

## DAFTAR ISI

DAFTAR ISI	1
<b>BAB 1. PENDAHULUAN</b>	2
1.1 Latar Belakang	
1.2 Justifikasi Ilmiah	
1.3 Penelitian Sebelumnya dan Kesenjangan yang Diidentifikasi	
1.4 Tujuan Khusus	
1.5 Manfaat Penelitian	
1.6 Urgensi Penelitian	
1.7 Target Penemuan	
1.8 Kontribusi terhadap Ilmu pengetahuan	
<b>BAB 2. TINJAUAN PUSTAKA</b>	4
2.1 Algoritma Naive Bayes dalam Aplikasi AI	
2.2 Aplikasi dalam Keamanan Kata Sandi	
2.3 Batasan dan Tantangan	
2.4 Integrasi dengan Set Data Berlabel	
<b>BAB 3. METODE RISET</b>	5
3.1 <i>Naive Bayes</i>	
3.2 <i>Logistic Regression</i>	
3.3 <i>Stochastic Gradient Descent</i>	
3.4 <i>Passive Aggressive Classifier</i>	
3.5 Kesimpulan Riset	
<b>BAB 4. BIAYA DAN JADWAL KEGIATAN</b>	9
4.1 Anggaran Biaya	9
4.2 Jadwal Kegiatan	10
<b>DAFTAR PUSTAKA</b>	11
<b>LAMPIRAN</b>	13
Lampiran 1. Biodata Ketua dan Anggota serta Dosen Pendamping	13

## **BAB 1. PENDAHULUAN**

### **1.1. Latar Belakang**

Di landscape digital kontemporer, keamanan informasi yang sensitif sangatlah penting. Seiring ancaman siber yang terus berkembang, kebutuhan akan mekanisme perlindungan kata sandi yang kuat menjadi semakin krusial. Kata sandi berfungsi sebagai garis pertahanan pertama melawan akses tanpa izin ke data pribadi dan organisasi. Namun, metode pembuatan kata sandi tradisional sering rentan terhadap serangan, mendorong eksplorasi pendekatan inovatif. Penelitian ini menggali pengembangan pembuat kata sandi yang aman berbasis kecerdasan buatan (AI), memanfaatkan algoritma pembelajaran mesin untuk meningkatkan kekuatan dan ketangguhan kata sandi yang dihasilkan.

### **1.2. Justifikasi Ilmiah**

Meningkatnya insiden peretasan data dan serangan siber menegaskan pentingnya untuk meningkatkan langkah-langkah keamanan kata sandi. Metode pembuatan kata sandi yang ada sering tidak memadai dalam menciptakan kata sandi yang dapat bertahan melawan serangan yang canggih. Penelitian ini bertujuan untuk menjembatani kesenjangan antara praktek konvensional dan dinamika ancaman siber dengan memanfaatkan kemampuan kecerdasan buatan. Dengan menggunakan set data berlabel yang mencakup kata sandi lemah, sedang, dan kuat, proyek ini bertujuan melatih model yang dapat menghasilkan kata sandi yang sangat aman secara cerdas.

### **1.3. Penelitian Sebelumnya dan Kesenjangan yang Diidentifikasi**

Penelitian yang luas telah dilakukan di bidang keamanan kata sandi, dengan fokus pada metode enkripsi, persyaratan kompleksitas, dan analisis perilaku pengguna. Namun, pendekatan yang ada belum sepenuhnya mengatasi sifat dinamis dari ancaman siber. Penelitian ini mengidentifikasi kesenjangan dalam metodologi yang ada, khususnya dalam menghasilkan kata sandi yang adaptif terhadap vektor serangan yang muncul. Solusi berbasis kecerdasan buatan yang diusulkan bertujuan untuk mengisi kesenjangan ini dengan menggunakan pembelajaran mesin untuk menciptakan kata sandi yang tidak hanya memenuhi standar keamanan saat ini, tetapi juga berkembang untuk melawan ancaman yang berkembang.

### **1.4. Tujuan Khusus**

Tujuan utama dari penelitian ini adalah sebagai berikut:

- Mengembangkan pembuat kata sandi berbasis AI berdasarkan set data berlabel.
- Melatih model untuk membedakan antara kata sandi lemah, sedang, dan kuat.
- Mengimplementasikan algoritma adaptif untuk meningkatkan kekuatan kata sandi dari waktu ke waktu.
- Mengevaluasi kinerja kata sandi yang dihasilkan oleh AI dibandingkan dengan metode tradisional.

### **1.5. Manfaat Penelitian**

Hasil dari penelitian ini diharapkan memberikan beberapa manfaat:

- Peningkatan keamanan kata sandi terhadap berbagai ancaman siber.
- Perlindungan pengguna yang ditingkatkan di lingkungan digital.
- Penurunan kerentanan terhadap pelanggaran terkait kata sandi dan akses tanpa izin.

### **1.6. Urgensi Penelitian**

Urgensi penelitian ini ditegaskan oleh meningkatnya frekuensi dan kompleksitas serangan siber. Saat metode perlindungan kata sandi tradisional terbukti tidak memadai, kebutuhan akan solusi yang cerdas dan adaptif menjadi mendesak.

### **1.7. Temuan yang Ditargetkan**

Penelitian ini bertujuan untuk memberikan wawasan mengenai:

- Efektivitas kata sandi yang dihasilkan oleh AI dalam menahan metode serangan umum.
- Adaptabilitas pembuat kata sandi yang diusulkan terhadap ancaman siber yang berkembang.
- Penerimaan dan kegunaan pengguna terhadap kata sandi yang dihasilkan oleh AI.

### **1.8. Kontribusi terhadap Ilmu Pengetahuan**

Penelitian ini memberikan kontribusi pada bidang keamanan siber dengan memperkenalkan pendekatan inovatif untuk pembuatan kata sandi. Penggunaan kecerdasan buatan dalam konteks ini mewakili perubahan paradigma, menawarkan solusi proaktif dan adaptif terhadap tantangan yang persisten dari serangan siber.

## **BAB 2. TINJAUAN PUSTAKA**

Bab ini menyajikan temuan dari penelitian sebelumnya yang dilakukan oleh peneliti lain, yang diperoleh dari literatur referensi dan menjadi landasan utama untuk pengembangan proposal ini. Tinjauan Pustaka bukan sekadar kumpulan teori; sebaliknya, ini merupakan rangkaian hasil yang diakui dan memiliki satu atau beberapa alur pemikiran tentang terjadinya suatu peristiwa ilmiah dalam suatu topik ilmiah yang akan dikaji atau diteliti. Sumber-sumber literatur yang diacu dalam bagian ini sebagian besar berasal dari jurnal ilmiah dan temuan penelitian terbaru yang dipublikasikan dalam 5 hingga 10 tahun terakhir.

Dalam konteks tinjauan pustaka ini, fokus kritis diberikan pada karya-karya yang secara langsung relevan dengan penggunaan algoritma Naive Bayes dalam aplikasi kecerdasan buatan (AI), khususnya dalam domain pembuatan kata sandi yang aman. Pemilihan literatur dipandu oleh pertimbangan aktualitas, kredibilitas, dan relevansi terhadap tujuan penelitian yang diusulkan.

### **2.1. Algoritma Naive Bayes dalam Aplikasi AI**

Beberapa penelitian dalam dekade terakhir telah menjelajahi efektivitas algoritma Naive Bayes dalam berbagai aplikasi kecerdasan buatan. Secara khusus, kesederhanaan algoritma, efisiensi komputasional, dan kemampuannya dalam mengatasi dataset besar menjadikannya pilihan yang menarik untuk tugas-tugas seperti klasifikasi dan pengenalan pola. Dalam konteks pembuatan kata sandi yang aman, penerapan Naive Bayes melibatkan pemanfaatan set data berlabel untuk melatih model membedakan antara kata sandi yang lemah, sedang, dan kuat.

### **2.2. Aplikasi dalam Keamanan Kata Sandi**

Literatur terkini telah menyoroti peran algoritma pembelajaran mesin, termasuk Naive Bayes, dalam memperkuat keamanan kata sandi. Sifat adaptif Naive Bayes memungkinkannya terus belajar dan beradaptasi dengan pola-pola baru yang muncul terkait kerentanan kata sandi. Temuan penelitian menegaskan potensinya dalam meningkatkan kekokohan sistem pembuatan kata sandi, sehingga mengurangi risiko terkait vektor serangan umum.

### **2.3. Batasan dan Tantangan**

Meskipun algoritma Naive Bayes memiliki kelebihan, penting untuk mengakui batasan dan tantangannya dalam konteks pembuatan kata sandi yang aman. Penelitian sebelumnya telah membahas masalah terkait asumsi independensi dan

potensi kerentanannya terhadap serangan yang canggih. Memahami batasan ini penting untuk implementasi yang efektif dari algoritma dalam generator kata sandi AI yang diusulkan.

#### **2.4. Integrasi dengan Set Data Berlabel**

Literatur telah menekankan pentingnya mengintegrasikan set data berlabel ke dalam proses pelatihan ketika menggunakan algoritma Naive Bayes. Pemanfaatan set data yang mengkategorikan kata sandi ke dalam kategori kekuatan (lemah, sedang, kuat) memfasilitasi proses pembelajaran algoritma, memungkinkannya membuat keputusan yang terinformasi dalam menghasilkan kata sandi yang sangat aman.

Tinjauan Pustaka ini membentuk pemahaman menyeluruh tentang lanskap pengetahuan yang ada terkait dengan algoritma Naive Bayes dalam konteks aplikasi kecerdasan buatan, khususnya dalam pembuatan kata sandi yang aman. Dengan mensintesis wawasan dari penelitian sebelumnya, bagian ini menjadi dasar untuk pengembangan dan implementasi proyek AI yang diusulkan selanjutnya.

### BAB 3. METODE RISET

Sebagai Metode Riset Model AI yang akan kami gunakan, 4 model yang akan kami pakai dan kami kira sesuai dengan project yang kami buat. Model tersebut adalah Naive Bayes, Logistic Regression, Stochastic Gradient Descent, dan Passive Aggressive Classifier dengan bahasa pemrograman Python.

Berikut adalah statistik hasil pengujian tingkat akurasi dari 4 model AI yang kami gunakan:

#### 1. Naive Bayes

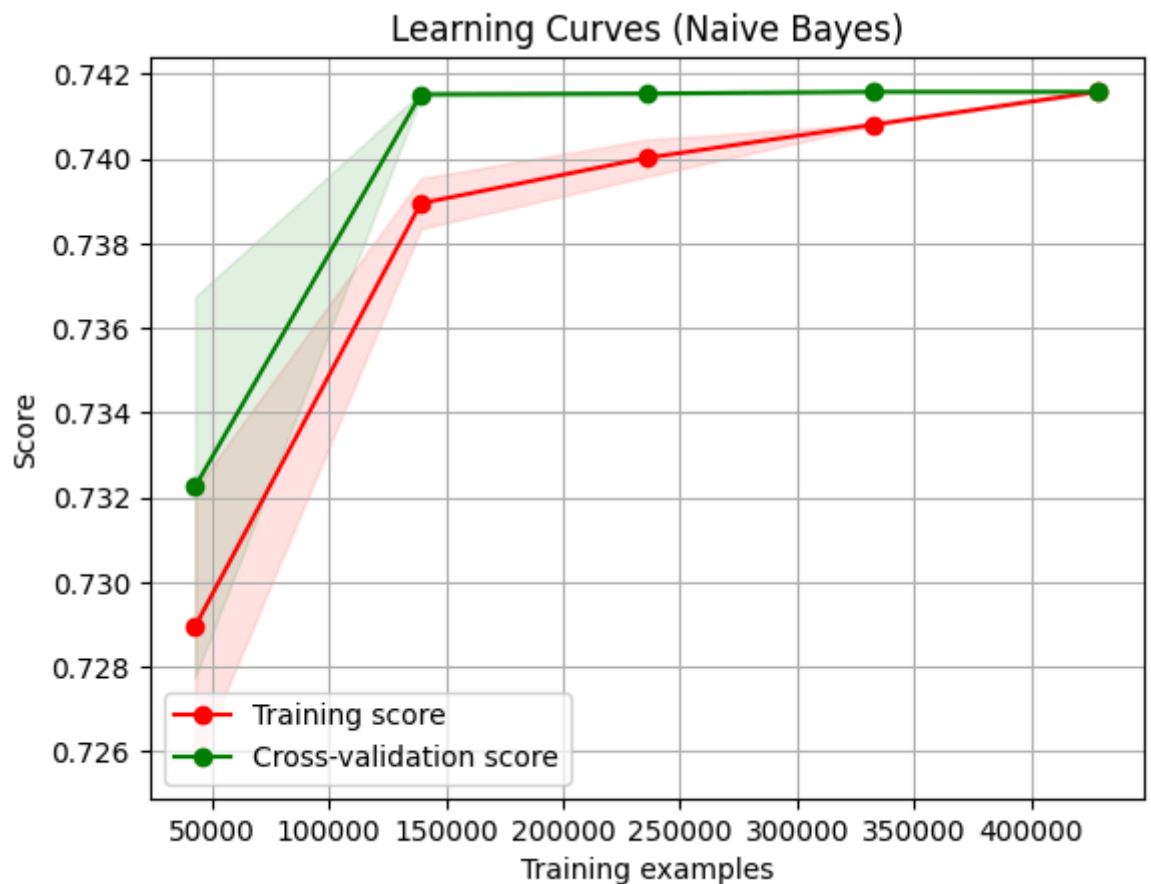
Accuracy : 0.7430

Precision : 0.5522

Recall : 0.7410

F1 Score : 0.6335

ROC AUC : 0.5443



## 2. Logistic Regression

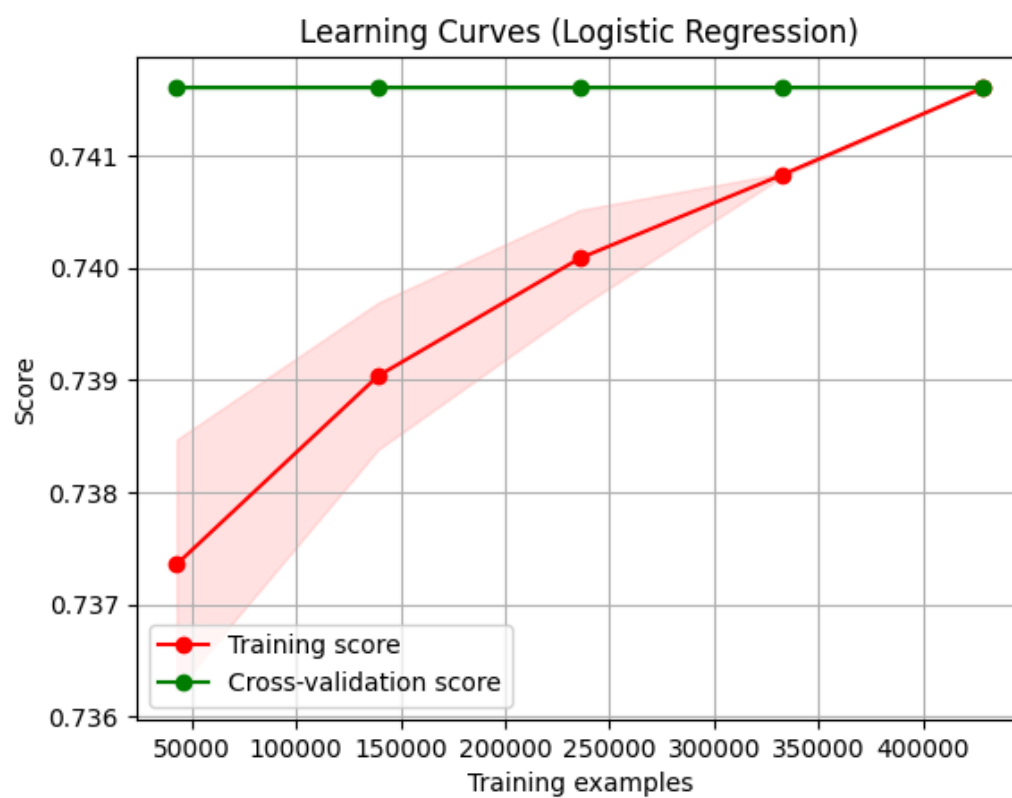
Accuracy : 0.7431

Precision : 0.5522

Recall : 0.7431

F1 Score : 0.6336

ROC AUC : 0.5278



### 3. Stochastic Gradient Descent

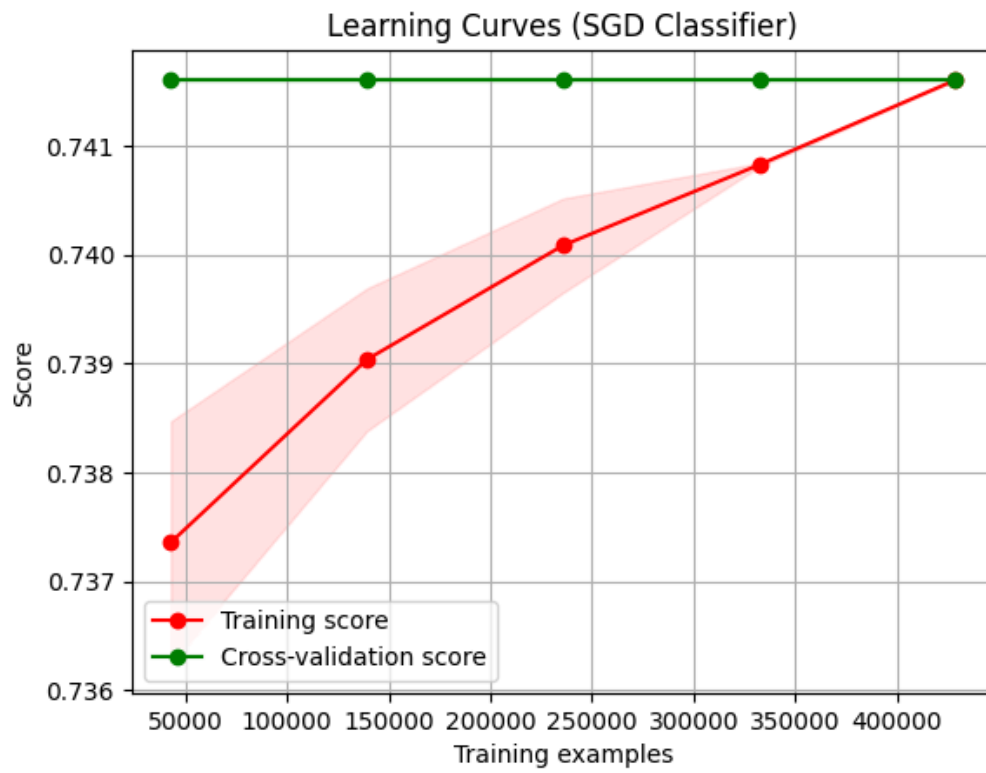
Accuracy : 0.7431

Precision : 0.5522

Recall : 0.7431

F1 Score : 0.6336

ROC AUC : 0.5272





#### 4. Passive Aggressive Classifier

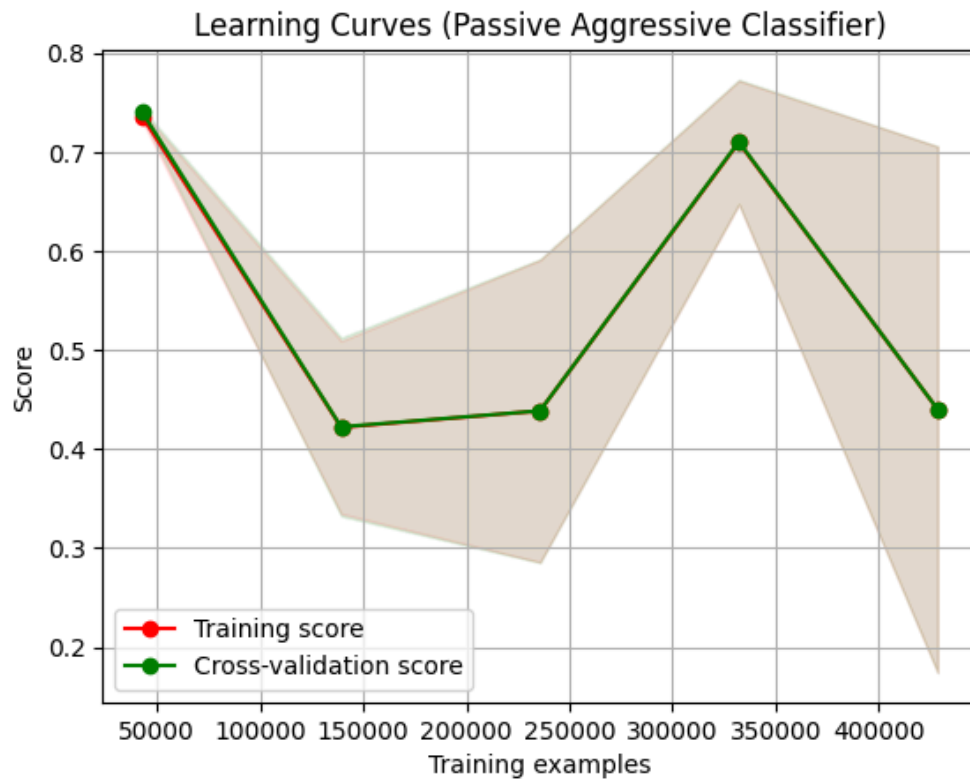
Accuracy : 0.7431

Precision : 0.5522

Recall : 0.7431

F1 Score : 0.6336

ROC AUC : 0.5



### **Kesimpulan Riset**

Dari perbandingan di atas, dapat dilihat bahwa model Logistic Regression, Stochastic Gradient Descent, dan Passive Aggressive Classifier memiliki akurasi, presisi, recall, dan f1-score yang mirip, di mana Naive Bayes memiliki akurasi terendah. Dengan passive aggressive classifier yang memiliki ROC AUC tertinggi diantaranya.

## BAB 4. BIAYA DAN JADWAL KEGIATAN

### 4.1 Anggaran Biaya

Tabel 4.1 Rekapitulasi Rencana Anggaran Biaya

N o	Jenis Pengeluaran	Sumber Dana	Besaran Dana (Rp)
1	Bahan habis pakai (contoh: ATK, kertas, bahan, dll) maksimal 60% dari jumlah dana yang diusulkan	Belmawa	Rp.0,00
		Perguruan Tinggi	Rp.0,00
		Instansi Lain (Jika ada)	Rp.0,00
2	Sewa dan jasa (sewa/jasa alat; jasa pembuatan produk pihak ketiga, dll), maksimal 15% dari jumlah dana yang diusulkan	Belmawa	Rp.4.000.00 0,00
		Perguruan Tinggi	Rp.1.000.00 0,00
		Instansi Lain (Jika ada)	Rp.0,00
3	Transportasi lokal maksimal 30% dari jumlah dana yang diusulkan	Belmawa	Rp.0,00
		Perguruan Tinggi	Rp.0,00
		Instansi Lain (Jika ada)	Rp.0,00
4	Lain-lain (contoh: biaya komunikasi, biaya bayar akses publikasi, dll) maksimal 15% dari jumlah dana yang diusulkan	Belmawa	Rp.3.000.00 0,00
		Perguruan Tinggi	Rp.750.000. 000,00
		Instansi Lain (Jika ada)	Rp.0,00
Jumlah			Rp.8.750.00 0,00
Rekap Sumber Dana		Belmawa	Rp.7.000.00 0,00
		Perguruan Tinggi	Rp.1.750.00 0,00
		Instansi Lain (Jika ada)	Rp.0,00
		Jumlah	Rp.8.750.00 0,00

## 4.2 Jadwal Kegiatan

Tabel 4.2 Jadwal Kegiatan

No	Jenis Kegiatan	Bulan				Penanggungjawab
		1	2	3	4	
1	Diskusi	X				Raziel Muhammad Bestari
2	Literature Review	X				Raziel Muhammad Bestari
3	Perancangan Model	X	X	X		Evan Gunawan
4	Perbandingan Model		X	X		Evan Gunawan
5	Pembuatan Laporan Kemajuan			X	X	Raziel Muhammad Bestari
6	Pembuatan Laporan Akhir			X	X	Raziel Muhammad Bestari
7	Pembuatan Artikel Ilmiah				X	Raziel Muhammad Bestari

## DAFTAR PUSTAKA

- Sanjay Murmu, Harsh Kasyap, & Tripathy, S. (2021). PassMon: A Technique for Password Generation and Strength Estimation. *Journal of Network and Systems Management*, 30(1). <https://doi.org/10.1007/s10922-021-09620-w>
- Bashar Saadoon Mahdi, Mustafa Jasim Hadi, & Abbas, A. R. (2022). Intelligent Security Model for Password Generation and Estimation Using Hand Gesture Features. *Big Data and Cognitive Computing*, 6(4), 116–116. <https://doi.org/10.3390/bdcc6040116>
- Faouzi Kamoun, Iqbal, F., Mohamed Amir Esseghir, & Baker, T. (2020). *AI and machine learning: A mixed blessing for cybersecurity*. <https://doi.org/10.1109/isncc49221.2020.9297323>
- Darbutaitė, E., Pavel Stefanovič, & Ramanauskaitė, S. (2023). Machine-Learning-Based Password-Strength-Estimation Approach for Passwords of Lithuanian Context. *Applied Sciences*, 13(13), 7811–7811. <https://doi.org/10.3390/app13137811>
- Farooq, U. (n.d.). *Real Time Password Strength Analysis on a Web Application Using Multiple Machine Learning Approaches*. <https://www.ijert.org/research/real-time-password-strength-analysis-on-a-web-application-using-multiple-machine-learning-approaches-IJERTV9IS120146.pdf>
- Seok Jun Kim, & Byung Mun Lee. (2023). Multi-Class Classification Prediction Model for Password Strength Based on Deep Learning. *Journal of Multimedia Information System*, 10(1), 45–52. <https://doi.org/10.33851/jmis.2023.10.1.45>

*Machine Learning-based Cyber Attacks Targeting on Controlled Information: A Survey*: *ACM Computing Surveys*: Vol 54, No 7. (2021). ACM Computing Surveys (CSUR). <https://dl.acm.org/doi/abs/10.1145/3465171>

Vijaya M.S, Jamuna K.S, & S. Karpagavalli. (2009). *Password Strength Prediction Using Supervised Machine Learning Techniques*. <https://doi.org/10.1109/act.2009.105>

## Lampiran 1. Biodata Ketua dan Anggota, serta Dosen Pendamping

### Biodata Ketua

#### A. Identitas Diri

1	Nama Lengkap	Evan Gunawan
2	Jenis Kelamin	Laki-laki
3	Program Studi	Cyber Security
4	NIM	2602079092
5	Tempat dan Tanggal Lahir	Jakarta, 20 Oktober 2004
6	Alamat E-mail	evan.gunawan001@binus.ac.id
7	Nomor Telepon/HP	081213386828

#### B. Kegiatan Kemahasiswaan Yang Sedang/Pernah Diikuti

No	Jenis Kegiatan	Status dalam Kegiatan	Waktu dan Tempat
1	FYP B27	Freshmen Leader & Freshmen Partner	September, Binus University
2			
3			

#### C. Penghargaan Yang Pernah Diterima

No.	Jenis Penghargaan	Pihak Pemberi Penghargaan	Tahun
1	-		
2			
3			

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan PKM-RE.

Jakarta, 08 01 2024

Ketua Tim



Evan Gunawan

## Biodata Anggota 1

## A. Identitas Diri

1	Nama Lengkap	Raziel Muhammad Bestari
2	Jenis Kelamin	Laki-laki / Perempuan
3	Program Studi	Cyber Security
4	NIM	2602064765
5	Tempat dan Tanggal Lahir	Jakarta, 2 Agustus 2002
6	Alamat E-mail	razielbestari@gmail.com
7	Nomor Telepon/HP	08118802829

## B. Kegiatan Kemahasiswaan Yang Sedang/Pernah Diikuti

No	Jenis Kegiatan	Status dalam Kegiatan	Waktu dan Tempat
1	-		
2			
3			

## C. Penghargaan Yang Pernah Diterima

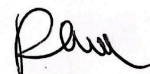
No.	Jenis Penghargaan	Pihak Pemberi Penghargaan	Tahun
1	-		
2			
3			

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan PKM-RE.

Jakarta, 08 Januari 2024

Anggota Tim



Raziel Muhammad Bestari



## Biodata Anggota 2

## A. Identitas Diri

1	Nama Lengkap	Ergan Ghiyasfari
2	Jenis Kelamin	Laki-laki
3	Program Studi	Cyber Security
4	NIM	2602181080
5	Tempat dan Tanggal Lahir	Jakarta, 3 Januari 2004
6	Alamat E-mail	ergan.ghiyasfari@binus.ac.id
7	Nomor Telepon/HP	08980608080

## B. Kegiatan Kemahasiswaan Yang Sedang/Pernah Diikuti

No	Jenis Kegiatan	Status dalam Kegiatan	Waktu dan Tempat
1	-		
2			
3			

## C. Penghargaan Yang Pernah Diterima

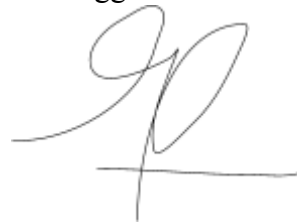
No.	Jenis Penghargaan	Pihak Pemberi Penghargaan	Tahun
1	-		
2			
3			

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan PKM-RE.

Jakarta, 08 01 2024

Anggota Tim



Ergon Ghiyasfari

## Biodata Dosen Pendamping

## A. Identitas Diri

1	Nama Lengkap (dengan gelar) Simeon Yuda Prasetyo, S.Kom., M.Kom.	
2	Jenis Kelamin	Laki-laki
3	Program Studi	Artifical Intelligence
4	NIP/NIDN	0326049801
5	Tempat dan Tanggal Lahir	
6	Alamat E-mail	simeon.prasetyo@binus.ac.id
7	Nomor Telepon/HP	0895386605050

## B. Riwayat Pendidikan

No	Jenjang	Bidang Ilmu	Institusi	Tahun Lulus
1	Sarjana (S1)			
2	Magister (S2)			
3	Doktor (S3)			

## C. Rekam Jejak Tri Dharma PT

## Pendidikan/Pengajaran

No	Nama Mata Kuliah	Wajib/Pilihan	sks
1.			
2.			

## Penelitian

No	Judul Penelitian	Penyandang Dana	Tahun
1.			
2.			

## Pengabdian Kepada Masyarakat

No	Judul Pengabdian kepada Masyarakat	Penyandang Dana	Tahun
1.			
2.			

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi. Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan PKM-RE.

Jakarta, 08 01 2024  
Dosen Pendamping

(Simeon Yuda Prasetyo,  
S.Kom., M.Kom.)