SISTEM PENGESANAN PANCINGAN DATA MENGGUNAKAN PEMBELAJARAN MESIN CNN

[1]Nurul Hazwani Kamarudin, [1]Nazhatul Hafizah Kamarudin

[1]Fakulti Teknologi & Sains Maklumat
43600 Universiti Kebangsaan Malaysia

Abstrak

Masyarakat digital masa kini berdepan dengan ancaman serangan pancingan data (phishing) yang semakin kompleks dan sukar dikesan, terutamanya dalam memperoleh maklumat sensitif seperti kata laluan dan data kewangan. Sistem keselamatan tradisional seperti penapis spam dan pengesanan URL berbahaya sering kali tidak mencukupi dalam menangani serangan ini. Oleh itu, projek ini membangunkan Sistem Pengesanan Pancingan Data Menggunakan Pembelajaran Mesin, yang memanfaatkan kecerdasan buatan (AI) bagi meningkatkan keupayaan pengesanan ancaman pancingan secara lebih berkesan. Masalah utama yang dikenal pasti adalah ketidakmampuan sistem konvensional dalam mengenal pasti serangan baharu yang semakin canggih. Penyelesaian yang dicadangkan ialah pembangunan sistem berasaskan pembelajaran mesin menggunakan algoritma CNN untuk menganalisis corak komunikasi dan mengenal pasti elemen yang berpotensi menjadi ancaman phishing. Metodologi pembangunan menggunakan pendekatan Agile, yang merangkumi fasa pengumpulan dan pra-pemprosesan data, pembinaan serta ujian model, dan integrasi sistem. Hasil projek yang dijangka adalah sistem yang mampu memberikan amaran masa nyata, meningkatkan ketepatan pengesanan ancaman baharu, serta mengurangkan risiko kecurian data dan kerugian kewangan akibat serangan pancingan.

Abstract

In today's digital era, phishing attacks have become increasingly complex and difficult to detect, particularly in obtaining sensitive information such as passwords and financial data. Traditional security systems, such as spam filters and harmful URL detection, are often insufficient in mitigating these threats. Therefore, this project develops a Phishing Detection System Using Machine Learning, leveraging artificial intelligence (AI) to enhance phishing threat detection more effectively. The main issue identified is the inability of conventional systems to detect evolving and sophisticated phishing attacks. The proposed solution involves developing a machine learning-based system using the CNN algorithm to analyze communication patterns and identify potential phishing threats. The development methodology

follows the Agile approach, which includes data collection and preprocessing, model building and testing, and system integration. The expected outcome of this project is a system capable of providing real-time alerts, improving the accuracy of phishing threat detection, and reducing the risk of data theft and financial losses due to phishing attacks.

1.0 PENGENALAN

Pancingan data atau *phishing* merupakan ancaman keselamatan siber yang semakin serius pada era digital. Serangan ini biasanya dilakukan melalui e-mel, mesej segera, atau laman web palsu yang menyerupai laman sah untuk memperdaya mangsa menyerahkan maklumat sulit seperti kata laluan, nombor kad kredit, dan butiran peribadi. Ancaman ini memberi kesan besar kepada individu dan organisasi, termasuk kerugian kewangan, pencurian data, serta kerosakan reputasi. Statistik global menunjukkan peningkatan kes phishing selari dengan perkembangan teknologi yang memudahkan penjenayah siber melaksanakan serangan mereka.

Masalah utama dalam serangan phishing ialah kesukaran mengenal pasti laman atau mesej palsu kerana ia direka menyerupai laman rasmi. Tambahan pula, teknik moden seperti *domain spoofing*, *spear-phishing*, *smishing* dan *vishing* menjadikan serangan lebih sukar dikesan. Kaedah tradisional seperti penapis spam dan senarai hitam URL masih digunakan tetapi mempunyai kelemahan, terutamanya kebergantungan kepada pangkalan data yang memerlukan kemas kini berterusan serta kegagalan mengesan ancaman baharu atau *zero-day attack*.

Bagi menangani isu ini, projek ini membangunkan Sistem Pengesanan Pancingan Data menggunakan Convolutional Neural Network (CNN). CNN dipilih kerana keupayaannya mengenal pasti corak kompleks dalam URL dan memberikan klasifikasi dengan lebih tepat berbanding kaedah tradisional. Sistem ini dibangunkan sebagai aplikasi web dengan antara muka ringkas yang membolehkan pengguna memasukkan URL untuk dianalisis, menerima keputusan klasifikasi, serta menyemak semula sejarah URL yang pernah diuji. Objektif projek adalah membangunkan sistem pengesanan berasaskan CNN, menilai prestasinya menggunakan metrik standard, dan menyediakan antara muka mesra pengguna yang beroperasi secara masa nyata.

2.0 KAJIAN LITERATUR

Penyelidikan mengenai pengesanan pancingan semakin mendapat perhatian dalam era digital, sejajar dengan peningkatan ancaman siber yang menyasarkan pengguna individu dan organisasi. Teknologi berkaitan seperti pembelajaran mesin dan pembelajaran mendalam kini menjadi tumpuan utama dalam membangunkan sistem pengesanan yang lebih pintar dan cekap. Kajian terdahulu menekankan cabaran dalam mengesan serangan pancingan zero-day, yang memerlukan pendekatan inovatif untuk mengenal pasti laman web atau mesej yang mencurigakan. Dengan evolusi teknik serangan siber yang semakin kompleks, pendekatan seperti analisis heuristik, pengesanan visual, dan algoritma pembelajaran telah menjadi asas kepada sistem pengesanan moden.

Dalam kajian oleh Ashraf H. Aljammal et al. (2023) menggunakan algoritma Information Gain untuk pemilihan ciri dan menilai enam algoritma pembelajaran mesin seperti RandomForest, NaiveBayes, ANN, KNN, J48, dan DecisionStump. Kajian ini mendapati RandomForest memberikan ketepatan tertinggi iaitu sehingga 98% pada dataset besar, tetapi prestasi menurun pada dataset kecil. Pendekatan ini menunjukkan keupayaan pembelajaran mesin dalam pengesanan laman web pancingan, tetapi ia bergantung kepada ciri dan dataset yang mencukupi untuk prestasi maksimum.

Kajian terkini oleh Chen et al. (2024) memperkenalkan DA-HGNN (Data Augmentation Method and Hybrid Graph Neural Network) untuk menangani ketidakseimbangan data dalam graf transaksi Ethereum. Pendekatan ini menggabungkan Conv1D dan GRU-MHA untuk analisis temporal serta SAGEConv untuk memahami hubungan struktur graf. Sistem ini mencapai ketepatan yang luar biasa dengan AUC-ROC 0.994, tetapi memerlukan sumber pengiraan tinggi. Pendekatan ini mencerminkan trend terkini dalam penggunaan rangkaian neural graf untuk data kompleks dan dinamik.

Terdapat kajian lain yang mencadangkan sistem serangan pancingan berasaskan teknik pemprosesan bahasa semula jadi (NLP) untuk menganalisis kandungan teks e-mel secara semantik dan mengesan e-mel pancingan. Kajian tambahan membincangkan rangka kerja pengesanan laman web pancingan menggunakan pendekatan pembelajaran mendalam dan pengelas multilayer perceptron untuk mengklasifikasikan laman web sebagai pancingan, mencurigakan, atau sah. Walaupun masalah ini tidak secara eksplisit menganalisis pelbagai sistem atau teknologi yang sedang digunakan dalam industri atau penyelidikan semasa, ia memberikan gambaran mengenai pengelas pembelajaran mesin yang digunakan dalam kajian, termasuk NaiveBayes, ANN, DecisionStump, KNN, J48, dan RandomForest. Pengelas-pengelas ini digunakan secara meluas dalam industri dan penyelidikan untuk pelbagai aplikasi pembelajaran mesin, termasuk pengesanan serangan pancingan.

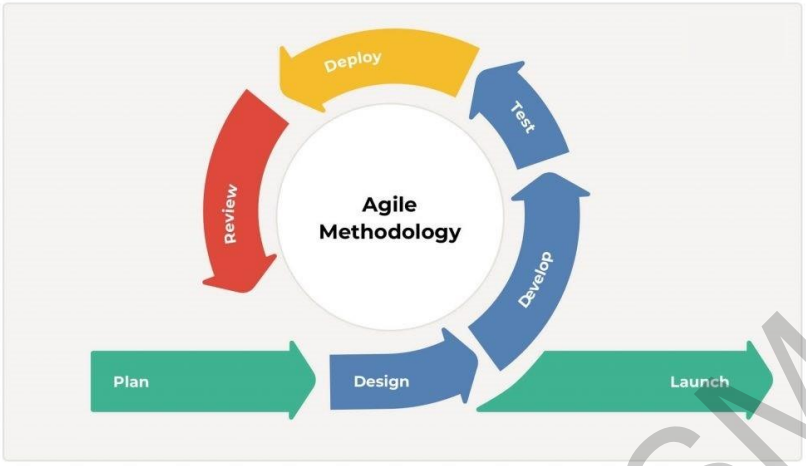
3.0 METODOLOGI

Bab ini membincangkan metodologi yang digunakan dalam pembangunan Sistem Pengesanan Pancingan Data menggunakan Convolutional Neural Network (CNN). Metodologi ini dirangka untuk memastikan sistem yang dibangunkan dapat memenuhi keperluan pengguna, memberikan keputusan klasifikasi dengan tepat, serta beroperasi secara stabil dan mesra pengguna. Pendekatan yang dipilih adalah pembangunan berasaskan model Agile yang fleksibel, disertai analisis keperluan sistem berdasarkan soal selidik, serta reka bentuk sistem yang melibatkan penyediaan rajah konseptual dan seni bina sistem.

3.1 Model Pembangunan Agile

Projek ini menggunakan model Agile kerana sifatnya yang fleksibel dan mampu menyesuaikan diri dengan perubahan, selaras dengan ancaman phishing yang sentiasa berkembang. Model ini dilaksanakan melalui beberapa kitaran sprint yang merangkumi fasa perancangan, pembangunan, pengujian dan penilaian. Pada peringkat awal, keperluan pengguna dikenal pasti melalui soal selidik dan kajian literatur sebelum digunakan sebagai panduan dalam pembinaan model CNN dan antaramuka pengguna berasaskan Flask.

Setiap modul diuji secara unit sebelum digabungkan ke dalam sistem penuh bagi memastikan fungsinya berjalan lancar. Fasa pengujian menilai fungsi input URL, ketepatan klasifikasi dan paparan hasil, manakala maklum balas pengguna digunakan untuk penambahbaikan. Proses iteratif ini membolehkan kelemahan dikesan lebih awal dan diperbaiki tanpa menjejaskan keseluruhan projek. Dengan pendekatan Agile, pembangunan sistem dapat dilakukan secara sistematik dan responsif terhadap perubahan, memastikan sistem akhir memenuhi objektif projek dan keperluan pengguna semasa.



Rajah 3.1 Model Agile

Rajah 3.1 menunjukkan model pembangunan agile ini diambil dari artikel di InterQuality. Model pembangunan Agile dipilih kerana sifatnya yang fleksibel serta sesuai dengan pembangunan sistem yang memerlukan penambahbaikan berterusan.

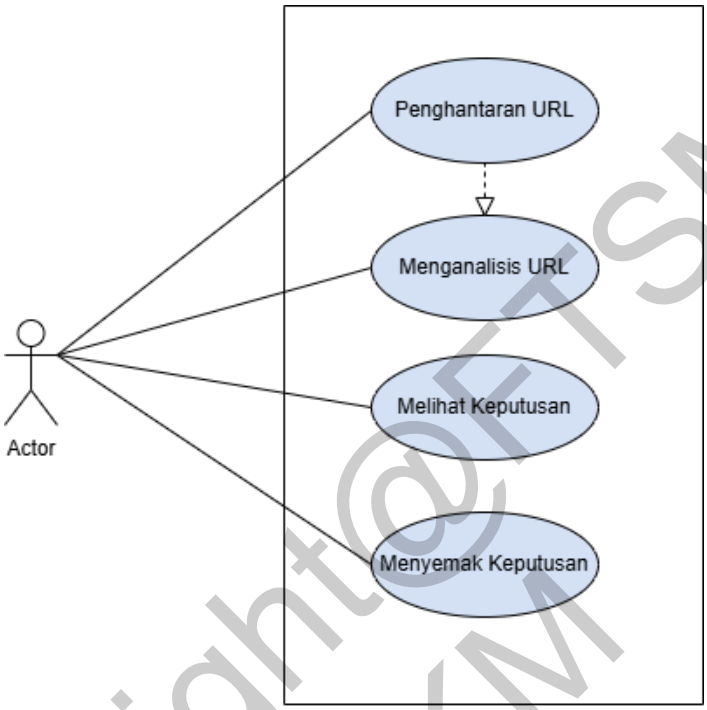
3.2 Keperluan Sistem

Keperluan sistem dikenal pasti melalui soal selidik yang dilaksanakan ke atas 25 responden bagi memahami keperluan dan tahap kesedaran pengguna terhadap ancaman phishing. Hasil tinjauan menunjukkan majoriti responden menekankan kepentingan sistem yang mudah digunakan, mesra pengguna, serta mampu memberikan keputusan dengan segera. Keperluan fungsian utama yang dikenalpasti ialah membolehkan pengguna memasukkan URL, menyemaknya melalui sistem, serta memaparkan keputusan klasifikasi sama ada URL tersebut selamat atau berbahaya. Selain itu, pengguna turut mengharapkan adanya fungsi sejarah semakan URL untuk memudahkan rujukan semula.

Dari segi keperluan bukan fungsian, pengguna menekankan aspek ketepatan dan kecekapan sistem. Mereka mahu keputusan diberikan secara masa nyata tanpa kelewatan, serta memerlukan antara muka yang jelas dan mudah difahami. Faktor keselamatan data turut diberi perhatian kerana pengguna bimbang tentang privasi apabila menghantar URL untuk dianalisis. Oleh itu, sistem direka untuk tidak menyimpan maklumat peribadi sensitif dan hanya merekodkan URL yang diuji jika perlu untuk tujuan log semakan.

Demografi responden memberikan gambaran jelas tentang kepelbagaian pengguna yang bakal menggunakan sistem ini. Sebahagian besar berusia antara 18 hingga 27 tahun, manakala selebihnya berusia 28 tahun ke atas. Dari segi pengetahuan, hanya sebilangan kecil responden

benar-benar mahir tentang phishing, manakala majoriti mempunyai pengetahuan asas atau sederhana. Menariknya, 20% daripada responden pernah menjadi mangsa serangan phishing, manakala 64% menyatakan kebimbangan yang tinggi tentang keselamatan dalam talian. Maklumat ini menunjukkan keperluan yang mendesak untuk sebuah sistem automatik yang mampu memberi amaran awal kepada pengguna. Justeru, pembangunan sistem ini dapat membantu pengguna biasa yang tidak mempunyai kepakaran teknikal melindungi diri mereka daripada ancaman phishing.



3.3 Reka Bentuk Sistem

Reka bentuk sistem ini menggunakan pendekatan seni bina berlapis yang merangkumi empat komponen utama iaitu antara muka pengguna, logik aplikasi, model CNN, dan pangkalan data. Antara muka berfungsi sebagai medium interaksi, membolehkan pengguna memasukkan URL dan menerima keputusan analisis. Logik aplikasi pula menguruskan aliran data daripada input pengguna ke model CNN, manakala pangkalan data menyimpan sejarah semakan untuk rujukan semula.

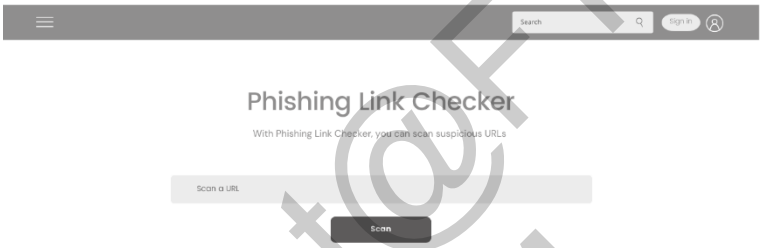
Rajah 3.3 menunjukkan rajah kes guna Sistem Pengesanan Pancingan Data Menggunakan Pembelajaran Mesin.

Model CNN direka dengan beberapa lapisan utama iaitu embedding untuk menukar URL kepada bentuk vektor, convolution untuk mengekstrak ciri penting, pooling untuk

Rajah 3.3 Rajah Kes Guna

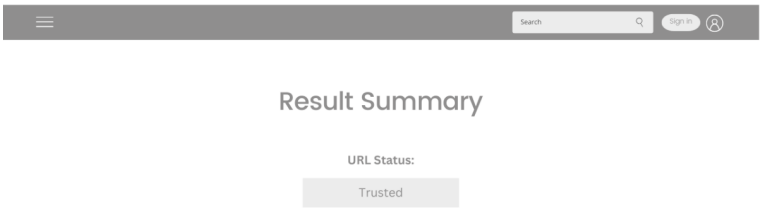
mengurangkan dimensi data, fully connected layer untuk pemprosesan lanjut, dan output sigmoid untuk menghasilkan keputusan akhir sama ada URL selamat atau phishing. Struktur ini membolehkan sistem mengenal pasti pola kompleks yang tidak dapat dikesan oleh kaedah tradisional, sekaligus meningkatkan ketepatan pengesanan.

Antara muka pengguna dibangunkan menggunakan Flask dengan reka bentuk ringkas dan mesra pengguna. Ia menyediakan ruangan input URL, paparan keputusan analisis yang jelas, serta senarai sejarah semakan bagi memudahkan pengguna membuat rujukan semula. Keputusan dipaparkan dalam mesej mudah difahami seperti “URL ini selamat” atau “Amaran: URL ini berpotensi sebagai phishing”, sekali gus meningkatkan pengalaman dan keyakinan pengguna semasa melayari internet.



Rajah 3.3.2 Rajah Muka Pengguna Menghantar URL

Rajah 3.3.3 Rajah Muka Pengguna Sistem Menganalisis URL



Rajah 3.3.4 rajah Muka Pengguna Menyemak Keputusan

4.0 HASIL

Bab ini membincangkan hasil pembangunan sistem pengesanan pancingan data yang dibangunkan menggunakan model Convolutional Neural Network (CNN). Perbincangan merangkumi proses pembangunan sistem yang dijalankan, serta pengujian dan penilaian prestasi untuk memastikan sistem berfungsi mengikut keperluan yang telah ditetapkan. Penilaian dilakukan melalui beberapa kaedah termasuk pengujian fungsi, prestasi, keselamatan, dan kebolehgunaan.

4.1 Pembangunan Sistem

Pembangunan sistem pengesanan pancingan data ini bermula dengan pengumpulan dataset daripada repositori keselamatan siber dan sumber terbuka. Dataset projek ini telah dibahagikan kepada dua bahagian utama iaitu set latihan sebanyak 80% dan set ujian sebanyak 20%. Model Convolutional Neural Network (CNN) dibangunkan menggunakan Keras dengan backend TensorFlow yang terdiri daripada lapisan embedding, convolution, pooling, fully connected serta output sigmoid. Proses latihan dijalankan secara berulang sehingga model mencapai tahap ketepatan yang tinggi dengan kehilangan (loss) yang rendah.

Setelah model mencapai prestasi yang memuaskan, proses integrasi dilakukan ke dalam sistem web menggunakan Flask. Integrasi ini membolehkan pengguna memasukkan URL melalui pelayar web dan menerima keputusan klasifikasi dalam masa nyata dengan pantas dan efisien.

Antara muka sistem direka bentuk secara ringkas dan mesra pengguna, menyediakan ruangan input URL, paparan keputusan analisis serta sejarah semakan. Keputusan dipaparkan dalam bentuk mesej yang jelas seperti "URL ini selamat" atau "Amaran: URL ini berpotensi sebagai phishing", bagi membantu pengguna membuat keputusan dengan yakin dan selamat.

4.2 Penilaian Sistem

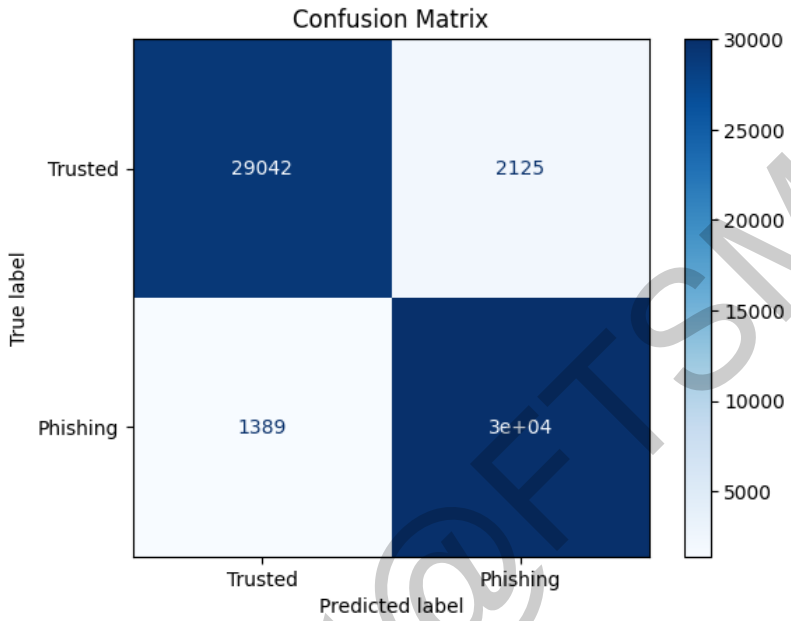
Pengujian sistem dijalankan secara menyeluruh untuk memastikan ketepatan, kestabilan, kepantasan, dan kebolehgunaan sistem. Strategi pengujian melibatkan ujian kotak hitam, ujian prestasi, ujian keselamatan, serta Ujian Penerimaan Pengguna (UAT). Melalui ujian kotak hitam, sistem berjaya mengklasifikasikan URL sah sebagai selamat dan URL phishing sebagai berbahaya dengan tahap ketepatan yang tinggi, membuktikan keupayaan sistem memenuhi keperluan fungsian utama.

Ujian prestasi menunjukkan sistem mampu memproses 50 URL berturut-turut dalam masa kurang daripada dua saat, membuktikan keberkesanan untuk kegunaan masa nyata. Ujian keselamatan turut dilaksana kan dengan memberi input berniat jahat atau tidak sah, dan sistem berjaya mengeluarkan mesej "Invalid URL" untuk menghalang eksploitasi, sekali gus menunjukkan tahap daya tahan sistem terhadap cubaan serangan input.

Ujian kebolehgunaan atau Ujian Penerimaan Pengguna (UAT) dilaksanakan melibatkan sekumpulan responden yang menilai kemudahan penggunaan sistem. Maklum balas yang diterima menunjukkan majoriti responden berpuas hati dengan antara muka yang ringkas, mudah difahami, serta keputusan analisis yang jelas. Lebih 70% responden menyatakan bahawa sistem ini memberi keyakinan tambahan kepada mereka dalam mengenal pasti pautan berisiko, manakala selebihnya menyarankan beberapa penambahbaikan dari segi reka bentuk visual.

Dari sudut prestasi model CNN, penilaian menggunakan metrik standard menunjukkan sistem mencapai ketepatan (Accuracy) sebanyak 94%. Nilai Precision dan Recall yang sama tinggi iaitu 0.94 membuktikan keseimbangan dalam pengesanan URL phishing dan URL selamat. Confusion Matrix yang dijana turut memperlihatkan taburan True Positive dan True Negative yang tinggi, menandakan model dapat meminimumkan kadar kesilapan. Graf Accuracy dan Loss sepanjang proses latihan menunjukkan kestabilan model tanpa berlaku overfitting, menandakan keupayaan model untuk menggeneralisasi data baharu dengan baik.
Secara keseluruhannya, keputusan pengujian membuktikan bahawa sistem yang dibangunkan berfungsi dengan baik, tepat dan stabil, selain memberi pengalaman pengguna yang positif. Gabungan pengujian fungsian, prestasi, keselamatan dan kebolehgunaan memastikan sistem ini bukan sahaja mampu mengesan serangan phishing dengan ketepatan tinggi, tetapi juga

praktikal untuk digunakan dalam situasi sebenar.



Rajah 4.2.1 Confusion Matrix

Kelas	Precision	Recall	F1-Score	Support
Trusted	0.95	0.93	0.94	31167
Phishing	0.93	0.96	0.94	31 402
Accuracy			0.94	62 569
Macro Avg	0.94	0.94	0.94	62 569
Weighted Avg	0.94	0.94	0.94	62 569

Rajah 4.2.2 menunjukkan menunjukkan laporan klasifikasi model CNN bagi mengesan URL trusted dan phishing. Model mencapai ketepatan keseluruhan accuracy sebanyak 94%, dengan nilai precision dan recall yang seimbang untuk kedua-dua kelas phishing dan trusted. Nilai F1-score juga konsisten pada 0.94, menunjukkan bahawa model ini mampu mengenal pasti pautan phishing dan selamat dengan tahap ketepatan yang tinggi dan seimbang.

5.0 KESIMPULAN

Rajah 4.2.2 Keputusan Ujian Dataset

Projek pembangunan Sistem Pengesanan Pancingan Data menggunakan CNN berjaya mencapai objektif dengan membangunkan sistem yang tepat, pantas dan mesra pengguna melalui integrasi aplikasi web berasaskan Flask. Sistem ini mencatatkan ketepatan 94% dengan masa respon kurang dua saat, serta menerima maklum balas positif daripada pengguna mengenai kemudahan penggunaan dan kejelasan keputusan. Mekanisme validasi input turut memastikan keselamatan sistem daripada eksploitasi. Walaupun begitu, sistem masih bergantung kepada dataset sedia ada dan boleh dipertingkatkan pada masa hadapan dengan penggunaan dataset lebih luas, algoritma pembelajaran mendalam yang lebih kompleks, serta integrasi amaran masa nyata bagi meningkatkan keberkesanan keselamatan siber.

6.0 PENGHARGAAN

Saya ingin berterima kasih kepada penyelia saya, Ts. Dr. Nazhatul Hafizah binti Kamarudin, atas segala tunjuk ajar, sokongan, serta dorongan yang diberikan sepanjang tempoh kajian ini. Setinggi-tinggi juga penghargaan buat kedua ibu bapa, keluarga dan rakan-rakan yang sentiasa memberi semangat dan dorongan sepanjang syaa menyelesaikan kajian ini.

7.0 RUJUKAN

Aljammal, A. H., taamneh , S. ., Qawasmeh, A. ., & Bani Salameh, H. (2023). Machine Learning Based Phishing Attacks Detection Using Multiple Datasets. International Journal of Interactive Mobile Technologies (iJIM), 17(05), pp. 71–83. https://doi.org/10.3991/ijim.v17i05.37575

Alshingiti, Z.; Alaqel, R.; Al-Muhtadi, J.; Haq, Q.E.U.; Saleem, K.; Faheem, M.H. A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN. Electronics 2023, 12, 232. https://doi.org/10.3390/electronics12010232

Claire Drumond. (2024). Agile Project Management - What is it and how to get started?, Atlassian. https://www.atlassian.com/agile/project-management

GeeksforGeeks. (2024). Agile Software Development – Software Engineering, GeeksforGeeks. https://www.geeksforgeeks.org/software-engineering-agile-software-development/?ref=header_outind

I. Saha, D. Sarma, R. J. Chakma, M. N. Alam, A. Sultana, and S. Hossain, "Phishing Attacks Detection using Deep Learning Approach," in 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 2020, pp. 1180-1185. https://doi.org/10.1109/ICSSIT48917.2020.9214132

Jaiswal, S. (2025) Understanding Layered Architecture: A Comprehensive guide. *Medium*. https://medium.com/@satyendra.jaiswal/understanding-layered-architecture-a-comprehensive-guide-4c2eee374d18/

Jnguyen. (2022). *What is Phishing? Types of Phishing Attacks*. Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/

Laoyan, S. (2024). What is Agile Methodology? (A Beginner's Guide) [2024] • Asana. *Asana*. https://asana.com/resources/agile-methodology

Masas, R. (2023). *What is phishing | Attack techniques & scam examples | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/phishing-attack-scam/

OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. (n.d.). https://owasp.org/

Rahman, M. (2024). Different ways to combine CNN and LSTM networks for time series classification tasks. *Medium*. https://medium.com/@mijanr/different-ways-to-combine-cnn-and-lstm-networks-for-time-series-classification-tasks-b03fc37e91b6

Roy, S.S.; Awad, A.I.; Amare, L.A.; Erkihun, M.T.; Anas, M. (2022) Multimodel Phishing Url Detection Using Lstm, Bidirectional Lstm, and Gru Models. Future Internet 14, 340. https://doi.org/10.3390/fi14110340

Shanice. (2024). *URL Phishing: What it is, Real world Examples & Strategies - Valimail*. Valimail -. https://www.valimail.com/resources/guides/guide-to-phishing/url-phishing-real-world-examples-strategies/

Sultan Asiri et al. (2024) PhishingRTDS: A Real-time Detection System for Phishing Attacks Using a Deep Learning Model. *Computers & Security*, *141*, 103843–103843. https://doi.org/10.1016/j.cose.2024.103843

Tiwari, T. (2021). *Phishing site URLs*. Kaggle. https://www.kaggle.com/datasets/taruntiwarihp/phishing-site-urls

Wayburn, J. (2024). *Phishing detection: Identifying phishing emails and websites* [Video]. Perception Point. https://perception-point.io/guides/phishing/phishing-detection-identifying-phishing-emails-and-websites/

What is agile? - Hygger.io guides. (2018). Hygger.io Guides. https://hygger.io/guides/agile/

Woollacott, E. (2024). What is phishing? Understanding Cyber attacks. *Forbes*. https://www.forbes.com/sites/technology/article/what-is-phishing/

Nurul Hazwani Kamarudin (A193929)
Dr. Nazhatul Hafizah Kamarudin
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia