PROPOSAL PENAWARAN PENGEMBANGAN PERANGKAT LUNAK

Judul Proyek : Analisis Dataset RokYou dan Kalkulator Keamanan Password

Diajukan Oleh : - Farraz Dzaky Faisa [System Analyst]

- Muhammad Bintang [Documentation]

- Muhammad Bukhori [Progammer]

- Muhammad Virgawan [Tester]

Tanggal : 13 Oktober 2025

Rekayasa Perangkat Lunak 2

Universitas Gunadarma

2025

I. GAMBARAN UMUM

Di era digital yang semakin berkembang, keamanan data menjadi isu yang sangat penting. Salah satu penyebab utama terjadinya kebocoran data adalah penggunaan password yang lemah dan mudah ditebak. Berdasarkan berbagai laporan keamanan, tercatat miliaran password telah bocor ke publik, salah satunya berasal dari dataset RockYou pada tahun 2009. Hal ini menunjukkan bahwa masih banyak pengguna yang belum memahami pentingnya membuat password yang kuat dan aman.

Permasalahan utama yang sering dihadapi pengguna awam adalah ketidakmampuan untuk menilai kekuatan password secara objektif. Banyak pengguna merasa password yang mereka buat sudah aman, padahal sebenarnya sangat rentan terhadap serangan Brute Force, yaitu metode peretasan dengan mencoba berbagai kombinasi password secara otomatis. Tanpa adanya alat bantu yang jelas dan mudah digunakan, pengguna cenderung mengabaikan aspek keamanan ini.

Sebagai solusi atas permasalahan tersebut, dikembangkan sebuah aplikasi berbasis web bernama **Password Entropy Calculator**. Aplikasi ini dirancang untuk membantu pengguna memahami tingkat keamanan password mereka secara langsung. Dengan memanfaatkan algoritma Shannon Entropy, sistem dapat menghitung tingkat kompleksitas password berdasarkan kombinasi karakter yang digunakan.

Fitur utama dari aplikasi ini adalah analisis secara *real-time*, di mana kekuatan password akan langsung ditampilkan saat pengguna mengetikkan password. Selain itu, aplikasi ini juga berfungsi sebagai sarana edukasi keamanan dengan menampilkan visualisasi data dari dataset nyata seperti RockYou(2009). Melalui visualisasi ini, pengguna dapat melihat perbandingan statistik antara password yang lemah dan password yang kuat, sehingga lebih memahami risiko penggunaan password sederhana.

Tidak hanya itu, aplikasi ini juga menyediakan rekomendasi perbaikan password. Jika password yang dimasukkan masih tergolong lemah, sistem akan memberikan saran seperti menambahkan panjang karakter, menggunakan kombinasi huruf besar, huruf kecil, angka, dan simbol. Dengan demikian, pengguna dapat meningkatkan kualitas password mereka hingga masuk ke dalam kategori “Kuat” dan lebih aman dari serangan *Cyber*.

1.2 Struktur Tim dan Pembagian Tugas

Untuk memastikan pengembangan aplikasi "Password Entropy Calculator" berjalan efektif dan sesuai target waktu, tim pengembang membagi tanggung jawab ke dalam empat peran utama dengan rincian tugas sebagai berikut:

1. Programmer: Muhammad Bukhori

Programmer bertanggung jawab penuh terhadap aspek teknis dan pengembangan sistem aplikasi. Peran ini berfokus pada penerjemahan kebutuhan sistem ke dalam bentuk kode yang dapat dijalankan. Tugas utama yang dilakukan meliputi:

- Mengembangkan logika backend menggunakan bahasa pemrograman Python, khususnya untuk mengimplementasikan rumus matematika Shannon Entropy dalam menghitung kekuatan password.
- Membangun antarmuka pengguna (*front-end*) berbasis web menggunakan framework Streamlit agar aplikasi mudah digunakan dan interaktif.
- Mengintegrasikan pustaka visualisasi data seperti Matplotlib atau Altair untuk menampilkan grafik dan statistik kekuatan password.
- Melakukan proses *deployment* aplikasi sehingga sistem dapat dijalankan dan diakses langsung melalui browser oleh pengguna.

2. System Analyst: Farraz Dzaky

Bertanggung jawab atas analisis data dan perancangan alur sistem. Tugas spesifik meliputi:

- Menganalisis dataset mentah RockYou(2009) yang berisi 14 juta data password bocor.
- Melakukan proses Data Preparation (pembersihan data), termasuk menghapus duplikasi, memfilter panjang karakter, dan validasi encoding ASCII.
- Merancang alur kerja sistem menggunakan metode CRISP-DM (*Cross-Industry Standard Process for Data Mining*).
- Menentukan parameter dan batasan klasifikasi kekuatan password (Sangat Lemah, Lemah, Sedang, Kuat) berdasarkan standar keamanan Cyber.

3. Documentation: Muhammad Bintang

Bertanggung jawab atas seluruh aspek administrasi dan dokumentasi tertulis proyek. Tugas spesifik meliputi:

- Menyusun dokumen formal proyek mulai dari Proposal Penawaran, Laporan Pendahuluan, Laporan Progres (Antara), hingga Laporan Akhir.
- Mendokumentasikan setiap tahapan pengembangan, termasuk menyisipkan diagram alur (flowchart), potongan kode program, dan hasil tangkapan layar (screenshot) aplikasi.
- Menyusun Panduan Pengguna (User Guide) yang berisi tutorial langkah demi langkah penggunaan aplikasi untuk pengguna awam.
- Memastikan format penulisan laporan sesuai dengan standar akademis atau standar industri yang berlaku.

4. Tester (Quality Assurance): Muhammad Virgawan

Bertanggung jawab melakukan pengujian terhadap fungsionalitas dan akurasi sistem. Tugas spesifik meliputi:

- Melakukan Black Box Testing dengan menginput berbagai kombinasi password (unik, panjang, pendek, berkarakter khusus) untuk memastikan tidak ada error saat kalkulasi.
- Memvalidasi akurasi hasil perhitungan Entropy aplikasi dengan perhitungan manual untuk memastikan ketepatan algoritma.
- Mengecek responsivitas tombol navigasi, input form, dan visualisasi grafik pada aplikasi web.
- Mencatat dan melaporkan bug atau error yang ditemukan kepada Programmer untuk segera diperbaiki sebelum rilis final.

II. METODE PENGEMBANGAN PERANGKAT LUNAK

Untuk memastikan kualitas hasil analisis data yang akurat dan dapat dipertanggungjawabkan, proyek ini menerapkan metodologi CRISP-DM (*Cross-Industry Standard Process for Data Mining*). Metodologi ini dipilih karena sangat sesuai untuk pengembangan aplikasi yang berbasis pada pengolahan dan analisis data (*data-driven*), seperti pada pengembangan Password Entropy Calculator. CRISP-DM memberikan alur kerja yang terstruktur sehingga setiap tahapan pengolahan data dapat dilakukan secara sistematis. Tahapannya meliputi:

1. Business Understanding

Pada tahap ini, fokus utama adalah memahami permasalahan keamanan password yang sering dihadapi pengguna. Banyak pengguna masih menggunakan password yang lemah tanpa menyadari risikonya terhadap serangan Cyber. Oleh karena itu, tujuan dari proyek ini adalah menyediakan alat yang mampu membantu pengguna menilai kekuatan password mereka secara objektif dan memberikan edukasi terkait pentingnya penggunaan password yang kuat.

2. Data Understanding

Tahap ini dilakukan dengan mengumpulkan dan mempelajari dataset yang akan digunakan, yaitu RockYou(2009). Dataset ini berisi jutaan password nyata yang pernah bocor, sehingga sangat relevan untuk memahami pola password yang sering digunakan dan mengidentifikasi karakteristik password yang tergolong lemah maupun kuat.

3. Data Preparation

Pada tahap persiapan data, dilakukan proses pembersihan (*cleaning*) terhadap sekitar 14 juta data password. Proses ini meliputi penghapusan data duplikat, data kosong, serta karakter yang tidak diperlukan. Tujuannya agar data yang digunakan benar-benar bersih dan siap untuk dianalisis, sehingga hasil perhitungan entropy menjadi lebih akurat.

4. Modeling

Tahap modeling dilakukan dengan menerapkan rumus Shannon Entropy untuk menghitung tingkat kekuatan setiap password. Rumus ini digunakan untuk mengukur kompleksitas password berdasarkan variasi karakter dan panjang password. Hasil dari tahap ini berupa nilai entropy yang menunjukkan apakah sebuah password tergolong lemah, sedang, atau kuat.

5. Evaluation

Setelah model diterapkan, dilakukan evaluasi untuk memastikan bahwa hasil perhitungan entropy sudah sesuai dan akurat. Validasi ini dilakukan dengan membandingkan hasil perhitungan terhadap standar kekuatan password serta contoh password dari dataset. Tahap ini penting untuk memastikan bahwa sistem dapat memberikan penilaian yang dapat dipercaya.

6. Deployment

Tahap terakhir adalah implementasi sistem ke dalam aplikasi berbasis web menggunakan framework Streamlit. Dengan Streamlit, aplikasi dapat menampilkan analisis kekuatan password secara real-time, visualisasi data, serta rekomendasi perbaikan password. Hasilnya, aplikasi dapat digunakan secara langsung oleh pengguna sebagai alat bantu evaluasi dan edukasi keamanan password.

III. TIMELINE PENGERJAAN

Estimasi pengerjaan proyek adalah 2 bulan (8 Minggu)

Minggu Ke-	Kegiatan	Output yang Dihasilkan
1	Analisis Kebutuhan & Studi Literatur	Dokumen Spesifikasi Kebutuhan
2	Pengumpulan & Pemahaman Data (*RockYou(2009)*)	Laporan Analisis Data Mentah
3	Data Preparation (Cleaning & Filtering)	Dataset Bersih (*Clean Data*)
4	Modeling (Implementasi Algoritma Entropy dengan Python)	Script Python Perhitungan Entropy
5-6	Perancangan UI/UX & Wireframing	Desain Antarmuka Aplikasi
7	Implementasi Web dengan Streamlit (Deployment)	Aplikasi Versi Beta
8	Testing, Evaluasi & Finalisasi Laporan	Aplikasi Final & Laporan Akhir

Minggu 1: Analisis Kebutuhan & Studi Literatur

Pada tahap awal ini, dilakukan identifikasi kebutuhan sistem dan tujuan proyek. Tim mempelajari referensi terkait keamanan password, algoritma Shannon Entropy, serta penelitian terdahulu yang relevan. Hasil dari tahap ini adalah dokumen spesifikasi kebutuhan yang menjadi dasar pengembangan aplikasi.

Minggu 2: Pengumpulan & Pemahaman Data

Pada minggu ini, dataset RockYou(q2009) dikumpulkan dan dianalisis secara awal. Proses ini bertujuan untuk memahami struktur data, pola password yang sering digunakan, serta karakteristik password lemah. Output dari tahap ini berupa laporan analisis data mentah.

Minggu 3: Data Preparation (Cleaning & Filtering)

Tahap ini berfokus pada pembersihan dataset yang berisi sekitar 14 juta password. Data duplikat, data kosong, dan data tidak relevan dihapus agar dataset siap digunakan. Hasil akhirnya adalah dataset bersih (*clean data*) yang dapat diolah dengan baik.

Minggu 4: Modeling (Algoritma Entropy)

Pada tahap ini dilakukan pengembangan model dengan mengimplementasikan rumus Shannon Entropy menggunakan bahasa pemrograman Python. Model ini digunakan untuk menghitung tingkat kekuatan password secara matematis. Output dari tahap ini berupa script Python yang siap diintegrasikan ke aplikasi.

Minggu 5 - 6: Perancangan UI/UX & Wireframing

Tahap ini berfokus pada desain tampilan aplikasi agar mudah digunakan oleh pengguna. Dibuat wireframe dan rancangan antarmuka yang menampilkan input password, hasil analisis entropy, visualisasi data, serta rekomendasi perbaikan password.

Minggu 7: Implementasi Web dengan Streamlit

Pada minggu ini, seluruh komponen sistem diintegrasikan ke dalam aplikasi berbasis web menggunakan framework Streamlit. Aplikasi mulai dapat dijalankan dan diuji secara fungsional, dengan hasil berupa versi beta aplikasi.

Minggu 8: Testing, Evaluasi & Finalisasi

Tahap terakhir adalah pengujian sistem untuk memastikan aplikasi berjalan dengan baik dan hasil perhitungan entropy sudah akurat. Setelah itu dilakukan perbaikan akhir dan penyusunan laporan final. Output tahap ini adalah aplikasi versi final serta laporan akhir proyek.