KAWALAN INTERNET BENDE PINTU PINTAR MENGGUNAKAN KESELAMATAN TEKNOLOGI BIOMETRIK DALAM PELANTAR TELEGRAM

YOGARASEN A/L MANIYARASAN

PROF. DR. ROSILAH HASSAN

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Darul Ehsan, Malaysia

Abstrak

Projek ini menangani permasalahan keselamatan akses fizikal yang masih bergantung pada sistem kunci tradisional yang mudah hilang, dipalsukan atau disalah guna. Tujuan kajian ini adalah untuk membangunkan satu sistem pintu pintar berasaskan teknologi biometrik yang lebih selamat, efisien dan sesuai dengan keperluan keselamatan moden. Kajian ini dijalankan secara aplikasi dan ujikaji di kawasan tertutup seperti pejabat dan premis komersial. Kaedah yang digunakan melibatkan penggabungan beberapa teknologi terkini iaitu sensor cap jari untuk pengesahan identiti, modul ESP32-CAM untuk rakaman gambar masa nyata, dan pelantar komunikasi Telegram untuk penghantaran notifikasi serta imej terus kepada pemilik sistem. Keseluruhan sistem diprogram menggunakan platform Arduino IDE dan disokong oleh rangkaian Internet Benda (IoT) bagi membolehkan komunikasi serta pemantauan berlaku dari jarak jauh. Hasil kajian menunjukkan sistem ini berfungsi dengan efektif dalam menyekat akses pengguna tidak sah melalui amaran buzzer serta pemberitahuan masa nyata, sekali gus mengurangkan risiko pencerobohan. Penemuan ini membuktikan bahawa teknologi kos rendah boleh digunakan untuk menghasilkan sistem keselamatan yang pintar dan praktikal. Sumbangan kajian ini kepada bidang teknologi maklumat dan keselamatan adalah dalam bentuk inovasi sistem integrasi yang menggabungkan biometrik, IoT, dan aplikasi mudah alih dalam satu rangka kerja yang ringkas dan berkesan. Dari segi implikasi dasar, sistem ini berpotensi untuk menyokong inisiatif keselamatan digital negara dan boleh diaplikasikan dalam sektor awam dan swasta bagi meningkatkan kecekapan pemantauan akses fizikal secara masa nyata.

Kata Kunci: Biometrik, Internet Benda, Telegram, Keselamatan Fizikal.

Abstract

This project addresses the issue of physical access security, which still relies on traditional key systems that are prone to being lost, forged, or misused. The aim of this study is to develop a smart door system based on biometric technology that is safer, more efficient, and aligned with modern security needs. The study was conducted through application and experimentation in enclosed areas such as offices and commercial premises. The method used involves the integration of several modern technologies, namely fingerprint sensors for identity verification, the ESP32-CAM module for real-time image capture, and the Telegram communication platform for sending notifications and images directly to the system owner. The entire system is programmed using the Arduino IDE platform and supported by the Internet of Things (IoT) network to enable remote communication and monitoring. The results of the study show that the system functions effectively in preventing unauthorized access through buzzer alerts and real-time notifications, thereby reducing the risk of intrusion. These findings demonstrate that low-cost technology can be utilized to produce a smart and practical security system. The study's contribution to the field of information technology and security lies in the innovation of an integrated system that combines biometrics, IoT, and mobile applications into a simple and efficient framework. In terms of policy implications, this system has the potential to support national digital security initiatives and can be applied in both public and private sectors to enhance the efficiency of real-time physical access monitoring.

1.0 PENGENALAN

Projek Kawalan Internet Benda Pintu Pintar Menggunakan Keselamatan Teknologi Biometrik Dalam Pelantar Telegram merupakan inisiatif inovatif yang menggabungkan teknologi Internet Benda (IoT), pengesahan biometrik (cap jari), modul ESP32 CAM, dan pelantar Telegram untuk menghasilkan sistem kawalan akses yang lebih cekap, selamat, dan fleksibel. Sistem ini direka khas untuk menggantikan kaedah kawalan akses tradisional seperti kunci fizikal dan kad akses yang mudah hilang, dicuri, atau disalin, seterusnya meningkatkan risiko keselamatan. Dengan pengimbas cap jari, sistem menjamin hanya individu yang dibenarkan sahaja boleh memasuki premis, manakala ESP32 CAM akan menangkap gambar pengunjung secara masa nyata dan menghantar notifikasi visual terus ke aplikasi Telegram pemilik, membolehkan identiti pengunjung dikenal pasti serta-merta dari mana-mana lokasi.

Projek ini bertujuan untuk mengkaji dan memanfaatkan teknologi IoT bagi mengurangkan kos operasi sistem pintu pintar, mereka bentuk sistem pengesahan berasaskan

biometrik cap jari, dan membangunkan sistem yang mampu mengawal serta memantau keselamatan menggunakan pelbagai sensor. Skop projek ini merangkumi pembangunan fungsi utama seperti pengesahan cap jari, penghantaran notifikasi visual, dan penyimpanan log akses melalui Telegram, namun tidak termasuk fungsi tambahan seperti pengenalan wajah, rakaman CCTV berterusan, penyimpanan awan untuk imej, atau aplikasi pemantauan selain Telegram. Hal ini membolehkan sistem kekal mudah, kos rendah, dan mudah digunakan.

Bagi memastikan projek dibangunkan secara sistematik dan berkesan, model Spiral dipilih sebagai metodologi utama. Model ini menawarkan pendekatan pembangunan yang fleksibel dan berorientasikan risiko dengan melalui empat fasa utama: perancangan, analisis risiko, pembangunan dan ujian. Melalui pendekatan ini, pasukan pembangunan dapat menilai dan mengurangkan risiko awal, membuat prototaip secara iteratif, dan mendapatkan maklum balas pengguna dalam setiap kitaran pembangunan. Ini membantu memastikan sistem yang dibangunkan memenuhi keperluan sebenar pengguna dan boleh diperbaiki dari masa ke masa.

Akhir sekali, projek ini dirancang untuk dilaksanakan dalam tempoh 18 minggu dengan jadual pelaksanaan yang dirancang secara terperinci mengikut struktur Work Breakdown Structure (WBS) dan carta Gantt. Setiap aktiviti dalam projek ini mempunyai kebergantungan yang jelas daripada perancangan dan analisis risiko, ke pembangunan sistem, ujian, dan akhirnya pelaksanaan dan penyerahan sistem kepada pengguna. Rangka masa ini memberi panduan kepada pasukan projek dalam menyusun tugasan dan memastikan segala aktiviti diselesaikan mengikut jadual, seterusnya menjamin kualiti dan keberkesanan sistem yang dibangunkan.

2.0 KAJIAN LITERATUR

Kawalan Internet Bende Pintu Pintar Menggunakan Keselamatan Teknologi Biometrik Dalam Pelantar Telegram

Sistem pintu pintar yang menggabungkan teknologi biometrik dan Internet Benda (IoT) semakin mendapat perhatian dalam meningkatkan keselamatan dan kemudahan akses. Penyelidikan terdahulu menunjukkan bahawa penggunaan sensor cap jari dan pengesahan

wajah bersama dengan platform komunikasi seperti Telegram dapat meningkatkan kawalan akses dan pemantauan masa nyata.

Satu kajian oleh Siswanto dan Alfyandi (2024) mengusulkan sistem pintu pintar berasaskan aplikasi Android yang menggunakan sensor cap jari untuk pengesahan identiti. Sistem ini membolehkan pemilik rumah melihat gambar pengunjung dan mengunci atau membuka pintu dari jauh melalui aplikasi. Selain itu, sistem ini juga dilengkapi dengan amaran kecurian yang menghantar pemberitahuan kepada pemilik melalui aplikasi mudah alih apabila percubaan pencerobohan dikesan.

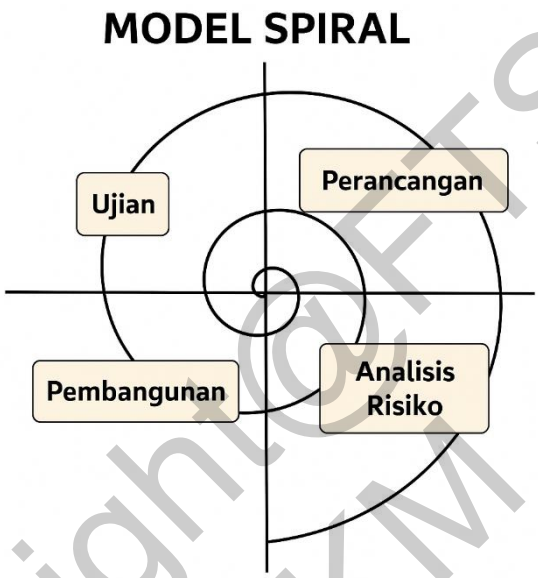
Kajian lain oleh Bello et al. (2025) membincangkan sistem pintu pintar berasaskan pengenalan wajah menggunakan modul ESP32-CAM. Sistem ini menggunakan algoritma pengenalan wajah untuk mengenal pasti individu yang dibenarkan dan mengawal kunci elektromagnetik berdasarkan keputusan pengenalan. Sistem ini menunjukkan ketepatan yang tinggi dalam mengenal pasti pengguna yang dibenarkan dan menolak akses kepada individu yang tidak dibenarkan, meningkatkan keselamatan dan kemudahan dalam kawalan akses.

Dalam kajian oleh Suneetha et al. (2025), sistem pintu pintar berasaskan IoT diperkenalkan yang menggabungkan pengesahan cap jari dan pengenalan wajah untuk meningkatkan keselamatan. Sistem ini menggunakan modul ESP32 dan kamera OV2640 untuk menangkap dan menganalisis imej wajah bagi mengenal pasti individu yang dibenarkan. Selain itu, sistem ini juga dilengkapi dengan ciri penghantaran imej individu yang tidak dibenarkan kepada pemilik melalui e-mel, meningkatkan pemantauan dan tindak balas terhadap percubaan pencerobohan.

Satu lagi kajian oleh Radzi et al. (2020) membincangkan penggunaan platform Telegram dalam sistem kawalan dan pemantauan pintu pintar berasaskan IoT. Sistem ini menggunakan modul Wemos untuk mengawal kunci pintu dan menghantar pemberitahuan kepada pemilik melalui Telegram apabila percubaan pencerobohan dikesan. Penggunaan Telegram membolehkan pemilik rumah memantau dan mengawal akses pintu dari jauh dengan mudah.

3.0 METODOLOGI KAJIAN

Bagi projek Sistem Kawalan Internet Bende Pintu Pintar Menggunakan Keselamatan Teknologi Biometrik dalam Pelantar Telegram, model pembangunan yang digunakan adalah Model Spiral. Model ini dipilih kerana ia menawarkan pendekatan fleksibel yang menumpukan kepada pengurusan risiko secara berperingkat dalam setiap fasa pembangunan. Ia menggabungkan kekuatan model waterfall dan iteratif dengan menekankan pembinaan prototaip dan maklum balas berterusan.



Rajah 1: Model Spiral yang digunakan dalam pembangunan sistem.

Fasa pertama ialah Perancangan, di mana keperluan pengguna dikenalpasti melalui sesi pengumpulan maklumat bersama pemilik premis. Fasa ini menghasilkan dokumen spesifikasi awal sistem.

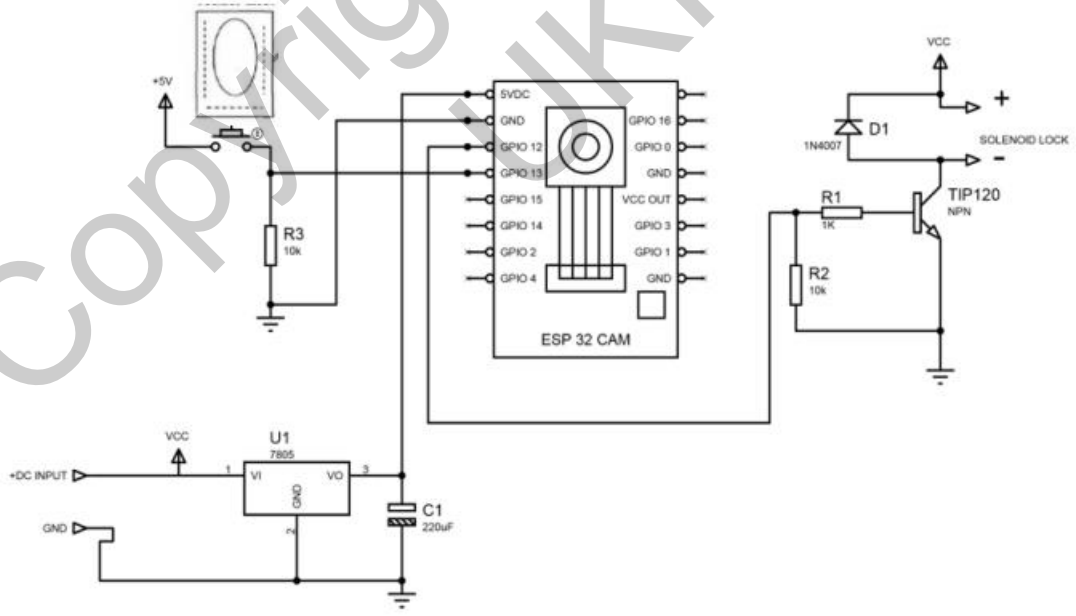
Fasa kedua ialah Analisis Risiko, yang mengenal pasti risiko seperti keselamatan data biometrik, kerumitan integrasi dengan pelantar Telegram, dan kemungkinan kekurangan komponen perkakasan seperti sensor cap jari atau ESP32-CAM. Strategi mitigasi dirangka untuk mengurangkan impak risiko-risiko ini.

Fasa ketiga adalah Pembangunan, melibatkan pengekodan sistem, termasuk pengaturcaraan modul pengesahan cap jari, penghantaran gambar oleh ESP32-CAM, serta integrasi dengan API Telegram. Sistem dibangunkan secara iteratif untuk membolehkan semakan dan penambahbaikan dilakukan dalam setiap kitaran.

Akhir sekali, fasa Ujian dilaksanakan untuk menguji fungsi sistem secara menyeluruh, seperti kebolehgunaan sensor cap jari, ketepatan sistem dalam mengenal pasti pengguna yang sah, keberkesanan notifikasi masa nyata, dan kestabilan sistem keseluruhan. Setiap iterasi diuji agar sistem mencapai tahap keselamatan dan kebolehgunaan yang tinggi.

3.1 Analisis Keperluan

Fasa ini menumpukan kepada penentuan keperluan sistem. Keperluan fungsian seperti pengesahan cap jari, penghantaran notifikasi visual melalui Telegram, dan pemantauan akses direkodkan. Keperluan bukan fungsian pula termasuk aspek kebolehgunaan, prestasi sistem, keselamatan data pengguna, dan kebolehpercayaan sistem. Sistem ini dirancang untuk menyelesaikan masalah sistem kunci konvensional dengan menggantikan peranan kunci fizikal kepada sistem pengesahan biometrik yang lebih selamat dan sukar dipalsukan. Dalam pembangunan sistem pintu pintar ini, keperluan pengguna adalah sangat penting untuk memastikan sistem yang dibangunkan memenuhi keperluan keselamatan yang tepat dan berkesan. Teknik yang digunakan untuk memperoleh keperluan pengguna termasuk lakaran prototaip, temubual, dan analisis sistem sedia ada.



Rajah 2: Prototaip sistem

Rajah 2 menunjukkan prototip awal sistem pintu pintar dibangunkan dengan lakaran skematik untuk memberi gambaran kepada pemegang taruh mengenai reka bentuk dan

fungsionaliti sistem. Lakaran prototaip ini membolehkan pemilik premis dan pentadbir memberikan maklum balas terhadap komponen dan ciri-ciri yang perlu ada dalam sistem.

3.2 Reka Bentuk Seni Bina

Reka bentuk sistem adalah satu aspek penting dalam pembangunan perisian kerana ia memberikan gambaran struktur dan aliran operasi sistem sebelum implementasi dilakukan. Dengan memastikan reka bentuk yang jelas dan sistematik, pembangunan sistem akan menjadi lebih cekap dan mudah dikendalikan. Bahagian ini akan menghuraikan pelbagai aspek reka bentuk, termasuk reka bentuk seni bina, pangkalan data, algoritma, dan antara muka pengguna. Setiap elemen ini memainkan peranan penting dalam memastikan sistem berfungsi dengan baik dan memenuhi keperluan pengguna

3.2.1 Seni Bina Berlapis

Sistem Kawalan Internet Bende Pintu Pintar Menggunakan Keselamatan Teknologi Biometrik Dalam Pelantar Telegram akan dibangunkan menggunakan reka bentuk berlapis. Terdapat tiga peringkat utama dalam reka bentuk ini iaitu:

i. Lapisan Persembahan: Bertanggungjawab terhadap interaksi pengguna dengan sistem, seperti Pelantar Telegram yang digunakan untuk kawalan dan notifikasi.

ii. Lapisan Logik: Mengendalikan logik perniagaan seperti pengesahan cap jari, pemprosesan data akses, dan kawalan peranti.

iii. Lapisan Data: Menyimpan semua data penting, termasuk log akses, data cap jari, dan rekod gambar.

3.2.2 Carta Modul Hierarki

Carta Modul Hierarki dalam Sistem Kawalan Internet Bende Pintu Pintar Menggunakan Keselamatan Teknologi Biometrik Dalam Pelantar Telegram dirancang untuk memastikan operasi yang sistematik dan efisien. Setiap modul mempunyai fungsi khusus yang menyokong keperluan keselamatan dan fleksibiliti kawalan akses. Terdapat 7 modul dalam sistem pintu pintar ini, iaitu modul pendaftaran biometrik, modul masukkan info pengguna, modul letakkan cap jari, modul sistem menghantar notifikasi kepada pentadbir, modul sistem menghantar gambar pengguna real-time, modul sistem membuka pintu/tidak memberi

kebenaran, dan modul pintu membuka/tidak dibuka.

3.2.3 Reka Bentuk Topologi Bintang

Sistem ini menggunakan topologi bintang (*Star Topology*) kerana reka bentuk ini memastikan komunikasi langsung antara setiap komponen IoT dengan pengawal utama (Arduino/ESP32) dan router, sebelum menghantar data ke Pelantar Telegram. Topologi bintang dipilih kerana beberapa kelebihan berikut:

I. Ketahanan Tinggi terhadap Kegagalan Nod – Jika salah satu komponen (contohnya, sensor cap jari) gagal berfungsi, nod lain masih dapat beroperasi tanpa menjejaskan keseluruhan sistem.

II. Kemudahan Penyelenggaraan dan Naik Taraf – Komponen seperti ESP32 CAM atau sensor cap jari boleh diganti atau ditambah dengan mudah tanpa menjejaskan operasi rangkaian.

III. Sambungan yang Stabil – Setiap komponen IoT berkomunikasi secara langsung dengan Arduino/ESP32 atau router sebagai pusat kawalan, memastikan kestabilan sambungan.

IV. Kecekapan Penghantaran Data – Komunikasi langsung antara nod dan pusat kawalan membolehkan penghantaran data dilakukan dengan pantas dan cekap.

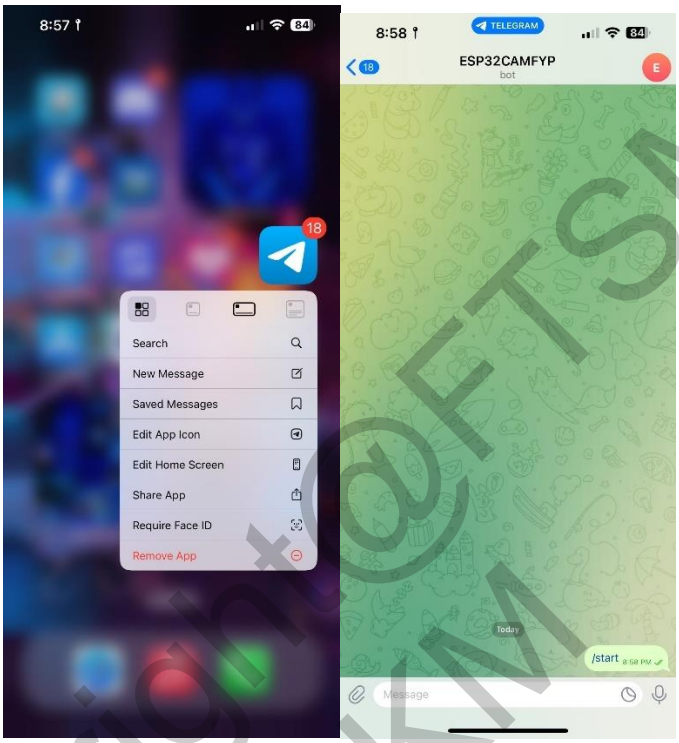
4.0 HASIL

4.1 Pembangunan Sistem

Sistem Pintu Pintar Berasaskan Teknologi Biometrik dan IoT disesuaikan untuk dilaksanakan melalui Pelantar Telegram, memanfaatkan kemudahan platform ini dalam memberikan antara muka yang intuitif dan responsif. Dengan menggunakan Telegram, sistem ini menumpukan kepada penyampaian maklumat dan fungsi yang mudah difahami pengguna, tanpa memerlukan pembangunan aplikasi khusus.

Dalam konteks ini, reka bentuk UI bertujuan untuk mencipta pengalaman pengguna yang praktikal, responsif, dan estetik. Penggunaan Telegram memanfaatkan susunan teks,

butang, dan elemen interaktif bawaan platform bagi memastikan pengguna dapat mengakses fungsi sistem dengan mudah. Apabila sesiapa menekan butang pintu, pentadbir akan mendapat pemberitahuan dalam Pelantar Telegram dengan foto orang itu. Selepas itu, anda boleh membuka kunci dan mengunci pintu dengan mudah daripada Pelantar Telegram.



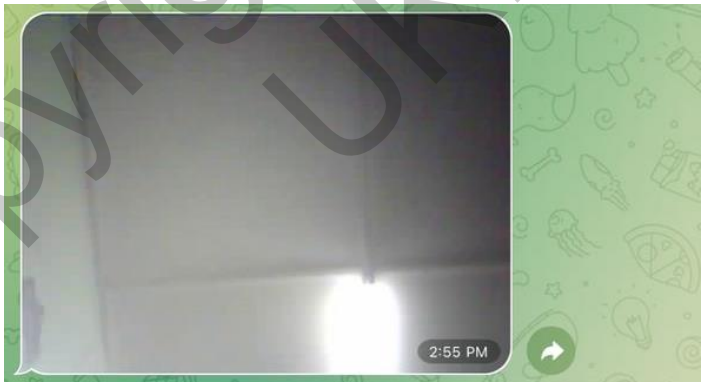
Rajah 3: Muka Halaman Aplikasi Telegram

Rajah 3 menunjukkan antara muka bagi halaman Telegram yang akan menggunakan sistem ini. ESP32 Cam chat tersebut menunjukkan contoh chat yang akan digunakan oleh pentadbir sebagai paparan untuk memantau “lock” atau “unlock” pintu.

```
  if (fingerprintID == 1)
  {
    Serial.println("Welcome YOGA");
    lcd.setCursor(0, 0);
    lcd.print("Welcome YOGA        ");
    lcd.setCursor(0, 1);
    lcd.print("                    ");
   // Blynk.virtualWrite(V4,"Welcome YOGA         ");

    digitalWrite(DOOR_DRIVER, HIGH);
    digitalWrite(DOOR_DRIVER2, HIGH);

    delay(5000);
 Serial.println("DOOR CLOSE");

 digitalWrite(DOOR_DRIVER, LOW);
digitalWrite(DOOR_DRIVER2, LOW);
     counter=0;
  }
  else if (fingerprintID == 5)
```

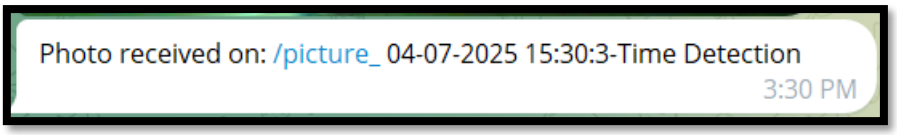
Rajah 4: Koding Arduino untuk Daftar Cap Jari

Rajah 4 menunjukkan koding arduino daftar cap jari pengguna yang telah dikod dalam arduino. Ini merupakan koding setelah pungguna meletakkan cap jari untuk mendapatkan akses.



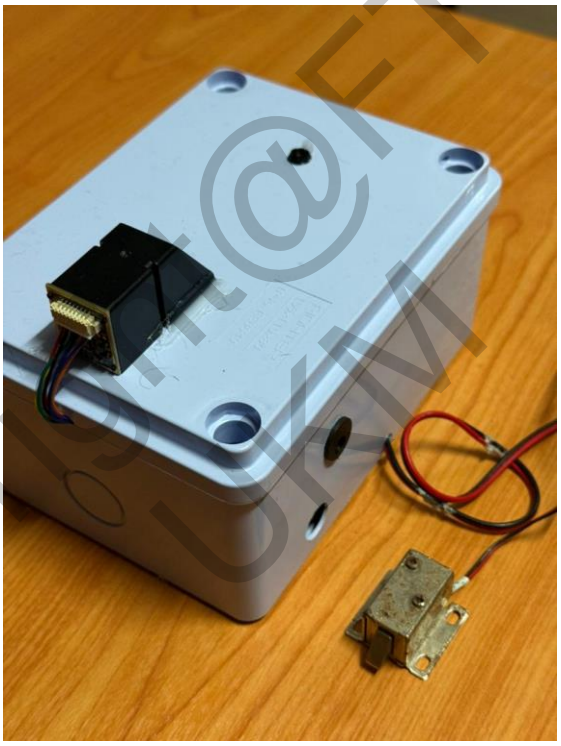
Rajah 5: Gambar Pengguna di Aplikasi Telegram

Rajah 5 menunjukkan selepas Cap Jari dikesan, Pentadbir akan mendapat notifikasi di Telegram dengan gambar pengguna di depan sistem kita.



Rajah 6: Halaman Akses Pintu dan Masa

Gambar 6 menunjukkan muka halaman membuka atau tidak memberi akses untuk membuka pintu serta mendapat informasi tentang masa dan tarikh gambar diterima, maksudnya pentadbir akan mendapat notifikasi sebegini serta masa dan tarikh pengguna cuba meletak cap jari depan sistem ini.



Rajah 7: Sistem yang berjaya dibina

Rajah 7 menunjukkan sistem yang telah dibina. Sistem ini telah dibina dengan semua komponen yang dinyatakan sepeti ESP32-CAM, Sensor Cap Jari, Buzzer dan aplikasi Telegram.

4.2 Pengujian Sistem

Pengujian sistem telah dijalankan di dalam persekitaran simulasi yang menyerupai pintu masuk ke bilik kebal bank sebenar. Modul-modul utama dalam sistem ini iaitu sensor cap jari

(Fingerprint R307), kamera ESP32-CAM, buzzer, serta fungsi penghantaran notifikasi gambar ke Telegram telah diaktifkan dan diuji secara bersepadu. Tujuan utama ujian ini adalah memastikan semua komponen berfungsi dengan baik secara integrasi, serta dapat bertindak balas terhadap input pengguna dalam masa nyata dengan stabil, selamat, dan boleh dipercayai.

Pengujian dilakukan secara manual. Untuk modul cap jari, tiga pengguna dengan ID cap jari berbeza digunakan. Dua orang pengguna telah didaftarkan sebagai pengguna sah, manakala seorang lagi tidak berdaftar di dalam sistem. Ketiga-tiga orang diminta mengimbas ibu jari masing-masing untuk memastikan sistem dapat membezakan pengguna sah dan tidak sah. Apabila cap jari sah diimbas, sistem merekod data pengesahan untuk tujuan audit keselamatan. Sekiranya percubaan tidak sah diulang beberapa kali, buzzer akan berbunyi dengan kuat sebagai isyarat amaran potensi percubaan pencerobohan.

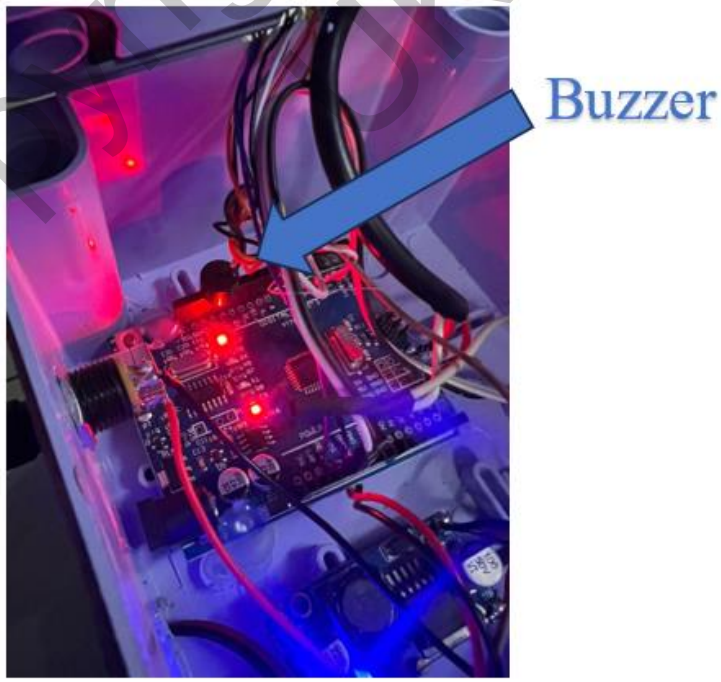
Rajah 8: Ujian Modul Cap Jari

Untuk modul kamera ESP32-CAM, ujian dilakukan dengan memastikan kamera mengambil gambar setiap kali cap jari diimbas, sama ada berjaya atau gagal, dan menghantar gambar tersebut ke Telegram bersama maklumat tarikh dan masa. Ini membantu pentadbir keselamatan menilai situasi secara jarak jauh dengan segera. Pengujian turut dijalankan untuk

memastikan mesej Telegram sampai tanpa kelewatan yang ketara.

Rajah 9: Ujian Modul Kamera ESP32-CAM

Ujian buzzer pula disimulasikan dengan beberapa percubaan akses gagal secara berturut-turut. Sistem diharap dapat mengaktifkan buzzer untuk memberi amaran kepada pegawai keselamatan bahawa terdapat cubaan memasuki vault secara tidak sah.



Rajah 10: Ujian Modul Buzzer

Semasa pengujian, beberapa aspek tambahan turut diperhatikan termasuk:

- Status sambungan Wi-Fi dan kestabilan rangkaian di kawasan sekuriti tinggi.
- Ketepatan tindak balas sistem terhadap pengesanan cap jari pengguna.
- Integriti dan kejelasan gambar yang dihantar oleh ESP32-CAM bersama tarikh dan masa.
- Kebolehpercayaan notifikasi Telegram untuk memantau setiap percubaan akses ke bilik kebal.

Setiap senario ujian dilaksanakan sekurang-kurangnya dua kali bagi memastikan konsistensi dan kebolehpercayaan. Sekiranya terdapat sebarang bacaan atau fungsi yang tidak selaras, pelarasan dilakukan pada kod atau konfigurasi perkakasan sebelum ujian diulangi. Keseluruhan proses ini membantu memastikan sistem keselamatan kawalan akses bilik kebal bank dapat beroperasi secara automatik, pantas, dan berkesan untuk perlindungan tahap tinggi.

Kesemua senario pengujian berjaya dilaksanakan dengan hasil yang konsisten dan mengikut jangkaan. Tiada masalah kritikal dikesan. Sistem juga menunjukkan prestasi yang stabil selepas beberapa jam operasi berterusan. Ujian membuktikan integrasi antara modul sensor cap jari, kamera ESP32-CAM, buzzer, serta komunikasi rangkaian ke Telegram adalah berfungsi sepenuhnya dan memenuhi keperluan keselamatan asas yang ditetapkan.

Jadual 1 Hasil Pengujian Kes Guna

ID Pengujian	ID Prosedur	Pengujian	Jangkaan Pengujian	Hasil Sebenar Pengujian	Status Pengujian
TC-01	TP-01-01	Kuasa hidup sistem	Sistem mula beroperasi dengan sambungan Wi-Fi stabil	Modul dihidupkan dan Wi-Fi bersambung seperti dijangka	Lulus
TC-02	TP-02-01	Imbas cap jari pengguna sah	Cap jari diterima dan disahkan, buka lock secara manual	Modul cap jari berjaya sahkan cap jari pengguna berdaftar	Lulus

	TP-02-02	Imbas cap jari pengguna tidak sah	Sistem menolak cap jari dan tidak buka pintu	Akses dinafikan seperti dijangka	Lulus
TC-03	TP-03-01	Percubaan akses gagal berulang	Buzzer berbunyi jika percubaan gagal berulang kali	Buzzer berbunyi kuat selepas 3 kali percubaan gagal	Lulus
TC-04	TP-04-01	Kamera aktif selepas imbasan	Kamera tangkap gambar & hantar ke Telegram	Gambar berjaya dihantar ke Telegram dengan masa & tarikh	Lulus
	TP-04-02	Paparan gambar di Telegram	Gambar jelas, waktu dan tarikh betul	Paparan Telegram tepat dan jelas	Lulus
TC-05	TP-05-01	Kestabilan sistem selepas 2 jam	Modul terus berfungsi tanpa ralat atau tergantung	Sistem berfungsi stabil selama tempoh ujian	Lulus
TC-06	TP-06-01	Sambungan Wi-Fi terganggu	Sistem cuba menyambung semula ke rangkaian	Sistem berjaya reconnect dalam 30 saat	Lulus

5.0 KESIMPULAN

Kesimpulannya, projek ini telah berjaya membangunkan sebuah sistem keselamatan pintu berasaskan teknologi biometrik cap jari yang diintegrasikan bersama modul kamera ESP32-CAM, buzzer, dan sistem notifikasi Telegram. Sistem ini menggunakan mikropengawal ESP32 sebagai pengawal utama, dengan sokongan modul pengimbas cap jari untuk kawalan akses yang selamat, serta kamera yang berupaya menghantar imej bersama masa dan tarikh setiap aktiviti akses ke Telegram. Projek ini telah diuji secara menyeluruh dalam persekitaran simulasi menyerupai bilik kebal sebenar dan menunjukkan prestasi stabil, dapat berfungsi secara masa nyata, serta mampu mengesan cubaan akses tidak sah dengan penghantaran notifikasi segera dan pengaktifan buzzer sekiranya percubaan berulang berlaku. Keunggulan utama projek ini ialah penggunaan teknologi kos efektif tetapi mampu mencapai tahap keselamatan yang tinggi, di samping ciri modular dan kebolehgunaan semula komponen. Sistem juga bersifat fleksibel untuk dikembangkan dengan modul tambahan seperti kamera HD, sensor getaran, atau sistem pengecaman wajah pada masa hadapan. Namun begitu,

terdapat beberapa kekangan sepanjang pembangunan projek, antaranya berkaitan aspek pendawaian dan konfigurasi rangkaian kamera, yang memerlukan ketelitian tambahan bagi memastikan kestabilan komunikasi antara ESP32 dan Telegram. Selain itu, peruntukan bajet yang terhad mengehadkan pembelian sensor tambahan untuk memperkukuhkan sistem keselamatan seperti sensor pintu terbuka/tutup atau sistem backup bateri. Walau bagaimanapun, sistem ini telah berjaya membuktikan kebolehfungsian yang baik dan sangat berpotensi untuk diaplikasikan dalam konteks keselamatan premis bernilai tinggi seperti bilik 106 kebal bank atau peti keselamatan korporat, sekali gus menjadi asas kukuh bagi pembangunan sistem keselamatan pintar berskala lebih besar pada masa hadapan.

6.0 PENGHARGAAN

Saya ingin merakamkan setinggi-tinggi kesyukuran kepada Tuhan atas rahmat dan kekuatan-Nya yang membolehkan saya menyelesaikan projek penyelidikan ini. Penghargaan saya juga ditujukan kepada penyelia saya, Prof. Dr. Rosilah Hassan, atas bimbingan, sokongan, dan nasihat yang sangat berharga sepanjang proses penyelidikan ini. Saya juga ingin mengucapkan terima kasih kepada Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia, atas kemudahan penyelidikan yang disediakan, serta kepada pihak pentadbiran fakulti yang memberi sokongan yang sangat membantu kelancaran penyelidikan ini.

Saya amat berterima kasih kepada ibu bapa saya atas doa dan sokongan moral yang tidak pernah putus sepanjang perjalanan akademik saya. Terima kasih juga kepada adik-beradik saya yang sentiasa memberi dorongan dan kekuatan kepada saya. Saya juga ingin mengucapkan terima kasih kepada Yuki Sabrina Nakaya dari Universitas Multimedia Nusantara, yang telah memberikan inspirasi, sokongan emosi, dan bantuan dalam menyediakan bahan-bahan yang diperlukan semasa menyiapkan projek ini.

Akhir sekali, penghargaan saya juga ditujukan kepada semua individu yang secara langsung atau tidak langsung telah memberikan bantuan dan galakan sepanjang perjalanan penyelidikan ini. Sokongan mereka sangat bermakna dan saya amat menghargai segala yang telah diberikan.

7.0 RUJUKAN

Ahmad, N., & Halim, A. R. A. (2022). "IoT-Based Smart Lock Systems for Residential Security." International Conference on Emerging Technologies in Engineering (ICETE).

Attariq Ziad, Eva Darnila & Kurniawati (2024) Development and Implementation of an ESP32 Microcontroller and Monitoring System for Smart Door Lock Using RFID Sensor for E-KTP ID and Fingerprint Based on the Internet of Things. MICoMS 2024. DOI: 10.29103/micoms.v4i.908

Bello, J., Umanah, A., & Sadiq, R. (2025). ESP32-CAM Module Facial Recognition Door Lock Security System. *ResearchGate*. Retrieved from https://www.researchgate.net/publication/389894228_ESP32-CAM_Module_Facial_Recognition_Door_Lock_Security_System

C. Sridhar Babu1 , Uttara Nanduri2 , G. Deepshikha 3 , Sai Sunidhi Pabba4 1Assistant Professor, Dept. of Electronics and Communications Engineering, G. Narayanamma Institute of Technology and Science, Telangana, India © 2023 IJNRD | Volume 8, Issue 4 April 2023 ISSN: 2456-4184 | IJNRD.ORG https://www.ijnrd.org/papers/IJNRD2304296.pdf

Dey, N., & Ashour, A. S. (2020). "Smart Home Security Using IoT: Concepts, Methods, and Future Directions." Journal of Security and Applications, 45, 102-115. Kajian Pustaka: Putu Eka Sumara Dita1, Ahmad Al Fahrezi2, Purwono Prasetyawan3, Amarudin4 1,2Teknik Komputer, Universitas Teknokrat Indonesia 3,4Teknik Elektro, Universitas Teknokrat Indonesia Jl. ZA. Pagar Alam No.9 -11, Labuhan Ratu, Bandar Lampung, Lampung putu.eka.sumara@teknokrat.ac.id1, ahmad.alfahrezi@teknokrat.ac.id2, purwono.prasetyawan@teknokrat.ac.id3, amarudin@teknokrat.ac.id4

Groover, M. P. (2019). Automation, Production Systems, and Computer-Integrated Manufacturing. Pearson Education.

Hamuda, H. (2025). Optimisation of ESP32 Cam based Smart Security…. Lovelace Journal of Information System, Security, Education and Network Artificial Intelligence, 1(1), 30–38.

Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to BIOMETRIKcs. Springer

Journal Of Technology || Issn No:1012-3407 || Vol 14 Issue 4 1Prof. Firoz Akhtar, 2Aditi Ghodeswar, 3Aqsa Khan, 4Adil Waghade, 5Sandesh Gajbhiye 1Assistant Professor,2Student,3Student,4Student,5Student. 1Electronics And Telecommunication Engineering Department, 1 J D College of Engineering and Management Nagpur, India https://technologyjournal.net/wp-content/uploads/3-JOT1257.pdf

Martin, J. (2018). IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. Cisco Press.

Permana, K. A., Piarsa, I. N., & Wiranatha, A. A. K. A. (2024)"IoT-Based Smart Door Lock System with Fingerprint and Keypad Access." Journal of Information Systems and Informatics, 6(3), 2086–2098.

Radzi, M., Saleh, R., & Afiq, M. (2020). Implementing Telegram in an IoT-Based Smart Door Control System. Journal of Electrical Engineering and Technology, 15(4), 507-513. Retrieved from https://journal.yrpipku.com/index.php/jaets/article/download/1042/738/6542

Rashid, S. (2020). "Data Centralization and Security in IoT Applications." Journal of Computer Science and Technology, 35(3), 560-573.

Siswanto, D., & Alfyandi, M. (2024). IoT-Based Smart Remote Door Lock and Monitoring System Using an Android Application. *ResearchGate*. Retrieved from https://www.researchgate.net/publication/385995025_IoT-Based_Smart_Remote_Door_Lock_and_Monitoring_System_Using_an_Android_Application

Smart Home Security System Using IoT https://www.scopus.com/record/display.uri?eid=2s2.085179841331&origin=resultslist&sort=plf f&src=s&sid=950a830242059b7c70252aba8529bec0&sot=b&sdt=b&s=TITLEABSEY%28smart+AND+door+AND+using+AND+BIOMETRIKc+AND+technology%9&sl=35&s essionSearchId=950a830242059b7c70252aba8529bec0&relpos=7

Suneetha, K., Venkatesh, M., & Shankar, S. (2025). IoT-Based Smart Door System with Fingerprint and Facial Recognition. *Papers.ssrn*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5205290

Syahri Ramadhani & Dhanny Permatasari Putri (2023) Design of a Home Door Security System Based on NodeMCU ESP32 Using a Magnetic Reed Switch Sensor and Telegram Bot Application. Sinkron: Jurnal dan Penelitian Teknik Informatika, 8(4). DOI: 10.33395/sinkron.v8i4.12688

Towards Wireless Spiking of Smart Locks Mohammed, A.Z. , Singh, A. , Dayanikli, G.Y. (2022) Proceedings - 43rd IEEE Symposium on Security and Privacy Workshops, SPW 2022

Wang, J., & Zhang, Y. (2021). "Design and Implementation of Real-Time Notification Systems Using IoT and Cloud Integration." IEEE Conference on Cloud Computing

Ziad, A., Darnila, E., & Kurniawati, (2024) “Development and Implementation of an ESP32 Microcontroller and Monitoring System for Smart Door Lock Using RFID Sensor for E KTP ID and Fingerprint Based on the Internet of Things.” MICoMS Conference Proceedings (2024).

YOGARASEN A/L MANIYARASAN (A205453)
PROF. DR. ROSILAH HASSAN
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia