ANALISIS POLA HASIL PENETRATION TESTING DENIAL OF SERVICE, MAN-IN-THE-MIDDLE, BRUTE FORCE, DAN SQL INJECTION PADA SISTEM DISASTER RECOVERY CENTER (DRC) MENGGUNAKAN METODE K-MEANS CLUSTERING

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH:

ARMANDA FATHURRAHMAN
09011282126055

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2025

AUTHENTICATION PAGE

SKRIPSI

PATTERN ANALYSIS OF PENETRATION TESTING RESULTS FOR DENIAL OF SERVICE, MAN-IN-THE-MIDDLE, BRUTE FORCE, AND SQL INJECTION ATTACKS ON A DISASTER RECOVERY CENTER (DRC) SYSTEM USING THE K-MEANS CLUSTERING METHOD

As one of the requirements for completing the Bachelor's

Degree Program in Computer Systems

By:

ARMANDA FATHURRHAMAN

09011282126055

Supervisor 1	:	**Dr. Ir. Ahmad Heryanto, M.T.**
		NIP. 198701222015041002
Supervisor 2	:	**Adi Hermansyah, S.Kom., M.T.**
		NIP. 198904302024211001

Approved by,

Head of Computer System Department

Dr. Ir. Sukemi, M.T
196612032006041001

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS POLA HASIL PENETRATION TESTING DENIAL OF SERVICE, MAN-IN-THE-MIDDLE, BRUTE FORCE, DAN SQL INJECTION PADA SISTEM DISASTER RECOVERY CENTER (DRC) MENGGUNAKAN METODE K-MEANS CLUSTERING

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

ARMANDA FATHURRHAMAN

09011282126055

Pembimbing 1	:	**Dr. Ir. Ahmad Heryanto, M.T.**
		NIP. 198701222015041002
Pembimbing 2	:	**Adi Hermansyah, S.Kom., M.T.**
		NIP. 198904302024211001

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T
196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at

Tanggal : 25 Juli 2025

Tim Penguji :

1. **Ketua** : **Prof. Deris Stiawan, S.Kom., M.T., Ph.D**
2. **Penguji** : **Yoppy Sazaki, M.T.**
3. **Pembimbing I** : Dr. Ir. Ahmad Heryanto, M.T.
4. **Pembimbing II** : Adi Hermansyah, S.Kom., M.T.

Mengetahui, 27/8/25

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	:	Armanda Fathurrahman
NIM	:	09011282126055
Judul	:	Analisis Pola Hasil Penetration Testing Denial of Services, Man-In-the-Middle, Brute Force, dan SQL Injection pada Sistem Disaster Recovery Center (DRC) Menggunakan Metode K-Means Clustering

Hasil Pengecekan Plagiat/Turnitin: 5%

Menyatakan bahwa laporan tugas akhir ini adalah hasil karya saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Saya menyadari jika terbukti adanya penjiplakan atau plagiat dalam laporan tugas akhir ini, saya siap menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, Pernyataan ini saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.

Palembang, 8 Agustus 2025

Penulis,

Armanda Fathurrahman

NIM. 09011282126055

PATTERN ANALYSIS OF PENETRATION TESTING RESULTS FOR DENIAL OF SERVICE, MAN-IN-THE-MIDDLE, BRUTE FORCE, AND SQL INJECTION ATTACKS ON A DISASTER RECOVERY CENTER (DRC) SYSTEM USING THE K-MEANS CLUSTERING METHOD

Armanda Fathurrahman (09011282126055)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: 09011282126055@student.unsri.ac.id

ABSTRACT

The Disaster Recovery Center (DRC) system ensures the availability of information services during incidents, but it remains vulnerable to cyber attacks such as DoS, MiTM, Brute Force, and SQL Injection. This study analyzes the patterns of penetration testing results on the DRC system using the K-Means Clustering method. Attack data is sourced from internal network simulations, involving preprocessing, balancing using ADASYN, and feature selection via PCA. Clustering results are visualized in two dimensions and evaluated using a confusion matrix. DoS and Brute Force attacks demonstrate high accuracy, while MiTM and SQLi exhibit poor performance due to data imbalance and unclear attack patterns. Additionally, the impact of attacks on CPU usage, memory, and disk I/O was quantitatively analyzed. This study contributes to visual attack detection, clustering evaluation, and the analysis of their impact on the DRC system.

***keywords*: Machine Learning, Penetration Testing, Cyberattacks, Disaster Recovery Center**

PATTERN ANALYSIS OF PENETRATION TESTING RESULTS FOR DENIAL OF SERVICE, MAN-IN-THE-MIDDLE, BRUTE FORCE, AND SQL INJECTION ATTACKS ON A DISASTER RECOVERY CENTER (DRC) SYSTEM USING THE K-MEANS CLUSTERING METHOD

Armanda Fathurrahman (09011282126055)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: 09011282126055@student.unsri.ac.id

ABSTRACT

The Disaster Recovery Center (DRC) system ensures the availability of information services during incidents, but it remains vulnerable to cyber attacks such as DoS, MiTM, Brute Force, and SQL Injection. This study analyzes the patterns of penetration testing results on the DRC system using the K-Means Clustering method. Attack data is sourced from internal network simulations, involving preprocessing, balancing using ADASYN, and feature selection via PCA. Clustering results are visualized in two dimensions and evaluated using a confusion matrix. DoS and Brute Force attacks demonstrate high accuracy, while MiTM and SQLi exhibit poor performance due to data imbalance and unclear attack patterns. Additionally, the impact of attacks on CPU usage, memory, and disk I/O was quantitatively analyzed. This study contributes to visual attack detection, clustering evaluation, and the analysis of their impact on the DRC system.

keywords: ***Machine Learning, Penetration Testing, Cyberattacks, Disaster Recovery Center***

ANALISIS POLA HASIL PENETRATION TESTING DENIAL OF SERVICE, MAN-IN-THE-MIDDLE, BRUTE FORCE, DAN SQL INJECTION PADA SISTEM DISASTER RECOVERY CENTER (DRC) MENGGUNAKAN METODE K-MEANS CLUSTERING

Armanda Fathurrahman (09011282126055)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: 09011282126055@student.unsri.ac.id

ABSTRAK

Sistem *Disaster Recovery Center* (DRC) menjamin ketersediaan layanan informasi saat insiden, namun tetap rentan terhadap serangan siber seperti DoS, MiTM, *Brute Force*, dan *SQL Injection*. Penelitian ini menganalisis pola hasil penetration testing pada sistem DRC menggunakan metode *K-Means Clustering*. Data serangan berasal dari simulasi jaringan internal, dengan tahapan *preprocessing*, penyeimbangan menggunakan ADASYN, serta seleksi fitur melalui PCA. Hasil *clustering* divisualisasikan dalam dua dimensi dan dievaluasi menggunakan *confusion matrix*. Serangan DoS dan *Brute Force* menunjukkan akurasi tinggi, sementara MiTM dan SQLi memiliki performa rendah akibat data imbalance dan pola serangan yang kurang jelas. Selain itu, analisis dampak serangan terhadap penggunaan CPU, memori, dan disk I/O dilakukan secara kuantitatif. Penelitian ini berkontribusi pada deteksi visual serangan, evaluasi *clustering*, dan analisis dampaknya terhadap sistem DRC.

kata kunci: ***Machine Learning, Penetration Testing*, Serangan Siber, *Disaster Recovery Center***

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Allah SWT., karena atas rahmat dan karunia-Nya, penulis dapat menyelesaikan tugas akhir yang berjudul "**Analisis Pola Hasil *Penetration Testing Denial of Services*, *Man-In-the-Middle*, *Brute Force*, dan *SQL Injection* pada Sistem *Disaster Recovery Center* (DRC) Menggunakan Metode *K-Means Clustering***". Penulisan ini disusun sebagai salah satu syarat untuk menyelesaikan program studi dan memperoleh gelar sarjana di Universitas Sriwijaya.

Dalam penyusunan tugas akhir ini, penulis berupaya memberikan kontribusi dalam bidang keamanan siber, khususnya dalam menganalisis dan mengelompokkan pola serangan pada sistem Disaster Recovery Center dengan memanfaatkan metode K-Means Clustering. Penelitian ini diharapkan dapat menjadi referensi dalam peningkatan keamanan infrastruktur jaringan terhadap serangan siber.

Penulis menyadari bahwa dalam penulisan tugas akhir ini tidak akan dapat terselesaikan tanpa bimbingan, dukungan, dan bantuan dari berbagai pihak baik secara materil maupun secara psikis. Sehubungan dengan hal tersebut, penulis menyampaikan ucapan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT yang telah memberi berkah, rezeki, dan nikmat yang melimpah serta kesempatan bagi penulis untuk mampu menyelesaikan penulisan tugas akhir ini.
2. Kedua orang tua, serta kakak dan adik yang selalu memberikan dukungan dan doa yang terbaik serta pembelajaran hidup yang sangat berharga untuk penulis sehingga penulis dapat menyelesaikan penulisan tugas akhir ini dengan baik.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya, atas dukungan dan fasilitas yang diberikan selama proses studi.
4. Bapak Dr. Ir. Ahmad Heryanto, S.Kom., M.T., dan Adi Hermansyah, S.Kom., M.T., selaku Dosen Pembimbing, yang telah meluangkan waktu untuk memberikan bimbingan terbaik, motivasi, serta saran yang sangat berarti dalam penyelesaian tugas akhir ini.
5. Sahabat seperjuangan saya, Andrian Kaspari yang sudah 4 tahun menemani saya, dan selalu sabar menemani dan mendampingi saya, hingga penulis berhasil menyelesaikan tugas akhir ini. Terima kasih yang

sebesar-besarnya, atas semua perjuangan, cerita, dan perjalanan yang telah ditempuh bersama selama ini.

6. Sahabat jauh saya, Muhammad Ryan dan Intan Hazawa yang sudah menjadi pendengar dan mendukung penulis baik secara psikis maupun mental disaat penulis mengalami kegalauan baik dalam urusan penulisan skripsi, maupun dalam hal-hal lainnya.
7. Sahabat masa kecil saya, Ragil Pramudya Putra dan Tilawa Sathia yang senantiasa mendukung penulis, dan menjadi pembangkit semangat dikala penulis pernah mengalami keterpurukan yang luar biasa. Terima kasih atas dukungan bagi penulis.
8. Sahabat-sahabat yang ada dalam grup "Sahabat Selamanya", yakni Bagas, Dhani, Fakhri, Dzaky, Resti, Lulu, dan Aldi yang sudah menjadi penyemangat, pendengar terbaik, dan menjadi pelipur lara bagi penulis dikala penulis sedang merasa jenuh selama proses penulisan tugas akhir ini.
9. Kak Angga selalu admin Jurusan Sistem Komputer yang telah membantu perihal pemberkasan yang diperlukan penulis.
10. Dan seluruh pihak yang tidak bisa disebutkan satu per satu telah memberikan dukungan, doa, dan saran serta motivasi bagi penulis untuk bisa menyelesaikan proposal tugas akhir ini.

Penulis menyadari bahwa tugas akhir ini masih memiliki kekurangan, baik dari segi isi maupun penulisan. Karenanya, kritik dan saran yang membangun sangat penulis harapkan untuk perbaikan di masa mendatang.

Akhir kata, semoga tugas akhir ini dapat bermanfaat bagi pembaca dan memberikan kontribusi positif dalam pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber.

Palembang, Agustus 2025

Penulis,

Armanda Fathurrahman

NIM. 09011282126055

DAFTAR ISI

AUTHENTICATION PAGE ..... **i**
HALAMAN PENGESAHAN ..... **ii**
HALAMAN PERSETUJUAN ..... **iii**
HALAMAN PERNYATAAN ..... **iv**
ABSTRACT ..... **v**
ABSTRAK ..... **vi**
KATA PENGANTAR ..... **vii**
DAFTAR ISI ..... **ix**
DAFTAR GAMBAR ..... **xii**
DAFTAR TABEL ..... **xv**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 4
1.4 Manfaat Penelitian 4
1.5 Batasan Masalah 4
1.6 Sistematika Penulisan 6
BAB II TINJAUAN PUSTAKA **7**
2.1 Pendahuluan 7
2.2 Keamanan Siber 28
2.2.1. Pentingnya Cyber Security 29
2.2.2. Prinsip Dasar Keamanan Informasi (CIA Triad) 31
2.2.3. Pentingnya Keamanan Siber dan Komponen Kuncinya 35
2.2.4. Tantangan dalam Cyber Security 39
2.3 *Denial of Service* (DoS) dan *Distributed Denial of Service* (DdoS) 46
2.3.1 Serangan *Bandwidth Depletion* 55
2.3.2 Serangan *Resource Depletion* 56
2.4 *Man-in-the-Middle* (MiTM) 57
2.5 *Brute Force Attack* (BFA) 59
2.6 *Structured Query Language Injection* (SQLi) 62
2.6.1. *In-Band SQL Injection* 63
2.6.2. Inferential *SQL Injection* 64
2.6.3. *Out-of-band SQL Injection* 64
2.7 *Disaster Recovery Center* (DRC) 65
2.7.1. Hot Standby 65
2.7.2. Cold Standby 66
2.7.3. Warm Standby 67

2.8 *Machine Learning* 68
2.8.1. *Supervised Learning* 69
2.8.2. *Unsupervised Learning* 71
2.8.3. *Reinforcement Learning* 72
2.9 *K-Means Clustering* 73
2.10 *Confusion Matrix* 79
2.10.1. *Accuracy* 80
2.10.2. *Recall* 81
2.10.3. Spesifitas 81
2.10.4. Presisi 81
2.10.5. F1 Score 81
2.11 *Macro Average* 81
BAB III METODOLOGI PENELITIAN 82
3.1 Pendahuluan 82
3.2 Kerangka Kerja 82
3.3 Kerangka Kerja Metodologi Penelitian 83
3.4 Kebutuhan Perangkat 84
3.5 Persiapan Dataset 86
3.6 Ekstraksi Data 88
3.7 *Disaster Recovery Center* (DRC) 89
3.8 *Preprocessing Data* 91
3.8.1 Seleksi Fitur 91
3.8.2 Normalisasi Data 95
3.9 *K-means Clustering* 95
3.10 Skenario Percobaan 99
3.11 Validasi Hasil 105
BAB IV HASIL DAN ANALISIS 109
4.1 Pendahuluan 109
4.2 Hasil Ekstraksi Dataset 109
4.3 Normalisasi Data dan *Feature Selection* 111
4.4 Hasil Uji Menggunakan *K-means Clustering* 111
4.5 Dampak Serangan terhadap Performa Sistem DRC 113
4.6 Dampak Serangan terhadap Performa Sistem DRC 117
4.7 Validasi Hasil 120
4.7.1 Validasi Hasil Data Latih 20% dan Data Uji 80% 120
4.7.2 Validasi Hasil Data Latih 50% dan Data Uji 50% 125
4.7.3 Validasi Hasil Data Latih 30% dan Data Uji 70% 129
4.8 Analisis Hasil Validasi 133
4.9 Hyperparameter Hasil Data 142

BAB V KESIMPULAN DAN SARAN 145
5.1 Kesimpulan..... 145
5.2 Saran 146
DAFTAR PUSTAKA.....148
LAMPIRAN.....153

DAFTAR GAMBAR

Gambar 2.1 *Confidentiality, Integrity, Availability* (CIA Triad).....32
Gambar 2.2 5 Komponen Penting dalam *Cyber Security*.....36
Gambar 2.3 Ancaman Dalam Keamanan Siber.....40
Gambar 2.4 Jenis-jenis *Malware*.....45
Gambar 2.5 Jenis-jenis *Phishing*.....46
Gambar 2.6 Skema Serangan *Denial of Service* (DoS).....48
Gambar 2.7 *Volumetric Attacks*.....50
Gambar 2.8 Protocol Attack.....51
Gambar 2.9 *Application Layer Attacks*.....52
Gambar 2.10 Skema Serangan *Distributed Denial of Service* (DdoS).....54
Gambar 2.11 Skema Serangan *Man-in-the-Middle* (MiTM).....58
Gambar 2.12 Skema Serangan *Brute Force Attack* (BFA).....60
Gambar 2.13 Skema Serangan *SQL Injection*.....62
Gambar 2.14 Skema DRC *Hot Standby*.....66
Gambar 2.15 Skema DRC *Cold Standby*.....67
Gambar 2.16 Skema DRC *Warm Standby*.....68
Gambar 2.17 Alur Kerja *Supervised Learning*.....70
Gambar 2.18 Alur Kerja *Unsupervised Learning*.....71
Gambar 2.19 Alur Kerja *Reinforcement Learning*.....73
Gambar 2.20 Algoritma Umum *K-means*.....75
Gambar 2.21 *Elbow Method*.....78
Gambar 3.1 Kerangka Kerja Penelitian.....83
Gambar 3.2 Kerangka Kerja Metodologi Penelitian.....84
Gambar 3.3 Model Penelitian.....86
Gambar 3.4 Topologi Skenario Serangan *Disaster Recovery Center* (DRC).....90
Gambar 3.5 *Flowchart* Penerapan dan Penyerangan DRC.....90
Gambar 3.6 Flowchart Preprocessing Data.....91
Gambar 3.7 Jumlah Komponen PCA DoS, BFA, MiTM, dan *SQL Injection*.....94
Gambar 3.8 Flowchart K-means.....99
Gambar 3.9 Grafik *Silhouette Score* DoS, MiTM, *Brute Force* dan *SQL Injection* 104
Gambar 3.10 Flowchart Validasi Data.....105
Gambar 4.1 Data berformat *.pcap*.....109

Gambar 4.2 Hasil Ekstraksi Dataset 110
Gambar 4.3 Hasil Ekstraksi Data Menggunakan CICFlowMeter 110
Gambar 4.4 Data Normal dan Data Serangan.....110
Gambar 4.5 Hasil Normalisasi Data Menggunakan *StandardScale* 111
Gambar 4.6 Hasil *Feature Selection* Menggunakan PCA 111
Gambar 4.7 Visualisasi Cluster *K-Means* Untuk Serangan *Denial of Services*.....112
Gambar 4.8 Visualisasi Cluster *K-Means* Untuk Serangan *Brute Force*.....112
Gambar 4.9 Visualisasi Cluster *K-Means* Untuk Serangan *SQL Injection* 112
Gambar 4.10 Visualisasi Cluster *K-Means* Untuk Serangan MiTM.....113
Gambar 4.11 Grafik Penggunaan *Resource* (RAM, CPU, *Disk* I/O) Sistem DRC Terhadap Serangan DoS 114
Gambar 4.12 Grafik Penggunaan *Resource* (RAM, CPU, *Disk* I/O) Sistem DRC Terhadap Serangan *Brute Force*.....114
Gambar 4.13 Grafik Penggunaan *Resource* (RAM, CPU, *Disk* I/O) Sistem DRC Terhadap Serangan MiTM.....115
Gambar 4.14 Grafik Penggunaan *Resource* (RAM, CPU, *Disk* I/O) Sistem DRC Terhadap Serangan *SQL Injection*.....115
Gambar 4.15 *Payload Brute Force Attack* 117
Gambar 4.16 *Payload* MiTM.....118
Gambar 4.17 *Payload* SQL *Injection*.....119
Gambar 4.18 Grafik Hasil Validasi Serangan dengan Rasio 80:20.....123
Gambar 4.19 Grafik Hasil Validasi Serangan dengan Rasio 50:50.....127
Gambar 4.20 Grafik Hasil Validasi Serangan dengan Rasio 70:30.....131
Gambar 4.21 Kurva *Macro Average* Serangan DoS, *Brute Force*, *SQL Injection*, dan MiTM 137
Gambar 4.22 Perbandingan *Cluster* DoS Sebelum dan Setelah *Balancing* Menggunakan ADASYN.....138
Gambar 4.23 Perbandingan *Cluster Brute Force* Sebelum dan Setelah *Balancing* Menggunakan ADASYN.....139
Gambar 4.24 Perbandingan *Cluster* SQL *Injection* Sebelum dan Setelah *Balancing* Menggunakan ADASYN.....139
Gambar 4.25 Perbandingan *Cluster* MiTM Sebelum dan Setelah *Balancing* Menggunakan ADASYN.....140

Gambar 4.26 Visualisasi jarak rata-rata intra-cluster dan inter-cluster per serangan141
Gambar 4.26 *Elbow Method* dan *Silhouette Score* DoS 142
Gambar 4.27 *Elbow Method* dan *Silhouette Score Brute Force*.....142
Gambar 4.28 *Elbow Method* dan *Silhouette Score* MiTM.....143
Gambar 4.29 *Elbow Method* dan *Silhouette Score SQL Injection* 143

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait 7
Tabel 2.2 Matriks Konfusi 80
Tabel 3.1 Spesifikasi Perangkat Keras 84
Tabel 3.2 Spesifikasi Perangkat Lunak 85
Tabel 3.3 Fitur Pada Dataset 86
Tabel 3.4 Atribut *Feature Extraction* 88
Tabel 3.5 Hasil Pengujian Berdasarkan Jumlah K *Cluster* Serangan DoS 101
Tabel 3.6 Hasil Pengujian Berdasarkan Jumlah K *Cluster* Serangan *Brute Force* 101
Tabel 3.7 Hasil Pengujian Berdasarkan Jumlah K *Cluster* Serangan MiTM 102
Tabel 3.8 Hasil Pengujian Berdasarkan Jumlah K *Cluster* Serangan *SQL Injection* 102
Tabel 3.9 Hasil Pengujian Berdasarkan Jumlah K-*Cluster* 106
Tabel 3.10 Hasil Pengujian Berdasarkan Jumlah K-*Cluster* DoS 106
Tabel 3.11 Hasil Pengujian Berdasarkan Jumlah K *Cluster Brute Force* 107
Tabel 3.12 Hasil Pengujian Berdasarkan Jumlah K *Cluster SQL Injection* 107
Tabel 3.13 Hasil Pengujian Berdasarkan Jumlah K *Cluster* MiTM 107
Tabel 4.1 Hasil Validasi Data Latih 80% dan Data Uji 20% 122
Tabel 4.2 Hasil Validasi Data Latih 50% dan Data Uji 50% 126
Tabel 4.3 Hasil Validasi Data Latih 30% dan Data Uji 70% 130
Tabel 4.4 Hasil Rata-rata Metrik Evaluasi dari Masing-Masing Serangan 133

DAFTAR LAMPIRAN

Lampiran 1. Cek Plagiarisme.....154
Lampiran 2. Form Revisi Penguji.....155
Lampiran 3. Form Revisi Pembimbing I.....156
Lampiran 4. Form Revisi Pembimbing II.....157

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan siber merupakan aspek krusial dalam menjaga integritas dan ketersediaan sistem informasi, terlebih pada infrastruktur kritis seperti Pusat Data Nasional (PDN). Insiden peretasan PDN pada Juni 2024 oleh kelompok Brain Cipher, yang berhasil mengenkripsi data strategis seperti Nomor Induk Kependudukan (NIK), menunjukkan bahwa sistem pertahanan siber nasional masih memiliki celah signifikan. Untuk mengantisipasi kerusakan lebih lanjut, diperlukan sistem cadangan yang andal seperti Disaster Recovery Center (DRC), yang mampu menjamin kelangsungan layanan dan pemulihan data secara cepat ketika serangan terjadi.

Penelitian sebelumnya[1], menjelaskan bahwa sistem *Disaster Recovery Center* (DRC) dapat memastikan ketersediaan sistem yang tinggi serta mengurangi waktu henti infrastruktur TI. Studi ini juga mencakup analisis topologi jaringan dan cara kerja aplikasi dalam kondisi normal maupun saat terjadi gangguan, menjadikannya solusi teknologi yang meningkatkan ketahanan sistem informasi. Selanjutnya pada penelitian, mengevaluasi berbagai ancaman yang dapat mengganggu operasional *Data Center*, baik dari faktor alam, manusia, maupun lingkungan. Studi ini menyoroti kewajiban pemilik *Data Center* untuk memiliki rencana keberlangsungan sesuai regulasi pemerintah. Selain itu, penelitian ini membandingkan biaya dan spesifikasi DRC berbasis *cloud* serta konvensional, serta menekankan urgensi implementasi *Disaster Recovery as a Service* (DRaaS) untuk menjaga keberlangsungan bisnis dan mengurangi risiko kehilangan data. Secara keseluruhan, penelitian ini memberikan wawasan mengenai strategi pengembangan DRC yang efisien dan efektif, khususnya dalam konteks pendidikan tinggi.

Meskipun telah dirancang dengan baik, serangan siber tetap berpotensi menembus pertahanan, bahkan pada sistem *Disaster Recovery Center* (DRC). Karenanya, instansi dan organisasi harus selalu waspada agar terhindar dari dampak fatal. Salah satu langkah yang perlu dilakukan adalah pengujian penetrasi (*penetration testing*), yang bertujuan mengidentifikasi serta memperbaiki kerentanan sebelum dieksploitasi oleh peretas. Melalui penelitian[2], organisasi dapat

mengantisipasi serangan, melindungi data sensitif, serta memenuhi regulasi keamanan. Selain itu, hasil pengujian dapat memberikan rekomendasi perbaikan dan membantu organisasi memahami risiko yang dihadapi.

Bahaya serangan siber dapat mengancam sistem *Disaster Recovery Center* (DRC) kapan saja. Berdasarkan penlitian [2], serangan *brute force* mampu menembus pertahanan dengan mencoba berbagai kombinasi kredensial secara paksa hingga berhasil mendapatkan akses ke data sensitif yang tersimpan di dalamnya. Penelitian [3] menuturkan bahwa serangan *man-in-the-middle* (MiTM) memungkinkan peretas menyusup ke komunikasi antara dua pihak, menyamar sebagai salah satu pihak, lalu mencuri atau memodifikasi data yang dikirim, bahkan mengarahkan korban ke situs berbahaya. Sementara itu, penelitian [4] menyatakan serangan *SQL Injection* dilakukan dengan memasukkan kode SQL berbahaya ke dalam kueri database, yang dapat menyebabkan pencurian data, kerusakan sistem, atau hilangnya kendali terhadap database. Terakhir, penelitian [5] menjelaskan serangan *denial of service* (DoS) bekerja dengan membanjiri target menggunakan permintaan tidak sah dalam jumlah besar, sehingga menyebabkan server menjadi lambat, tidak responsif, atau bahkan tidak dapat diakses sama sekali.

Dari berbagai serangan yang mampu membahayakan sistem DRC ini, serangan DoS menjadi serangan yang menjadi ancaman terbesar bagi sistem DRC ini. Penelitian [6], [7], [8] menyatakan serangan DoS lebih mengancam, karena sistem ini bekerja secara terus-menerus untuk bisa melakukan pencadangan sistem, sekaligus membuat layanan terus aktif, apabila sistem ini diserang dengan DoS, maka ia kehilangan kemampuan untuk melakukan pencadangan data. Tidak hanya itu, DoS juga mampu menyerang dengan berbagai cara, seperti membanjiri target dengan trafik palsu (*flood attack*), mengeksploitasi kerentanan pada sistem (*exploit attack*), atau mengganggu koneksi jaringan. Sehingga, sistem DRC menjadi rentan terhadap serangan DoS, dan menjadi pengawasan ekstra terhadap serangan ini ketika suatu instansi menerapkan sistem DRC.

Penelitian ini bertujuan mendeteksi serangan terhadap sistem DRC menggunakan metode *K-Means Clustering*. Dengan metode ini, pola dalam data serangan dapat diidentifikasi dan dikelompokkan, memungkinkan analisis lebih mendalam terkait karakteristik dan perilaku serangan. Hasilnya berupa visualisasi pola serangan, yang membantu pemahaman cara kerja serangan serta pengembangan

strategi mitigasi yang lebih efektif. Selain itu, Penelitian [7] menuturkan bahwa *K-Means Clustering* juga memberikan wawasan tentang distribusi data dalam cluster, yang dapat digunakan untuk mengoptimalkan sumber daya jaringan dan meningkatkan keamanan sistem.

Penerapan *Disaster Recovery Center* (DRC) sangat diperlukan untuk menjaga keamanan data dan memastikan sistem tetap berfungsi dalam situasi krusial. Namun, sistem ini tetap rentan terhadap serangan siber seperti DoS, MiTM, *Brute Force*, dan *SQL Injection*, sehingga diperlukan penetration testing sebagai langkah perlindungan. Untuk memahami pola serangan, metode *K-Means Clustering* dapat digunakan guna mengelompokkan pola serangan dan memberikan wawasan bagi tim IT dalam meningkatkan keamanan sistem DRC. Sehubungan dengan hal tersebut, latar belakang yang dibuat oleh penulis ini akan digunakan untuk melakukan penelitian terhadap Analisis Pola Hasil *Penetration Testing* (*Denial of Service, Man-in-the-Middle, Brute Force,* dan *SQL Injection*) pada *Sistem Disaster Recovery Center* (DRC) Menggunakan Metode *K-Means Clustering*.

Penelitian ini memberikan kontribusi dalam tiga aspek utama. Pertama, penggunaan dataset aktual hasil simulasi serangan nyata terhadap sistem DRC memungkinkan pendekatan yang lebih relevan terhadap kondisi operasional dunia nyata. Kedua, penelitian ini menyajikan visualisasi clustering untuk masing-masing jenis serangan berbasis metode *Principal Component Analysis* (PCA), yang berguna dalam mendukung pemahaman pola serangan secara intuitif. Ketiga, dilakukan analisis dampak serangan terhadap performa sistem dari sisi pemakaian sumber daya, seperti beban CPU, memori, dan aktivitas disk, yang memberikan gambaran konkret mengenai risiko operasional akibat setiap jenis serangan.

1.2 Rumusan Masalah

Dari latar belakang yang ada, terdapat perumusan masalah yang di bahas dari penelitian ini, yaitu sebagai berikut:

1. Bagaimana penerapan simulasi serangan DoS, MiTM, *Brute Force,* dan *SQL Injection* pada sistem DRC?
2. Bagaimana metode *K-Means Clustering* dapat diterapkan untuk menganalisis dan mengelompokkan kerentanan yang ditemukan dalam pengujian penetrasi pada DRC?

3. Apa dampak dari serangan siber terhadap efektivitas sistem DRC dan bagaimana langkah mitigasi yang dapat diambil untuk meningkatkan keamanan sistem?
4. Bagaimana performa deteksi serangan dengan K-Means Clustering terhadap metrik evaluasi seperti akurasi, presisi, recall, spesifisitas, dan F1-Score?

1.3 Tujuan Penelitian

Adapun tujuan dari penulisan Tugas Akhir ini adalahsebagai berikut:

1. Mengimplementasikan simulasi serangan DoS, MiTM, *Brute Force*, dan *SQL Injection* pada sistem DRC.
2. Mengidentifikasi dan menganalisis serangan siber yang berpotensi mengancam *Disaster Recovery Center* (DRC), dengan fokus pada *DoS*, *MITM*, *Brute Force*, dan *SQL Injection*.
3. Mendapatkan nilai optimal berupa akurasi, presisi, *recall*, spesifitas, dan F1-Score dari uji penetrasi pada sistem DRC menggunakan metode *K-means Clustering*.
4. Menerapkan metode *K-means Clustering* untuk melakukan deteksi terhadap serangan DoS, MiTM, *Brute Force*, dan *SQL Injection*.

1.4 Manfaat Penelitian

Berikut merupakan manfaat yang akan diperoleh dari penulisan Tugas Akhir ini, yaitu:

1. Memberikan pemahaman lebih dalam terhadap kerentanan sistem DRC terhadap berbagai jenis serangan siber.
2. Menunjukkan pentingnya pengujian penetrasi (*penetration testing*) sebagai bagian dari pertahanan sistem.
3. Menyajikan pola serangan dalam bentuk visualisasi *cluster* yang dapat membantu dalam proses deteksi dan mitigasi ancaman siber.

1.5 Batasan Masalah

Merujuk pada rumusan masalah sebelumnya, maka batasan masalah yang terdapat pada penyusunan tugas akhir ini, yaitu:

1. Penelitian ini menerapkan *penetration testing* pada sistem *Disaster Recovery Center* (DRC) yang menggunakan strategi pemulihan *Hot Standby*.
2. Serangan yang digunakan dalam penelitian ini adalah *DoS*, *MITM*, *Brute Force*, dan *SQL Injection*.
3. Teknik klasifikasi dan analisis pola serangan menggunakan metode *K-Means*

Clustering tanpa pendekatan supervised learning.

4. Dataset dari keempat jenis serangan memiliki jumlah data yang tidak seimbang, dan meskipun telah dilakukan penyeimbangan menggunakan ADASYN, perbedaan jumlah data awal tetap menjadi keterbatasan dalam proses analisis.

1.6 Sistematika Penulisan

Dalam pengerjaan Tugas Akhir agar mempermudah penulis dalam penyusunan Tugas Akhir, maka dibuat sistematika penulisan, yakni sebagai berikut:

BAB I PENDAHULUAN

Bab pertama menguraikan secara sistematis mengenai mengenai latar belakang pentingnya keamanan siber pada sistem DRC, rumusan masalah yang akan dikaji, tujuan dan manfaat dari penelitian ini, batasan ruang lingkup agar fokus penelitian tetap terarah, serta sistematika penulisan tugas akhir secara keseluruhan.

BAB II TINJAUAN PUSTAKA

Bab kedua membahas teori-teori dasar dan penelitian sebelumnya yang relevan, termasuk jenis-jenis serangan siber (DoS, MiTM, *Brute Force*, dan *SQL Injection*), konsep *Disaster Recovery Center* (DRC), teknik *K-Means Clustering*, serta metrik evaluasi yang digunakan dalam pengujian performa klasifikasi.

BAB III METODOLOGI PENELITIAN

Bab ketiga menjelaskan tahapan teknis penelitian yang mencakup proses simulasi serangan, *preprocessing data*, penanganan data yang tidak seimbang menggunakan ADASYN, reduksi dimensi dengan PCA, serta penerapan algoritma *K-Means* untuk mengelompokkan data serangan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini memaparkan hasil eksperimen berupa visualisasi *cluster* dari masing-masing jenis serangan, evaluasi performa model menggunakan *confusion matrix*, serta analisis kuantitatif antar *cluster* untuk melihat efektivitas pemisahan kelompok serangan.

BAB V KESIMPULAN DAN SARAN

Bab ini menyajikan temuan-temuan utama yang diperoleh selama penelitian dan memberikan saran pengembangan ke depan, termasuk pemanfaatan metode hybrid serta integrasi sistem deteksi serangan dengan solusi keamanan seperti IDS atau SIEM.

DAFTAR PUSTAKA

[1] Dhanujati N and Girsang S, "Data Center-Disaster Recovery Center (DC-DRC) For High Availability IT Service," *Bina Nusantara University*, p. 576, Sep. 2018.

[2] A. Razaque *et al.*, "Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain," *IEEE Access*, vol. 7, pp. 168774–168797, 2019, doi: 10.1109/ACCESS.2019.2950849.

[3] A. Kosugi, K. Teranishi, and K. Kogiso, "Experimental Validation of the Attack-Detection Capability of Encrypted Control Systems Using Man-in-the-Middle Attacks," *IEEE Access*, vol. 12, pp. 10535–10547, 2024, doi: 10.1109/ACCESS.2024.3353289.

[4] N. M. Sheykhkanloo, "Employing Neural Networks for the detection of SQL injection attack," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Sep. 2014, pp. 318–323. doi: 10.1145/2659651.2659675.

[5] O. M. Almorabea, T. J. S. Khanzada, M. A. Aslam, F. A. Hendi, and A. M. Almorabea, "IoT Network-Based Intrusion Detection Framework: A Solution to Process Ping Floods Originating from Embedded Devices," *IEEE Access*, vol. 11, pp. 119118–119145, 2023, doi: 10.1109/ACCESS.2023.3327061.

[6] S. Agrawal and R. Singh Rajput, "Denial of Services Attack Detection using Random Forest Classifier with Information Gain," *International Journal of Engineering Development and Research*, vol. 5, 2017, [Online]. Available: www.ijedr.org

[7] Putri N, Stiawan D, Heryanto A, Septian T, Siregar L, and Budiarto R, "Denial of Service Attack Visualization with Clustering using K-Means Algorithm," *International Conference on Electrical Engineering and Computer Science (ICECOS)*, 2017.

[8] A. R. A. Yusof, N. I. Udzir, A. Selamat, H. Hamdan, and M. T. Abdullah, "Adaptive feature selection for denial of services (DoS) attack," in *2017 IEEE Conference on Applications, Information and Network Security, AINS 2017*, Institute of Electrical and Electronics Engineers Inc., Jul. 2017, pp. 81–84. doi: 10.1109/AINS.2017.8270429.

[9] Y. Y. Aung and M. M. Min, *Hybrid Intrusion Detection System using K-means and Classification and Regression Trees Algorithms*. IEEE Computer Society, 2018.

[10] H. S. Abdullah and A. Mohsin Abdulazeez, "Detection of SQL Injection Attacks Based on," 2024.

[11] R. M. Balajee, S. Kallam, and M. K. Jayanthi Kannan, "Network Intrusion Classifier with Optimized Clustering Algorithm for the Efficient Classification," in *Proceedings - 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 439–446. doi: 10.1109/ICICV62344.2024.00075.

[12] A. A. J. Al-Abadi, M. B. Mohamed, and A. Fakhfakh, "Enhanced Random Forest Classifier with K-Means Clustering (ERF-KMC) for Detecting and Preventing Distributed-Denial-of-Service and Man-in-the-Middle Attacks in Internet-of-Medical-Things Networks," *Computers*, vol. 12, no. 12, Dec. 2023, doi: 10.3390/computers12120262.

[13] H. Yang, L. Cheng, and M. Chuah, *Deep-Learning-Based Network Intrusion Detection for SCADA Networks*. IEEE, 2019.
[14] L. Xiao, Z. Shao, and G. Liu, "K-means Algorithm Based on Particle Swarm Optimization Algorithm for Anomaly Intrusion Detection," Jun. 2006.
[15] N. Yalcin, S. Cakir, and S. Ualdi, "Attack Detection Using Artificial Intelligence Methods for SCADA Security," *IEEE Internet Things J*, 2024, doi: 10.1109/JIOT.2024.3447876.
[16] M. L. Siddiq *et al.*, "SQLIFIX: Learning Based Approach to Fix SQL Injection Vulnerabilities in Source Code." [Online]. Available: https://github.com/
[17] M. H. Kamarudin, C. Maple, T. Watson, and N. S. Safa, "A LogitBoost-Based Algorithm for Detecting Known and Unknown Web Attacks," *IEEE Access*, vol. 5, pp. 26190–26200, Nov. 2017, doi: 10.1109/ACCESS.2017.2766844.
[18] D. Chen, Q. Yan, C. Wu, and J. Zhao, "SQL Injection Attack Detection and Prevention Techniques Using Deep Learning," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Feb. 2021. doi: 10.1088/1742-6596/1757/1/012055.
[19] A. Joshi and V. Geetha, *SQL Injection Detection using Machine Learning*. IEEE, 2014.
[20] H. A. Al-Essa and A. A. Abdulbaki, "Disaster Recovery Datacenter's Architecture on Network Replication Solution," 2016, doi: 10.1109/EMS.2016.36.
[21] H. Zhang and L. Zhao, *Data Security in Disaster Recovery System*. IEEE, 2010.
[22] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, and K. M. Koumadi, "Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN)," *Journal of Computer Networks and Communications*, vol. 2019, 2019, doi: 10.1155/2019/4683982.
[23] T. Jun-Feng, Z. Jia-Yao, and D. Rui-Zhong, "Date Hierarchical Storage Strategy for Data Disaster Recovery," *IEEE Access*, vol. 6, pp. 45606–45616, Aug. 2018, doi: 10.1109/ACCESS.2018.2862468.
[24] P. Wlazlo *et al.*, "Man-in-the-middle attacks and defence in a power system cyber-physical testbed," *IET Cyber-Physical Systems: Theory and Applications*, vol. 6, no. 3, pp. 164–177, Sep. 2021, doi: 10.1049/cps2.12014.
[25] A. Widjajarto, M. Lubis, and A. R. Lubis, "Service Level Agreement (SLAs) Model for Disaster Recovery Center (DRC) Based on Computational Resource Model of Virtual Machine," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 1476–1483. doi: 10.1016/j.procs.2024.03.148.
[26] Y. Wang, *RESEARCH ON REMOTE DISASTER RECOVERY SYSTEM OF DIGITAL LIBRARY*. I E E E, 2009.
[27] D. Stiawan, E. Alzahrani, S. Sandra, and R. Budiarto, *Comparative Analysis of K-Means Method and Naïve Bayes Method for Brute Force Attack Visualization*. IEEE, 2017.
[28] J. J. Villalobos, I. Rodero, and M. Parashar, "An unsupervised approach for online detection and mitigation of high-rate DDoS attacks based on an in-memory distributed graph using streaming data and analytics," in *BDCAT 2017 - Proceedings of the 4th IEEE/ACM International Conference on Big Data Computing, Applications and Technologies*, Association for Computing

Machinery, Inc, Dec. 2017, pp. 103–112. doi: 10.1145/3148055.3148077.
[29] S. Sandra, D. Stiawan, and A. Heryanto, "Visualisasi Serangan Brute Force Menggunakan Metode K-Means dan Naïve Bayes," 2016. [Online]. Available: http://ars.ilkom.unsri.ac.id
[30] C. Asnawi, D. Hariyadi, U. S. Aesyi, and P. W. Cahyo, "Analisis dan Penanganan Insiden Siber SQL Injection Menggunakan Kerangka NIST SP 800-61R2 dan Algoritma Klusterisasi K-Means," *Jurnal Komtika (Komputasi dan Informatika)*, vol. 7, no. 2, pp. 134–144, Nov. 2023, doi: 10.31603/komtika.v7i2.10527.
[31] A. A. Elmarady and K. Rahouma, "Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment," *IEEE Access*, vol. 9, pp. 143997–144016, 2021, doi: 10.1109/ACCESS.2021.3121230.
[32] M. Wills, "Information Security Fundamentals," 2019.
[33] E. N. Ylmaz, B. Ciylan, S. Gönen, E. Sindiren, and G. Karacayilmaz, "Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect," in *Proceedings - 2018 6th International Istanbul Smart Grids and Cities Congress and Fair, ICSG 2018*, Institute of Electrical and Electronics Engineers Inc., Jul. 2018, pp. 81–85. doi: 10.1109/SGCF.2018.8408947.
[34] B. D. Rawat and C. Bajracharya, *Cyber Security for Smart Grid Systems: Status, Challenges and Perspectives*. Florida: Institute of Electrical and Electronics Engineers, 2015.
[35] M. Ghiasi, M. Dehghani, T. Niknam, A. Kavousi-Fard, P. Siano, and H. H. Alhelou, "Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform," *IEEE Access*, vol. 9, pp. 29429–29440, 2021, doi: 10.1109/ACCESS.2021.3059042.
[36] S. Gupta, C. Maple, and R. Passerone, "An Investigation of Cyber-Attacks and Security Mechanisms for Connected and Autonomous Vehicles," 2023, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2023.3307473.
[37] D. Shahjee and N. Ware, "Integrated Network and Security Operation Center: A Systematic Analysis," *IEEE Access*, vol. 10, pp. 27881–27898, 2022, doi: 10.1109/ACCESS.2022.3157738.
[38] A. Yeboah-Ofori *et al.*, "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security," *IEEE Access*, vol. 9, pp. 94318–94337, 2021, doi: 10.1109/ACCESS.2021.3087109.
[39] S. A. M. Al-Juboori, F. Hazzaa, Z. S. Jabbar, S. Salih, and H. M. Gheni, "Man-in-the-middle and denial of service attacks detection using machine learning algorithms," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 1, pp. 418–426, Feb. 2023, doi: 10.11591/eei.v12i1.4555.
[40] N. Mamuriyah, S. E. Prasetyo, and A. O. Sijabat, "Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi," *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 6, no. 1, pp. 162–167, Jan. 2024, doi: 10.47233/jteksis.v6i1.1124.
[41] R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS attack & its effect in cloud environment," in *Procedia Computer Science*, Elsevier B.V., 2015, pp. 202–210. doi: 10.1016/j.procs.2015.04.245.
[42] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R.

Budiarto, “Investigating Brute Force Attack Patterns in IoT Network,” *Journal of Electrical and Computer Engineering*, vol. 2019, 2019, doi: 10.1155/2019/4568368.

[43] M. Nadeem, A. Arshad, S. Riaz, S. S. Band, and A. Mosavi, “Intercept the cloud network from brute force and ddos attacks via intrusion detection and prevention system,” *IEEE Access*, vol. 9, pp. 152300–152309, 2021, doi: 10.1109/ACCESS.2021.3126535.

[44] Q. Li, W. Li, J. Wang, and M. Cheng, “A SQL Injection Detection Method Based on Adaptive Deep Forest,” *IEEE Access*, vol. 7, pp. 145385–145394, 2019, doi: 10.1109/ACCESS.2019.2944951.

[45] M. A. Prabakar, M. K. Keyan, and K. Marimuthu, *AN EFFICIENT TECHNIQUE FOR PREVENTING SQL INJECTION ATTACK USING PATTERN MATCHING ALGORITHM*. [IEEE], 2013.

[46] A. Rai, M. M. I. Miraz, D. Das, H. Kaur, and Swati, “SQL Injection: Classification and Prevention,” in *Proceedings of 2021 2nd International Conference on Intelligent Engineering and Management, ICIEM 2021*, Institute of Electrical and Electronics Engineers Inc., Apr. 2021, pp. 367–372. doi: 10.1109/ICIEM51511.2021.9445347.

[47] P. R. McWhirter, K. Kifayat, Q. Shi, and B. Askwith, “SQL Injection Attack classification through the feature extraction of SQL query strings using a Gap-Weighted String Subsequence Kernel,” *Journal of Information Security and Applications*, vol. 40, pp. 199–216, Jun. 2018, doi: 10.1016/j.jisa.2018.04.001.

[48] K. Zhang, “A machine learning based approach to identify SQL injection vulnerabilities,” in *Proceedings - 2019 34th IEEE/ACM International Conference on Automated Software Engineering, ASE 2019*, Institute of Electrical and Electronics Engineers Inc., Nov. 2019, pp. 1286–1288. doi: 10.1109/ASE.2019.00164.

[49] J. Mendonça, E. Andrade, P. T. Endo, and R. Lima, “Disaster recovery solutions for IT systems: A Systematic mapping study,” *Journal of Systems and Software*, vol. 149, pp. 511–530, Mar. 2019, doi: 10.1016/j.jss.2018.12.023.

[50] A. Setyawan, Y. Giri Sucahyo, and A. Gandhi, “Design of disaster recovery plan: State university in indonesia,” in *2020 5th International Conference on Informatics and Computing, ICIC 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/ICIC50835.2020.9288543.

[51] Zulkarnain, “ANALISA PENERAPAN DISASTER RECOVERY PLAN PADA DATA CENTER PERUSAHAAN,” *Computer Based Information System Journal*, vol. 10, Sep. 2022, [Online]. Available: http://ejournal.upbatam.ac.id/index.php/cbishttp://ejournal.upbatam.ac.id/index.php/cbis

[52] A. L’Heureux, K. Grolinger, H. F. Elyamany, and M. A. M. Capretz, “Machine Learning with Big Data: Challenges and Approaches,” *IEEE Access*, vol. 5, pp. 7776–7797, 2017, doi: 10.1109/ACCESS.2017.2696365.

[53] S. Bødker, E. Giaccardi, A. Taylor, and R. Fiebrink, “Machine Learning in Interaction.”

[54] B. Mahesh, “Machine Learning Algorithms - A Review,” *International Journal of Science and Research (IJSR)*, vol. 9, no. 1, pp. 381–386, Jan. 2020, doi: 10.21275/art20203995.

[55] S. L. Brunton, B. R. Noack, and P. Koumoutsakos, “Machine Learning for Fluid Mechanics,” *Annual Review*, vol. 7, p. 29, 2025, doi: 10.1146/annurev-fluid-010719.
[56] K. Gupta, A. V. Srivastava, and G. Raj, *K-mean Clustering in Web Service Quality Datasets Using AWS and RapidMiner*. IEEE, 2018.
[57] L. Xiao, Z. Shao, and G. Liu, “K-means Algorithm Based on Particle Swarm Optimization Algorithm for Anomaly Intrusion Detection,” Jun. 2006.
[58] C. Zhang and S. Xia, “K-means clustering algorithm with improved initial center,” in *Proceedings - 2009 2nd International Workshop on Knowledge Discovery and Data Mining, WKKD 2009*, 2009, pp. 790–792. doi: 10.1109/WKDD.2009.210.
[59] S. Dwivedi Lalit Kumar PBhaiya, “A Systematic Review on K-Means Clustering Techniques.”
[60] A. Singh, “K-means with Three different Distance Metrics,” 2013.
[61] T. M. Kodinariya and P. R. Makwana, “Review on determining number of Cluster in K-Means Clustering,” *International Journal of Advance Research in Computer Science and Management Studies*, vol. 1, no. 6, 2013, [Online]. Available: www.ijarcsms.com
[62] A. Fakhruddin, J. S. Kom, A. Ridwan, and S. Mmsi, “Performance Measurement of Confusion Matrix Accuracy in Sentiment Analysis with Decision Trees, Naïve Bayes, K-Nearest Neighbor methods Using Rapidminer,” *International Research Journal of Advanced Engineering and Science*, vol. 8, no. 4, pp. 123–127, 2023.
[63] M. Sokolova and G. Lapalme, “A systematic analysis of performance measures for classification tasks,” *Inf Process Manag*, vol. 45, no. 4, pp. 427–437, Jul. 2009, doi: 10.1016/j.ipm.2009.03.002.
[64] C. Zhu, C. U. Idemudia, and W. Feng, “Improved logistic regression model for diabetes prediction by integrating PCA and K-means techniques,” *Inform Med Unlocked*, vol. 17, Jan. 2019, doi: 10.1016/j.imu.2019.100179.
[65] Z. H. Zhou, *Machine Learning*. Springer Nature, 2021. doi: 10.1007/978-981-15-1967-3.
[66] J. Han, M. Kamber, and J. Pei, “Data Mining. Concepts and Techniques, 3rd Edition (The Morgan Kaufmann Series in Data Management Systems),” 2011.
[67] S. B. Kotsiantis, “Supervised Machine Learning: A Review of Classification Techniques,” 2007.