SEDARNET: SISTEM PENGESANAN ANCAMAN RANGKAIAN

MUHAMMAD RUSYDAN ADNEEN BIN ABU SEMAN

NUR HANIS SABRINA SUHAIMI

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

ABSTRAK

Projek ini bertujuan untuk membangunkan Sistem Pengesanan Ancaman Rangkaian Wi-Fi dengan mengubahsuai Jam Deauth ESP8266 bagi meningkatkan keselamatan pengguna dalam persekitaran rangkaian tanpa wayar. Projek ini memberi tumpuan kepada pengesanan tiga jenis ancaman utama iaitu pengesanan rangkaian Wi-Fi palsu, pengesanan serangan deautentikasi dan pengesanan isyarat rangkaian Wi-Fi yang lemah. Masalah utama yang dikenal pasti adalah risiko keselamatan siber terhadap rangkaian Wi-Fi. Beberapa aduan telah diterima mengenai rangkaian Wi-Fi yang tidak stabil, menyebabkan gangguan kepada pelajar dan pensyarah semasa sesi pembelajaran atas talian. Perkara ini boleh memberikan implikasi buruk jika hal ini dipandang remeh kerana jika rangkaian Wi-Fi yang mereka sedang gunakan itu merupakan rangkaian Wi Fi yang tidak selamat akan mendatangkan konsekuensi buruk seperti serangan siber. Objektif projek ini amat jelas dimana untuk mengenal pasti parameter yang diperlukan untuk pengubahsuaian Jam Deauther ESP8266 bertujuan mengesan ancaman rangkaian Wi-Fi ini dan difokuskan di kawasan kolej Universiti Kebangsaan Malaysia. Metodologi pembangunan melibatkan fasa reka bentuk seni bina berlapis, pengaturcaraan algoritma pengesanan ancaman dan ujian dalam persekitaran terkawal. Hasil yang dijangkakan ialah satu peranti mudah alih yang mampu memantau rangkaian W-Fi secara proaktif, mengurangkan risiko serangan siber dan juga meningkatkan kesedaran pengguna terhadap keselamatan rangkaian. Sistem ini diharap dapat menjadi penyelesaian praktikal untuk semua lapisan pengguna terutamanya di kawasan universiti.

Kata Kunci : ESP8266 Deauther, Serangan Deautentikasi, Wi-Fi Palsu, Pengesanan Ancaman, Keselamatan Rangkaian Wi-Fi

ABSTRACT

This project aims to develop a Wi-Fi Network Threat Detection System by modifying the ESP8266 Deauther Watch to enhance user safety in wireless network environments. The project focuses on detecting three main types of threats: fake Wi-Fi networks, deauthentication attacks, and weak Wi-Fi signal strength. The primary problem identified is the cybersecurity risk posed to Wi-Fi networks. Several complaints have been received regarding unstable Wi-Fi connections, causing disruptions to students and lecturers during online learning sessions. This issue could have serious implications if neglected, as using an unsecured Wi-Fi network may lead to harmful consequences such as cyberattacks. The project's objective is clear which is to identify the parameters required to modify the ESP8266 Deauther Watch to detect these Wi-Fi threats, with a focus on the Universiti Kebangsaan Malaysia college area. The development methodology involves layered architecture design, threat detection algorithm programming and testing in a controlled environment. The expected outcome is a portable device capable of proactively monitoring Wi-Fi networks, reducing the risk of cyberattacks and increasing user awareness of network security. This system is intended to be a practical solution for all levels of users, particularly in university environments.

Keywords: ESP8266 Deauther, Deauthentication Attack, Fake Wi-Fi, Threat Detection, Wi-Fi Network Security

PENGENALAN

Teknologi hujung jari memberikan manfaat besar kepada pelajar dan pensyarah dalam kehidupan seharian, terutama dalam persekitaran pembelajaran atas talian. Wi-Fi telah menjadi keperluan asas, namun, ketiadaan akses Wi-Fi yang stabil sering mengganggu kelancaran komunikasi dan pembelajaran. Namun, ketiadaan akses Wi-Fi yang stabil atau gangguan yang tidak dijangka boleh menghalang aktiviti harian, terutama dalam penggunaan aplikasi pembelajaran atas talian. Dalam beberapa kes, masalah ini boleh menjadi lebih serius apabila rangkaian diserang, menyebabkan kehilangan akses Wi-Fi atau ancaman terhadap data pengguna.. Untuk mengatasi masalah ini, projek ini bertujuan untuk mengubahsuai peranti ESP8266 Deauther, yang asalnya digunakan untuk serangan, menjadi alat pengesan serangan rangkaian yang dapat menganalisis dan memberi amaran mengenai masalah Wi-Fi yang berpotensi berlaku. Selain itu, serangan siber terhadap rangkaian Wi-Fi semakin menjadi perhatian utama dalam kalangan pengguna, terutama di institusi pengajian tinggi. Serangan

deautentikasi dan pencerobohan rangkaian boleh menyebabkan gangguan yang serius terhadap aktiviti harian pelajar dan pensyarah, serta menjejaskan keselamatan data yang dihantar melalui rangkaian tersebut.

KAJIAN LITERATUR

Pelbagai penyelidikan telah dijalankan untuk membangunkan sistem pengesanan ancaman rangkaian berskala kecil menggunakan teknologi kos rendah seperti ESP8266. Athira Remesh et al. (2020) membangunkan sistem pengesanan pencerobohan berasaskan ESP8266 untuk IoT yang praktikal dan ringan, namun terhad dari segi prestasi pada rangkaian trafik tinggi.

Ananay Arora (2020) pula menggunakan teknik pencincangan SHA512 dan Pengenal Unik Unit Sejagat untuk pengesahan, yang berkesan tanpa memerlukan pengubahsuaian perkakasan, tetapi kurang sesuai untuk rangkaian trafik tinggi atau kompleks. Poudel (2020) memanfaatkan Python dan Scapy untuk analisis masa nyata yang mudah dan boleh dipercayai pada rangkaian kecil, namun prestasinya menurun pada rangkaian bersaiz besar.

Dalam skala lebih besar, Fanglu Guo et al. (2023) menerapkan pembelajaran mendalam berasaskan CNN dan pembelajaran pemindahan untuk pengesanan ancaman dengan ketepatan tinggi, tetapi memerlukan kuasa pemprosesan besar yang tidak sesuai untuk peranti sumber rendah. Poltak Sihombing et al. (2019) pula menggunakan pengesahan berterusan berasaskan data RSSI yang berkesan dengan sumber minimum, walaupun sukar digunakan dalam persekitaran yang sangat terganggu.

Bagi projek SedarNet, ESP8266 diubah suai untuk mengesan serangan Wi-Fi seperti deautentikasi dan Wi-Fi palsu. Pendekatan ini kos efektif, ringkas dan sesuai untuk rangkaian berskala kecil, namun terhad oleh kekangan perkakasan sedia ada.

METODOLOGI KAJIAN

Metodologi yang digunakan dalam pembangunan projek ini ialah Waterfall. Beberapa model telah saya teliti. Setelah beberapa faktor yang telah saya ambil kira, saya membuat keputusan untuk menggunakan model Waterfall. Hal ini kerana ianya ringkas, berurutan dan mudah untuk diikuti.

Fasa Analisis Dan Keperluan

Pada peringkat awal analisis dan penentuan keperluan, adalah penting untuk mengenal pasti keperluan teras sistem bagi memastikan pembangunan sistem mencapai objektif yang ditetapkan. Keperluan utama termasuk kebolehan untuk mengesan serangan rangkaian, memberi amaran kepada pengguna, serta merekodkan insiden keselamatan. Selain itu, maklumat teknikal seperti piawaian Wi-Fi dan struktur paket data perlu dikumpulkan bagi menyokong pembangunan fungsi pengesanan secara tepat dan berkesan.

Fasa reka bentuk

Pada fasa reka bentuk, ianya akan meliputi cara alat akan menghidu paket, pengesanan dan mekanisme amaran, gambar rajah akan dibuat bagi menggambarkan cara sistem itu akan berfungsi.

Fasa pelaksanaan

Pada fasa pelaksanaan pula, proses pengekodan sistem akan dimulakan dan akan mula memfokuskan kepada menyediakan alat dalam mod rambang untuk menangkap paket Wi-Fi. Di sini juga algoritma pengesanan akan dibangunkan untuk mengenal pasti bingkai deautentikasi. Antara muka pengguna dan sistem pemberitahuan juga akan dilaksanakan. Kod firmware ditulis dalam Arduino IDE menggunakan bahasa C++. Fungsi penting termasuk scanWiFiNetworks(), runThreatDetection(), promiscuousCallback() dan displayThreat() telah dibangunkan.

Fasa pengujian

Fasa pengujian bertujuan untuk memastikan sistem SedarNet berfungsi dengan betul dan memenuhi keperluan keselamatan serta kebolehgunaan seperti yang telah ditetapkan. Dalam pengujian unit, setiap fungsi utama seperti pengesanan serangan deauth, pengesanan Wi-Fi palsu, dan amaran isyarat lemah diuji secara berasingan untuk mengenal pasti sebarang ralat. Pengujian ini dijalankan menggunakan persekitaran simulasi dengan bantuan alat seperti aireplay-ng dan airbase-ng bagi menghasilkan senario serangan sebenar terhadap sistem.

Seterusnya, pengujian integrasi dilakukan bagi memastikan semua komponen sistem seperti paparan OLED, butang kawalan, dan logik pengesanan ancaman berfungsi secara serentak dengan lancar. Pengujian ini juga melibatkan pemantauan kestabilan sistem dalam jangka

masa penggunaan yang panjang serta pengesahan tindak balas sistem terhadap pelbagai jenis rangkaian.

Selain itu, pengujian tidak fungsi dijalankan untuk menilai prestasi sistem dari aspek masa tindak balas, kecekapan penggunaan memori, dan kemesraan pengguna. Penilaian dilakukan berdasarkan ketepatan mesej amaran, kejelasan paparan, dan kebolehan pengguna mengendalikan sistem tanpa latihan teknikal. Kesemua pengujian ini memastikan sistem SedarNet berupaya memberikan amaran awal yang berkesan terhadap ancaman rangkaian dalam persekitaran kampus secara masa nyata dan tanpa sambungan Internet.

Fasa Kerahan

Fasa kerahan ini ialah sistem akan digunakan untuk ujian lanjut dalam senario atau kes yang sebenar dan berkongsi kepada orang lain untuk mendapatkan maklum balas. Ianya juga akan memastikan ia mesra pengguna dan beroperasi dengan berkesan.

Fasa Penyelenggaraan dan Penilaian

Di fasa terakhir ini iaitu fasa penyelenggaraan dan penilaian iaitu selepas penggunaan sistem itu, ianya akan terus dipantau untuk sebarang kemungkinan isu yang timbul. Maklum balas akan segera dikumpul daripada pengguna dan sebarang kemas kini yang perlu akan dibuat. Model Waterfall juga menggalakkan kerja yang tersusun dan teratur. Ia memudahkan untuk kita memahami dan mengatur tugasan. Ianya juga membantu mengurus tugas dan tarikh akhir dengan lebih berkesan. Selain itu, ia menggalakkan amalan pengekodan yang baik dengan mereka bentuk sebelum pengekodan.

KEPUTUSAN DAN PERBINCANGAN

Sistem SedarNet telah berjaya dibangunkan dan diuji dalam persekitaran sebenar bagi mengenal pasti ancaman rangkaian Wi-Fi seperti serangan deauthentication, kewujudan Wi-Fi palsu dan isyarat lemah. Hasil pengujian menunjukkan bahawa sistem berfungsi dengan berkesan serta mampu memberikan amaran kepada pengguna dalam masa nyata. Tiga bentuk ancaman yang diuji memberikan hasil seperti berikut:

1) Pengesanan Serangan Deautentikasi

Sistem berjaya mengenal pasti bingkai 0xC0 yang dihantar menggunakan aireplay-ng. Apabila nilai ambang serangan (seperti ditetapkan 5 bingkai) dicapai, paparan OLED secara automatik memaparkan mesej amaran “Deauth Attack!” dan meminta pengguna agar berhenti menyambung ke rangkaian tersebut.

Gambar 1 Pengesanan Serangan Deautentikasi

2) Pengesanan Wi-Fi Palsu

Dalam ujian menggunakan airbase-ng untuk mencipta Wi-Fi palsu dengan SSID yang sama tetapi BSSID berbeza, sistem dapat mengenal pasti kewujudan AP mencurigakan melalui logik perbezaan BSSID dan kekuatan isyarat. Mesej “Fake Wifi Detected!” dipaparkan sebagai amaran kepada pengguna.

Gambar 2 Pengesanan Wi-Fi Palsu

3) Pengesanan Isyarat Lemah

Sistem berjaya mengesan rangkaian dengan RSSI di bawah nilai ambang -80 dBm. Dalam ujian ini, sistem memaparkan mesej “Weak Signal!”, menasihatkan pengguna untuk menyemak lokasi atau kekuatan isyarat sambungan Wi-Fi.

Gambar 3 Pengesanan Isyarat Lemah

4) Wi-Fi Selamat

Jika tiada ancaman dikesan, sistem akan memaparkan mesej “This WiFi is Safe / OK”. Hal ini menunjukkan bahawa logik kendalian normal sistem juga berfungsi dengan stabil.

Gambar 4 Pengesanan Wi-Fi Selamat

Cadangan Penambahbaikan

Bagi meningkatkan keupayaan sistem SedarNet agar lebih menyeluruh dan sesuai digunakan dalam dunia sebenar, beberapa penambahbaikan telah dikenal pasti. Antara cadangan utama termasuklah menambah fungsi penyimpanan log untuk merekod sejarah ancaman, membolehkan analisis risiko dan pemantauan trend rangkaian secara berterusan. Selain itu,

penerapan kecerdasan buatan seperti pembelajaran mesin juga dicadangkan bagi mengklasifikasikan ancaman dan menetapkan ambang secara automatik dan mengurangkan mesej amaran palsu. Tambahan pula, sokongan kepada platform lain seperti ESP32 dan reka bentuk fizikal yang lebih tahan lasak akan membolehkan sistem ini digunakan di lebih banyak lokasi termasuk luar bangunan. Kesemua cadangan ini bertujuan menjadikan SedarNet sebuah sistem pemantauan keselamatan rangkaian yang lebih berskala dan praktikal.

KESIMPULAN

Secara keseluruhannya, sistem SedarNet telah berjaya dibangunkan dengan menggunakan pendekatan perkakasan dan perisian bersepadu yang memenuhi keperluan yang telah ditetapkan dalam objektif kajian. Sistem ini mampu mengesan ancaman rangkaian seperti serangan deautentikasi, Wi-Fi palsu, dan isyarat lemah secara masa nyata, tanpa memerlukan sambungan internet atau pelayan luaran. Walaupun terdapat beberapa cabaran dari segi konfigurasi teknikal dan kekangan perkakasan, kesemua isu tersebut berjaya diatasi melalui proses pembangunan yang berperingkat. Diharapkan SedarNet dapat menjadi titik permulaan bagi kajian dan inovasi selanjutnya dalam bidang keselamatan rangkaian bersaiz kecil.

Kekuatan Sistem

Kekuatan utama SedarNet terletak pada keupayaannya untuk beroperasi secara kendiri tanpa memerlukan sambungan ke pelayan luaran, sekali gus menjadikannya sesuai untuk digunakan di kawasan tanpa liputan internet. Sistem ini juga mudah digunakan oleh pengguna biasa kerana antara mukanya yang ringkas dan mesej amaran yang jelas dipaparkan melalui paparan OLED. Dari segi pembangunan, projek ini menunjukkan keberkesanan dalam memanfaatkan modul ESP8266 dan fungsi mod rambang bagi mengesan paket rangkaian dengan kos pembangunan yang rendah. Tambahan pula, butang kawalan fizikal memberikan navigasi yang stabil sepanjang penggunaan sistem.

Kelemahan Sistem

Antara kelemahan yang dikenal pasti ialah ketiadaan storan log yang menghalang pengguna daripada merekod dan menjejak sejarah ancaman yang telah dikesan. Selain itu, sistem ini bergantung sepenuhnya kepada tindak balas pengguna secara manual terhadap mesej amaran kerana tiada integrasi dengan peranti lain seperti telefon pintar. Dari segi pembangunan pula,

kekangan seperti ruang memori yang terhad serta had fungsi pada ESP8266 menjadikan sistem sukar untuk ditambah baik secara besar-besaran tanpa pengoptimuman lanjut. Walau bagaimanapun, semua kekangan ini telah dikenal pasti dan boleh diatasi melalui cadangan penambahbaikan yang dicadangkan pada fasa pembangunan masa hadapan.

PENGHARGAAN

Penulis ingin merakamkan setinggi-tinggi penghargaan yang tulus ikhlas dan setulus budi kepada penyelia yang dikasihi, Dr. Hanis Sabrina Suhaimi atas segala curahan ilmu, tunjuk ajar yang tidak pernah putus, serta bimbingan penuh hikmah sepanjang perjalanan projek ini. Bagaikan pelita yang menerangi dalam kegelapan, nasihat dan dorongan beliau telah menjadi panduan utama dalam menempuh setiap cabaran hingga membawa kepada kejayaan yang bermakna. Segala jasa dan bakti beliau akan sentiasa terpahat dalam ingatan dan sanubari penulis sebagai sumber inspirasi yang abadi.

Penulis kajian ini turut merakamkan setinggi-tinggi penghargaan dan terima kasih kepada semua pihak yang telah memberikan bantuan, sama ada secara langsung mahupun tidak langsung, dalam menjayakan projek ini. Segala bentuk sokongan, dorongan, dan pertolongan yang dihulurkan amatlah dihargai dan menjadi penyumbang penting kepada kelancaran pelaksanaan kajian ini. Semoga segala jasa baik tersebut diberkati dan dibalas dengan sebaik-baik ganjaran oleh Tuhan Yang Maha Esa.

RUJUKAN

Arora, A. (2018). Preventing wireless deauthentication attacks over 802.11 networks. arXiv preprint arXiv:1901.07301. https://arxiv.org/abs/1901.07301 Diakses pada 10 Oktober 2024.

CiferTech. (2024). How to Detect Deauth Attacks Using ESP8266. https://cifertech.net/detect-deauth-attacks-on-wi-fi-network-using-esp8266 Diakses pada 10 April 2025.

Cisco Systems, Inc. (2016). *Wireless Signal Strength Basics*. Retrieved July 28, 2025, from https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116057-sitesurvey-guidelines-wlan-00.html

CyberSecurity Malaysia. (n.d.). Curb hacking by only using secured WiFi connection. The Sun Daily. https://thesun.my/malaysia-news/cybersecurity-malaysia-curb hacking-by-only-usingsecured-wifi-connection-BC9334627 Diakses pada 10 Mei 2025.

draw.io. (n.d.). Draw.io - Free flowchart maker and diagrams online. https://draw.io/ Diakses pada 18 Mei 2025.

Gebresilassie, S. K., Rafferty, J., Chen, L., Cui, Z., & Abu-Tair, M. (2023). Transfer and CNN-based de-authentication (disassociation) DoS attack detection in IoT. Electronics, 12(3731). https://www.mdpi.com/2079-9292/12/17/3731 Diakses pada 15 Jun 2025.

Ghorbani, A. A., et al. (2010). Network attacks. In Network Intrusion Detection and Prevention: Concepts and Techniques (pp. 1–25). Diakses pada 22 Oktober 2024.

Long, M., Wu, C.-H., & Hung, J. Y. (2005). Denial of service attacks on network-based control systems: impact and mitigation. IEEE Transactions on Industrial Informatics, 1(2), 85–96. Diakses pada 1 November 2024.

Lutkevich, B., & Lewis, S. (2022, November 14). Waterfall model. Software Quality. https://www.techtarget.com/searchsoftwarequality/definition/waterfall-model Diakses pada 5 Disember 2024.

Poudel, R. (2020). Practically detecting WiFi deauthentication attack, 802.11 deauth packets using Python and Scapy [Technical Report]. https://www.researchgate.net/publication/343472668_Practically_Detecting_ WiFi_Deauthentication_Attack_80211_Deauth_Packets_using_Python_and_S capy Diakses pada 15 Januari 2025.

Ramadevi, P., Manikandan, B., & Jayasankar, T. (2022). Implementing a continuous authentication protocol to improve robustness against security threats on IoT using ESP8266. International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), 10(10). https://www.researchgate.net/publication/366257509_An_Implementing_A_C

ontinuous_Authentication_Protocol_To_Improve_Robustness_Security_Threats_On_IoT_Using_ESP8266 Diakses pada 22 Januari 2025.

Remesh, A., Muralidharan, D., Raj, N., Gopika, J., & Binu, P. K. (2020). Intrusion detection system for IoT devices. Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC 2020). https://www.researchgate.net/publication/343438698_Intrusion_Detection_System_for_IoT_Devices Diakses pada 2 Mei 2025.

Saranya, L., Reddy, R. V., Reddy, A. B., Dinesh, B. S., & Muneeruddin, M. (2024). Detect Wi-Fi de-authentication attacks using ESP8266. International Journal of Engineering Research & Technology (IJERT), 13(03). https://www.ijert.org/detect-wi-fi-de-authentication-attacks-using-esp8266 Diakses pada 15 April 2025.

SecurityBoat Workbook. (2024). Wi-Fi Deauther - SecurityBoat Workbook. https://workbook.securityboat.net/Pentesting/Physical/NodeMCU%20ESP8266/WiFi%20Deauther Diakses pada 8 Februari 2025.

Sihombing, P., Manullang, M., Sitompul, D., & Dumayanti, I. S. (2019). The heart attack detection by ESP8266 data communication at a real time to avoid sudden death. Journal of Physics: Conference Series, 1235(012044). https://iopscience.iop.org/article/10.1088/1742-6596/1235/1/012044/pdf Diakses pada 28 Februari 2025.

SpacehuhnTech. (t.t.h.). Detect Deauthentication Frames Using an ESP8266. https://github.com/spacehuhn/DeauthDetector Diakses pada 14 Februari 2025.

Muhammad Rusydan Adneen Bin Abu Seman(A196071)
Ts. Dr. Nur Hanis Sabrina Suhaimi
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia