kerana Internet melangkaui sambungan dan membolehkan mana-mana litar tertanam berkomunikasi antara satu sama lain menggunakan infrastruktur internet semasa. Tidak dapat dinafikan bahawa Internet Of Thing (IOT) dapat membantu pengguna mengendalikan satu atau lebih peranti dan secara automatik melakukan banyak tugas harian. Dengan menggunakan Internet Of Thing (IOT), ia dapat membantu dalam pengawalan kawalan akses dan menghantar pemberitahuan melalui Internet.

2 PENYATAAN MASALAH

Sistem kunci pintu yang ada pada masa kini lebih fokus kepada cetakan cap jari, kata laluan dan penggunaan kad pengenalan untuk mendapatkan akses. Malangnya sistem ini tidak cukup untuk membantu kunci pintu daripada ancaman yang boleh berlaku seperti rompakan. Orang lain masih akan berupaya untuk mendapatkan akses pintu rumah dimana data seseorang itu boleh dicuri dengan menggunakan pelbagai kecanggihan teknologi yang ada pada masa kini. Ini adalah jelas bahawa data peribadi masih tidak selamat dan boleh diakses oleh orang lain.

Selain itu, sebilangan besar reka bentuk kunci pintu dengan kunci biasanya menghadapi beberapa kerosakan seperti kunci yang hilang, lupa untuk membawa kunci dan masalah yang paling serius ialah lupa mengunci pintu kerana kecuaiian. Keselamatan setiap penghuni haruslah diutamakan dalam bagaimana cara sekalipun.

3 OBJEKTIF KAJIAN

Sistem ini bertujuan untuk mencegah insiden seperti kehilangan kunci dan berlakunya rompakan. Demi mencapai matlamat tersebut, sistem ini seharusnya dapat melaksanakan objektif seperti berikut :

- i. Mengecam pengguna yang diberi autoriti dan rekaan sistem kecaman wajah masa nyata.
- ii. Senang diguna dan mudah difahami oleh pengguna.
- iii. Kebolehan menjana bunyi penggera semasa ancaman dikesan.

4 SKOP KAJIAN

Produk akhir akan merangkumi kamera untuk menangkap imej, dan sistem perisian yang akan memproses imej dan membuat keputusan. Sistem yang direka akan mempunyai pangkalan data yang mempunyai fail untuk gambar pengguna. Sistem ini akan mengenali wajah manusia terlebih dahulu. Sekiranya terdapat wajah di pangkalan data, pintu akan terbuka dan sekiranya tidak, sistem akan mempunyai kemampuan untuk mengenali pengguna dan memutuskan untuk menghasilkan bunyi penggera.

4.1 Fasa Perancangan

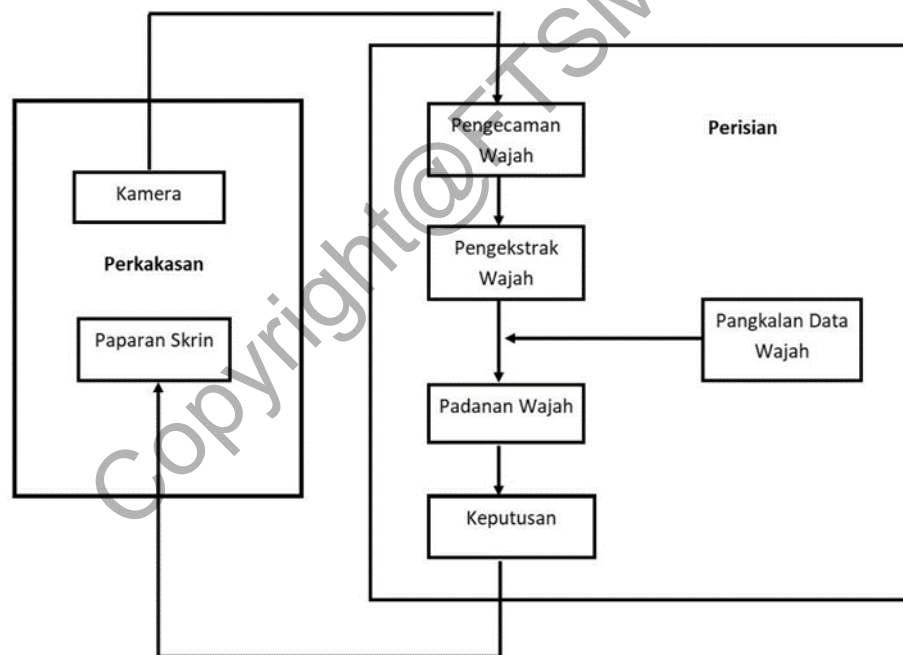
Fasa ini melibatkan proses mengenal pasti masalah, tujuan, meneliti masalah, dan menentukan skop. Langkah seterusnya melibatkan pengumpulan dan pencarian jurnal dan penyelidikan sebelumnya untuk menjana idea dan inspirasi. Banyak topik yang berkaitan dengan projek ini telah dicari, termasuk konsep reka bentuk sistem pengenalan wajah yang ada. Di samping itu, pada fasa ini, maklumat mengenai penggunaan projek dan alatnya juga diperlukan.

4.2 Fasa Analisis

Fasa analisis ini melibatkan maklumat yang dikumpulkan dalam peringkat perancangan pada fasa sebelum ini. Topik yang berkaitan dan bersesuaian serta penilaian kepentingan telah dianalisis bagi menjalankan projek. Selain itu, analisis tentang perkakasan dan perisian juga dilakukan untuk memastikan bahawa perkakasan dan perisian yang ada sesuai untuk projek ini.

4.3 Fasa Reka Bentuk

Fasa ini adalah fasa penting dari keseluruhan projek. Terdapat dua proses penting pada fasa ini, iaitu reka bentuk algoritma dan reka bentuk pangkalan data. Sistem yang dibina ini akan menjalankan pemrosesan data yang menggunakan pangkalan data dari *Amazon Web Services (AWS)*. Gambar yang diambil dari kamera raspberry pi seterusnya akan disimpan di *cloud* dimana ia hanya berada di dalam satu pangkalan data. Sistem ini tidak menggunakan pangkalan data yang sebenarnya, tetapi hanya menggunakan data yang disimpan di dalam format gambar (.jpg). Gambar yang digunakan akan disimpan dan tidak akan dipapar kerana sistem akan terus merekod data gambar wajah pengguna di dalam *cloud*. Algoritma ini dipecah kepada empat bahagian, iaitu mengesan wajah dalam imej, analisis ciri muka, perbandingan dengan wajah dalam pangkalan data dan membuat keputusan.



Rajah 1 Reka bentuk aliran sistem diasingkan dengan perisian dan perkakasan

4.4 Fasa Pengujian

Fasa ini bertujuan untuk menguji model yang dihasilkan dalam fasa reka bentuk. Teknik reka bentuk kes ujian yang baik sangat penting untuk meningkatkan kualiti proses ujian perisian. Ini membantu meningkatkan kualiti dan keberkesanan keseluruhan perisian yang dikeluarkan.

Pengujian keselamatan adalah subtype pengujian perisian yang melibatkan mengenal pasti risiko, ancaman, dan kerentanan dalam aplikasi. Tujuan ujian ini adalah untuk mengelakkan penjenayah siber memasuki aplikasi dan melancarkan serangan jahat.

Sistem ini telah dibina, diuji dan dimodifikasi berkali-kali untuk memastikan bahawa sistem akhir dapat berfungsi dengan baik. Keseluruhan projek hanya menggunakan bahasa *Python* di persekitaran *Windows 10* dan beberapa alat untuk mempercepat dan menyelesaikan proses pembangunan. Sebahagian daripada algoritma pengenalan wajah adalah pustaka *Python* yang dibina oleh Adam Geitgey. Sistem ini mempunyai beberapa bahagian kod kunci utama, bahagian penggunaan pustaka pengecaman wajah, bahagian penutupan kamera dan bahagian pengambilan serta penyimpanan gambar.

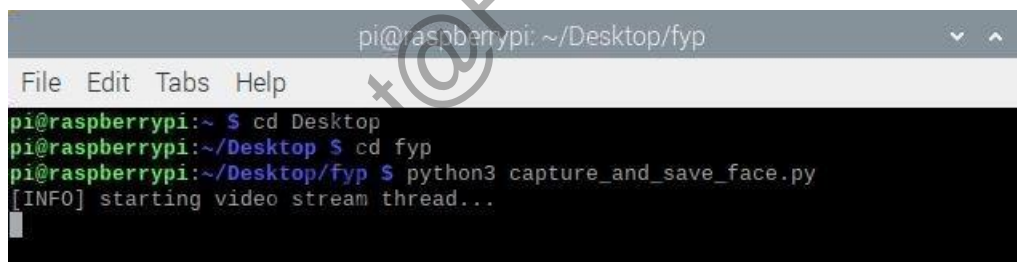
Sistem ini menggunakan servis rekognito yang telah disediakan AWS untuk penggunaan pengecaman wajah dimana ia lebih cepat dan pantas untuk dihasilkan. AWS merupakan satu *cloud* dimana ia membantu dalam menyimpan data untuk pengecaman wajah. Pustaka sistem ini juga memerlukan *Visual Studio Code* yang dipasang bersama bahasa *Python*. Di samping itu, untuk menggunakan kamera yang ada di komputer, pemasangan program python opencv diperlukan. Setelah membina semua pustaka dan persekitaran komputer, proses pembinaan kod dapat dimulakan. Berikut merupakan senarai komponen bagi pemasangan raspberry pi bagi memudahkan pembangunan sistem;

- Official RPi 15W (5V/3A) PSU USB C UK Plug-White
- 12VDC Solenoid Door Lock
- 18650 Battery Holder
- 3.7V 200mAh Li-Ion Battery
- ICH Active H/L 5V OptoCoupler Relay Module
- CH-2 Quick Wiring Terminal Press Type
- Maker pHAT: Simplifying Raspberry Pi
- 16GB Micro SD Card with NOOBS for RPI
- Raspberry Pi 8MP Camera Module V2
- Raspberry Pi 4 Model B

5 HASIL KAJIAN

Bahagian ini membincangkan tentang proses pembangunan sistem kunci pintu pengecaman wajah menggunakan raspberry pi. Untuk ujian keperluan bukan fungsian, ujian kebolegunaan akan digunakan. Pengguna akan cuba menggunakan produk binaan dan memerhatikan sama ada syarat keperluan bukan fungsian telah dipenuhi. Sepanjang proses pengujian, pengguna akan diberi panduan ke langkah seterusnya. Melalui ujian kebolegunaan sistem ini, bukan sahaja keperluan bukan fungsian dapat diperiksa, tetapi juga peralatan sistem dapat diuji. Pengguna akan menguji semua fungsi atau butang sistem dan menentukan sama ada berlakunya bug atau error.

Perkara pertama yang berlaku dalam sistem ini ialah pengguna akan masuk ke antara muka daftar masuk sistem selepas membuka fail *Python*. Pengguna akan mendaftar masuk ke dalam sistem iaitu dengan mendaftar wajah mereka dengan menaip “*python3 capture_and_save_face.py*” dan seterusnya kamera raspberry pi akan terbuka dan mula mengecam wajah mereka bagi tujuan penyimpanan data.



```

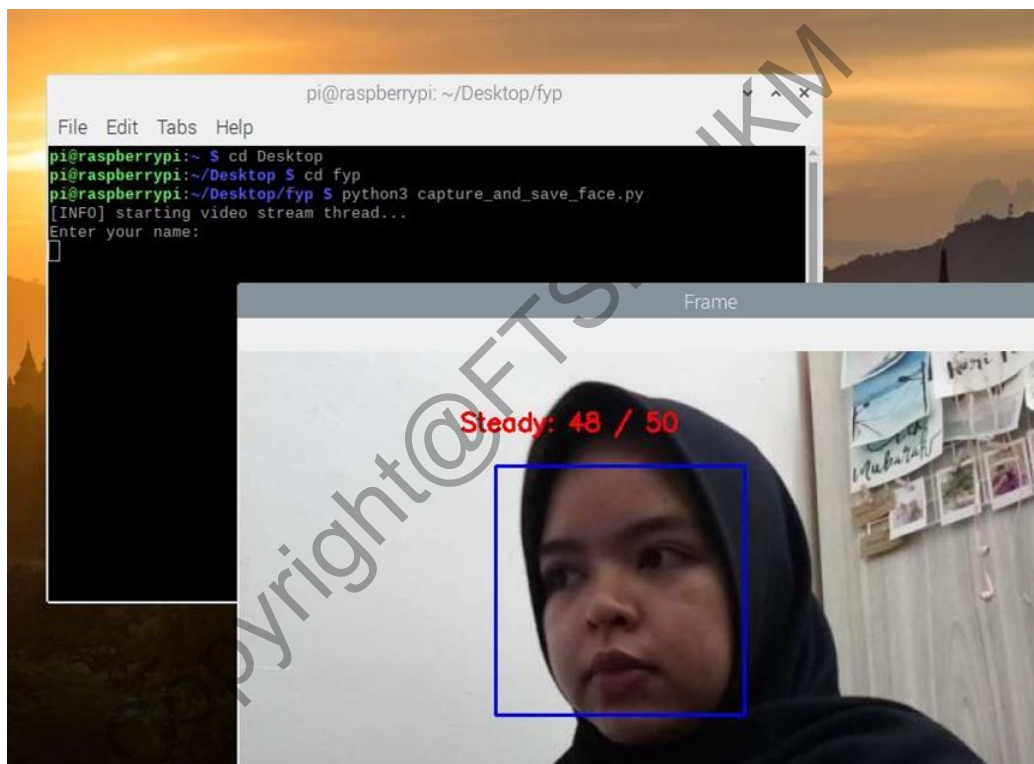
pi@raspberrypi: ~/Desktop/fyp
File Edit Tabs Help
pi@raspberrypi:~ $ cd Desktop
pi@raspberrypi:~/Desktop $ cd fyp
pi@raspberrypi:~/Desktop/fyp $ python3 capture_and_save_face.py
[INFO] starting video stream thread...

```

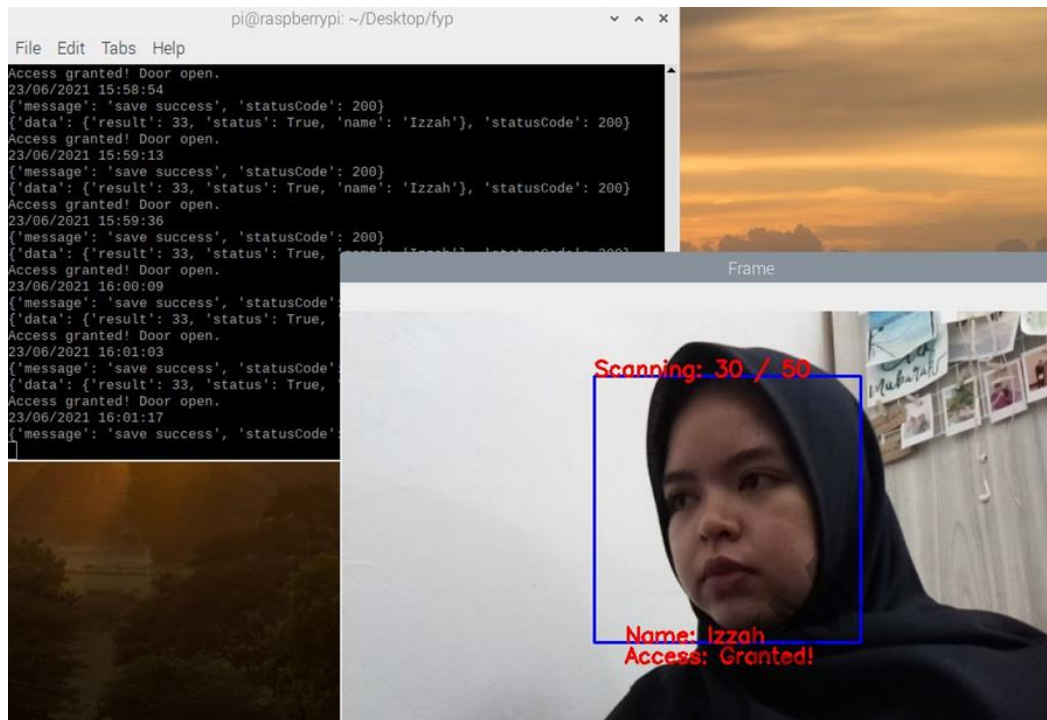
Rajah 2 Pengguna harus menaip seperti di dalam rajah di atas bagi tujuan mendaftar masuk ke dalam sistem.

Seterusnya, pengguna perlu memasukkan nama bagi membenarkan wajah mereka untuk disimpan di dalam pangkalan data dan menjadi pengguna yang berautoriti. Selepas pendaftaran wajah pengguna diambil, pengguna dapat masuk ke dalam sistem dengan hanya berada di depan kamera raspberry pi bagi tujuan pengecaman wajah dan kunci pintu akan terbuka. Dalam sistem ini juga, pengguna dapat menyemak rekod penggunaan yang berautoriti melalui pangkalan data di laman web *Amazon Web Services(AWS)*. Sistem ini juga akan menyimpan gambar dalam format *.jpg* melalui *Windows*.

Setelah sistem pengecaman wajah diaktifkan, produk akhir tidak akan mempunyai pemberitahuan dan *pop out windows*. Pengguna hanya dapat mengetahui bahawa sistem berjalan melalui lampu pada kamera. Untuk menampilkan proses pengecaman wajah dalam produk ini, *windows* akan digunakan. Kemudian, apabila paparan kamera ditutup, pengguna dibawa ke fail dengan catatan pengguna di depan komputer. Semua gambar yang disimpan adalah dalam format tarikh YY-MM-DD dan format masa HH-MM-SS, supaya senang dapat mencarinya sekiranya terdapat sebarang kesulitan.

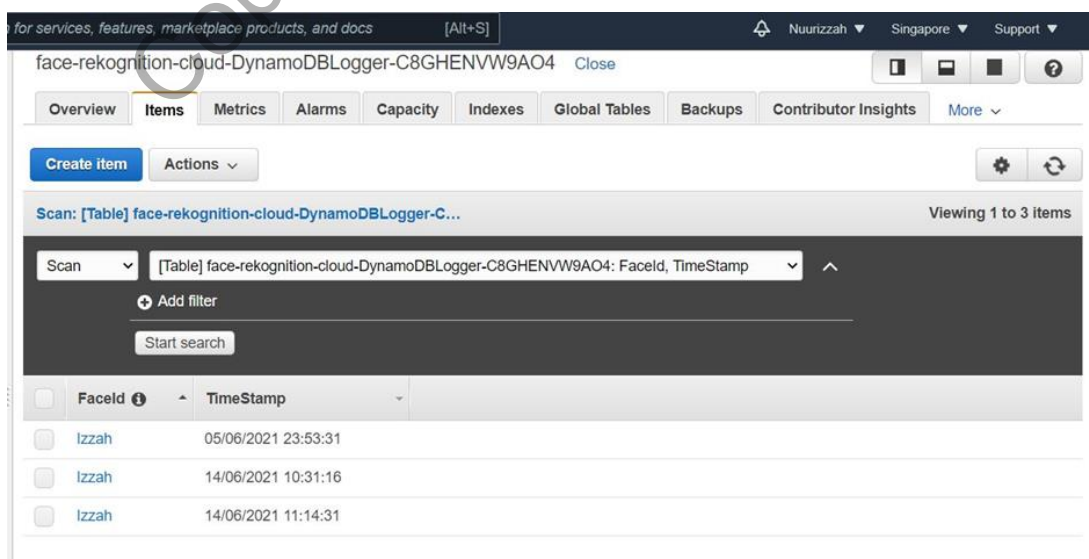


Rajah 3 Sistem akan mengecam wajah dan pengguna harus memasukkan nama bagi tujuan penyimpanan data ke dalam *cloud*.



Rajah 4 Sistem akan mengecam wajah dan menerima mesej daripada pangkalan data sama ada pengguna berautoriti ataupun tidak.

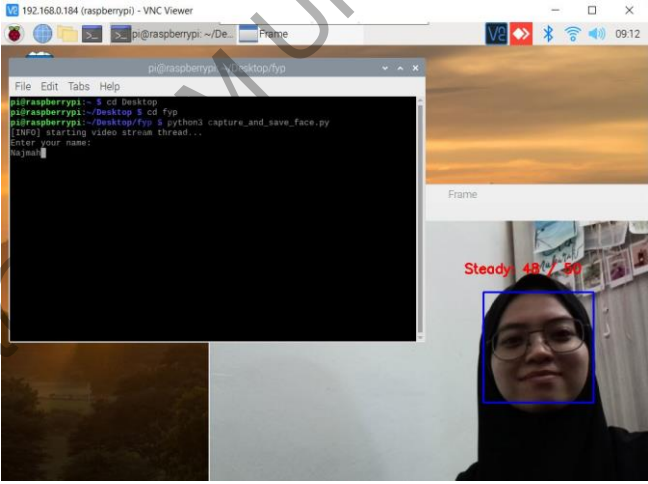
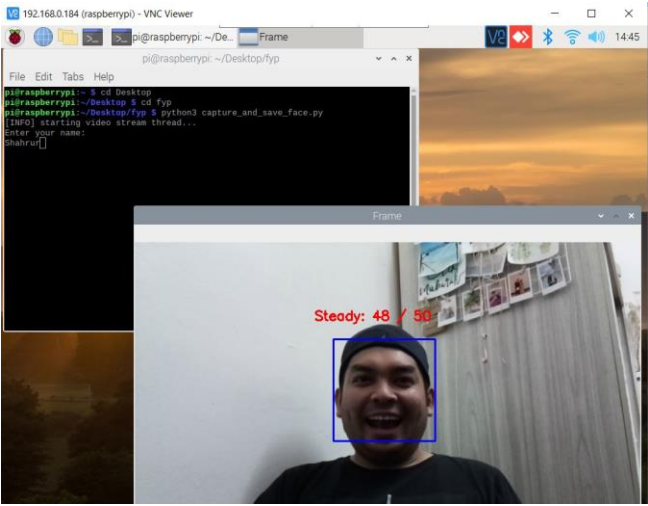
Untuk tujuan semakkan pengguna, sistem telah diselarikan dengan pangkalan data dari *Amazon Web Services(AWS)*. Pengguna perlu log masuk ke dalam akaun AWS untuk menyemak rekod pengguna yang menggunakan sistem kunci pintu pengecaman wajah ini. Semakan rekod pula hanya akan menunjukkan rekod pengguna yang berautoriti.



Rajah 5 Pangkalan data (AWS) untuk semakkan rekod pengguna.

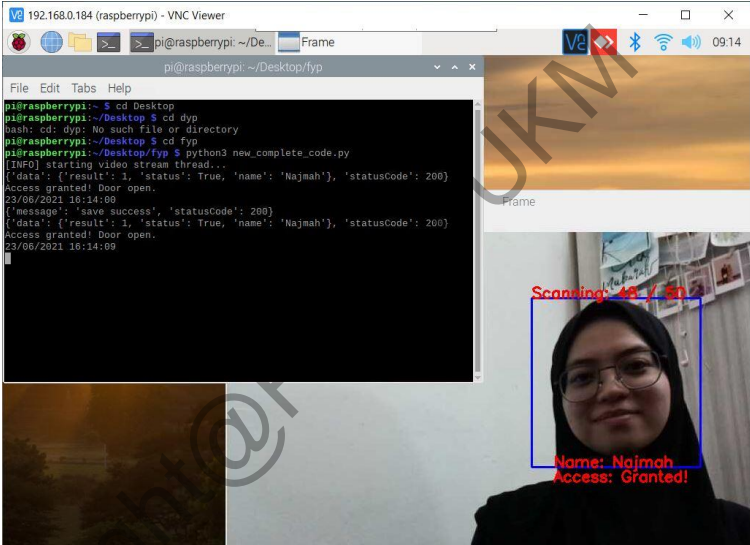
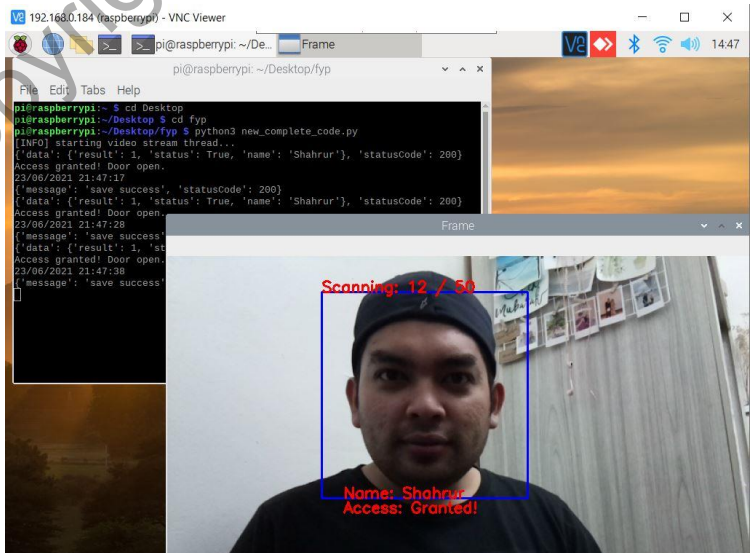
Ujian dibawah merupakan ujian bagi sistem kunci pintu pengecaman wajah yang telah disiap dibina. Ujian ini telah melibatkan beberapa pengguna lain yang diberi autoriti dalam sistem dan juga yang tidak berautoriti bagi menguji kebolehan sistem berfungsi.

Jadual 1 Ujian penyimpanan gambar wajah pengguna

Bil pengguna	Penyimpanan gambar wajah pengguna di dalam cloud
1	
2	

Jadual memaparkan bahawa sistem berjaya menyimpan gambar wajah pengguna di dalam *cloud*. Sistem akan mengeluarkan mesej “Enter your name” setiap kali penyimpanan gambar wajah dilakukan.

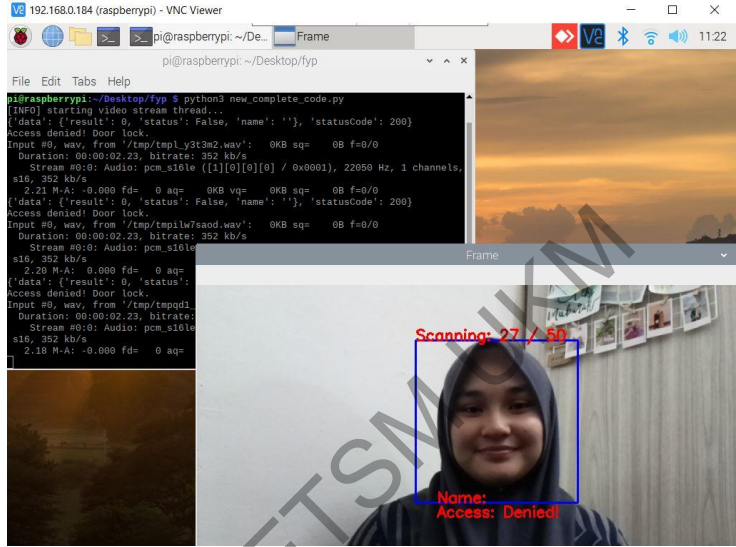
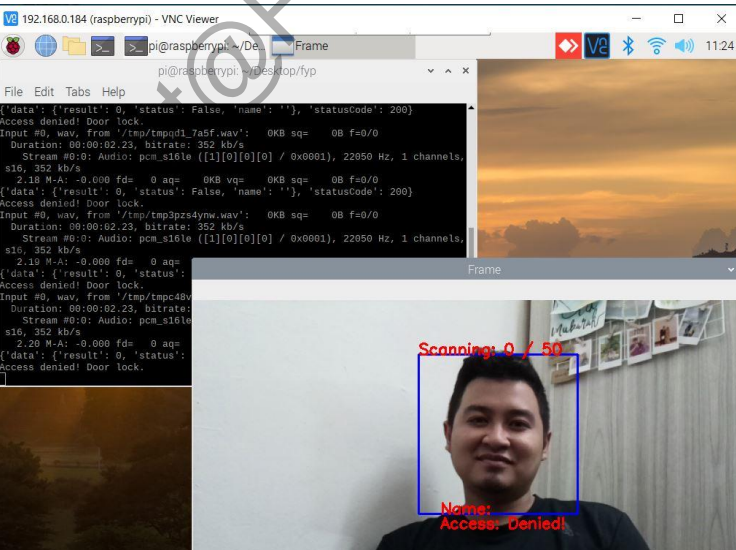
Jadual 2 Ujian Pengguna Berautoriti

Bil pengguna	Pengecaman wajah pengguna yang berautoriti
1	 <p>The screenshot shows a VNC viewer window titled '192.168.0.184 (raspberrypi) - VNC Viewer'. The terminal window displays the following commands and output:</p> <pre> pi@raspberrypi:~\$ cd Desktop pi@raspberrypi:~/Desktop\$ cd dyp bash: cd: dyp: No such file or directory pi@raspberrypi:~/Desktop\$ cd fyp pi@raspberrypi:~/Desktop/fyp\$ python3 new_complete_code.py [INFO] starting video stream thread... {"data": {"result": 1, "status": True, "name": "Najmah"}, "statusCode": 200} Access granted! Door open. 23/06/2021 16:14:08 {"message": "save success", "statusCode": 200} {"data": {"result": 1, "status": True, "name": "Najmah"}, "statusCode": 200} Access granted! Door open. 23/06/2021 16:14:09 </pre> <p>The video stream shows a woman's face with a bounding box and text: "Scanning: 42 / 50", "Name: Najmah", and "Access: Granted!".</p>
2	 <p>The screenshot shows a VNC viewer window titled '192.168.0.184 (raspberrypi) - VNC Viewer'. The terminal window displays the following commands and output:</p> <pre> pi@raspberrypi:~\$ cd Desktop pi@raspberrypi:~/Desktop\$ cd fyp pi@raspberrypi:~/Desktop/fyp\$ python3 new_complete_code.py [INFO] starting video stream thread... {"data": {"result": 1, "status": True, "name": "Shahrur"}, "statusCode": 200} Access granted! Door open. 23/06/2021 21:47:17 {"message": "save success", "statusCode": 200} {"data": {"result": 1, "status": True, "name": "Shahrur"}, "statusCode": 200} Access granted! Door open. 23/06/2021 21:47:28 {"message": "save success", "statusCode": 200} {"data": {"result": 1, "st": "Shahrur"}, "statusCode": 200} Access granted! Door open. 23/06/2021 21:47:38 {"message": "save success", "statusCode": 200} </pre> <p>The video stream shows a man's face with a bounding box and text: "Scanning: 12 / 50", "Name: Shahrur", and "Access: Granted!".</p>

Jadual 2 telah menunjukkan hasil daripada penyimpanan data di dalam cloud, sistem dapat mengecam pengguna yang mempunyai autoriti. Di setiap gambar pengguna yang dapat

dikecam akan dinyatakan nama pengguna dan pangkalan data akan menghantar mesej “Access granted! Door open”.

Jadual 3 Ujian Pengguna Tidak Berautoriti

Bil pengguna	Pengecaman wajah pengguna yang tidak berautoriti
1	
2	

Seperti yang dipaparkan dalam jadual 3, pintu tidak akan dibuka kepada pengguna yang tidak diberi autoriti ataupun tidak berdaftar dalam sistem. Sistem akan mengeluarkan mesej “Access denied! Door lock”. Bukan itu saja, setelah sistem mengenali pengguna yang tidak dibenarkan, sistem akan membunyikan penggera.

Dari segi keperluan bukan fungsian pula, purata masa sistem membuat keputusan adalah 3 saat. Dalam proses pengecaman wajah, setiap pengguna hanya boleh menggunakan satu gambar. Dalam proses pengecaman wajah, setiap pengguna hanya dapat menggunakan satu gambar. Ketepatan pengecaman wajah dapat disesuaikan melalui tahap kepekaan yang dapat diubah, dan produk akhir mempunyai kepekaan dan ketepatan yang tinggi, sekitar 90%. Namun, jika pengguna bergerak dengan postur yang aneh, sistem akan mengesan pengguna sebagai orang yang tidak dikenali kerana tahap sensitif yang tinggi.

Sepanjang ujian keseluruhan, pengguna mesti berdiri di depan kamera, kira-kira 30 cm dari paparan kamera. Keperluan bukan fungsian yang terakhir adalah dapat mengenal pasti dua pengguna pada masa yang sama. Pada ketika ini, ujian kebolegunaan sistem telah berakhir. Semua keperluan yang bukan fungsian telah dipenuhi, dan sistem yang dibina berjalan lancar.

6 KESIMPULAN

Kesimpulannya, proses pengembangan sistem kunci pintu pengecaman wajah menggunakan Raspberry Pi sangat lancar. Algoritma pepadanan sebelumnya telah dikaji semula untuk meningkatkan proses pepadanan yang dilakukan.

Proses pembangunan merupakan proses yang sangat sukar dan memerlukan banyak maklumat yang perlu dicari dari laman web untuk menambah produk akhir. Walaupun kod asal yang digunakan adalah karya dari orang lain, pelbagai perubahan dan penambahbaikan telah dilakukan pada kod tersebut. Kod penghubung antara fungsi juga telah ditambah baik agar produk akhir wujud sebagai *standalone application* yang sebenar. Dengan menguji alat yang telah lengkap, segala ralat dalam aplikasi ini dapat dikesan. Tahap ini sangat penting dan perlu diulang untuk memastikan semua komponen yang digunakan berfungsi dengan baik.

Secara umum, sistem pengecaman wajah yang terbina dapat mengenal pasti dan membezakan antara pengguna yang berautoriti dan yang tidak. Sistem pengecaman wajah ini juga dapat mematikan paparan kamera sekiranya berlaku sebarang ancaman. Sistem ini juga telah memenuhi semua keperluan fungsian dan bukan fungsian dan dapat dibuktikan sebagai produk yang berjaya.

7 RUJUKAN

- “Class: AWS.Rekognition — AWS SDK for JavaScript.” *Amazon.com*, 2016, docs.aws.amazon.com/AWSJavaScriptSDK/latest/AWS/Rekognition.html.
- ageitgey. (2017). Face Recognition. Retrieved from Github: https://github.com/ageitgey/face_recognition.ageitgey.
- “Ageitgey/Face_recognition.” *GitHub*, 14 June 2021, github.com/ageitgey/face_recognition.
- G.Senthilkumar, K. Goplakrishnan,V.S. Kumar. (2014). *"Embedded image capturing system using raspberry pi system" vol. 3 No. 2,pp. 213-215.*
- Geitgey, A. (2016,). *Machine Learning is Fun! Part4: Modern Face Recognition with Deep Learning.*
- Hrishikesh Kulkarni, D. (2018). *Unconstrained Facial Recognition using Supervised Deep Learning on Video.*
- Marwan Ibrahim Alshar'e, R.S. (2014). *A USER PROTECTION MODEL FOR THE TRUSTED COMPUTING ENVIRONMENT.* Research Centre for Software Technology and Management (Softam), Faculty of Information Science and Technology, National University of Malaysia, Malaysia.
- Muhammad Naeem, I. (2015). *FACE RECOGNITION TECHNIQUES AND APPROAVHES: A SURVEY.* Pakistan.
- Muhammad SHARIF, A. (2011). *Face Recognition using Gabor Filters.* Journal of Applied Computer Science & Mathematics, no. 11(5)/2011, Suceava.
- Nurul Azma Abdullah, M. (2017). *Face Recognition for criminal identification: An implementation of principal component analysis for face recognition.*