P-ISSN : 2502-3357
E-ISSN : 2721-284X

TANTANGAN DAN SOLUSI IMPLEMENTASI ANONIMISASI DAN PSEUDONIMISASI DATA DALAM SISTEM OPERASI WINDOWS

Rakhmadi Rahman S.T,M.Kom[1], Paulus Jemianus Ome [2], Farah Diyanah Adwah [3]
[123]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare

E-mail: paulusjemianusome@gmail.com

Abstrak

Pesatnya perkembangan teknologi informasi saat ini tidak dapat dibendungi seiring dengan perkembangan zaman dan merupakan bagian dari perkembangan dalam industri 4.0 menuai banyaknya data bermunculan per tahun nya, baik itu data perusahan, organisasi, maupun data pribadi, tentunya merupakan hal yang krusial dan perlu perlindungan yang lebih untuk menjaga data tersebut dari oknum yang ingin menyalah gunakan data pribadi sesorang dengan motif yang tidak etis bahkan memeras korban dengan meminta tebusan yang tidak sedikit. Dalam kajian ini membahas mengenai tantangan dan solusi penerapan anonimisasi data dan pseudonimisasi pada sistem operasi *Windows*, yang bertujuan untuk menjadi langkah awal bagaimana kita dapat melindungi data kita dengan menggunakan kedua konsep tersebut untuk melindungi data pribadi atau data sekelompok orang dari individu yang menyalah gunakan data informasi pribadi seseorang. Penelitian ini menggunakan metode penelitian skunder yang melibatkan dengan pengumpulan dan analisis data yang suda ada,seperti artikel, jurnal, dan sumber-sumber lainnya yang relevan, serta pengembang sistem menggunakan bahasa pemrograman *python* untuk mengimplementasikan konsep anonimisasi dan pseudonimisasi pada sistem operasi *windows*, sehinga dalam hasil penelitian ini menunjukan bahwa penerapan anonimisasi dan pseudonimisasi dapat meningkatkan perlindungan data pribadi atau menyamarkan data sebagai wujud perlindungan data.
Kata kunci: Anonimisasi, Pseudonimisasi, Keamanan Data, Privasi data, Sistem Operasi windows

Abstract

The rapid development of information technology today cannot be stopped along with the times and is part of developments in industry 4.0, reaping the large amount of data appearing every year, whether it is company, organizational or personal data, of course this is crucial and needs more protection. to protect this data from individuals who want to misuse someone's personal data with unethical motives and even blackmail the victim by asking for a large ransom. This study discusses the challenges and solutions for implementing data anonymization and pseudonymization on the Windows operating system, which aims to be the first step in how we can protect our data by using these two concepts to protect personal data or data of groups of people from individuals who misuse information data. someone's personality. This research uses secondary research methods which involve collecting and analyzing existing data, such as articles, journals and other relevant sources, as well as system developers using the Python programming language to implement the concepts of anonymization and pseudonymization on the Windows operating system, so that in The results of this research show that the application of anonymization and pseudonymization can increase the protection of personal data or disguise data as a form of data protection
.***Key word:*** *Anonymization, Pseudonymization, Data Security, Data privacy, Operating System window*

1) Pendahuluan

Dalam era digital yang semakin berkembang, identitas digital telah menjadi salah satu aset yang paling berharga. Informasi pribadi yang tidak terlindungi dengan baik dapat diekploitasi untuk berbagai tujuan yang tidak etis,seperti pencurian identitas, penipuan, dan pelangaran privasi. Ditengan ancaman ini, teknik anonimisasi dan pseudonimisasi muncul sebagai solusi kursial dalam perlindugan data pribadi sambil tetap memungkinkan pemrosesan dan analisi data(Narayana & Shamtikov,2010; El Emam et al.,2011; Fung et al. 2010).

Sistem operasi *Windows*, yang banyak digunakan di seluruh dunia, menjadi platform utama di mana data pribadi diproses dan disimpan. Mengingat luasnya penggunaan sistem operasi *Windows* dalam berbagai sektor, termasuk

P-ISSN : 1858-3938
E-ISSN : 2721-284X

kesehatan, keuangan, dan pemerintahan, penerapan teknik anonimisasi dan pseudonimisasi yang efektif di sistem ini sangat penting untuk memastikan keamanan dan privasi data serta memastikan bahwa teknik yang digunakan sesuai dengan regulasi privasi internasional seperti GDPR (*General Data Protection Regulation*) dan CCPA (*California Consumer Privacy Act*); integrasi teknologi kriptografi canggih untuk meningkatkan keamanan data yang dipseudonimkan; serta mengembangkan mekanisme untuk memantau dan mengaudit proses anonimisasi dan pseudonimisasi secara berkelanjutan (Narayana & Shmatikov, 2010; El Emam et al., 2011; Fung et al., 2010)

Dengan cara mengembangkan metode sistematis untuk mengidentifikasi dan mengamankan data sensitif dalam sistem operasi Windows, merancang dan mengimplementasikan algoritma anonimisasi dan pseudonimisasi yang efisien dan efektif, menerapkan teknik anonimisasi dan pseudonimisasi yang memenuhi persyaratan regulasi privasi, mengintegrasikan teknologi kriptografi atau teknik yang digunaka untuk elindungi informasi dengan mengubahnya menjadi format yang tidak dapat di baca oleh pihak yang tidak berwenang untuk meningkatkan keamanan data, serta mengembangkan sistem pemantauan dan audit untuk memastikan teknik yang digunakan tetap efektif dan sesuai regulasi. Dengan mengatasi tantangan-tantangan ini, penelitian ini berharap dapat memberikan kontribusi signifikan dalam meningkatkan keamanan dan privasi data pada sistem operasi Windows, sekaligus membantu organisasi untuk mematuhi regulasi privasi yang ketat. Penelitian ini tidak hanya relevan bagi para pengembang dan administrator sistem, tetapi juga bagi pembuat kebijakan dan peneliti yang bekerja di bidang keamanan dan privasi data (Narayana & Shmatikov, 2010; El Emam et al., 2011; Fung et al., 2010).

2) Metode Penelitian

Penelitian ini bertujuan untuk mengkaji tantangan dan solusi dalam penerapan teknik anonimisasi dan pseudonimisasi data pada sistem operasi Windows. Pendekatan yang digunakan dalam penelitian ini menggabungkan metode deskriptif dan eksperimental. Metode deskriptif digunakan untuk menggambarkan fenomena yang ada, sedangkan metode eksperimental digunakan untuk menguji solusi yang diusulkan dalam konteks yang terkendali. Pengumpulan data yang digunakan dalam penelitian ini dikumpulkan melalui dua sumber utama : literatur skunder dan eksperimen langsung

i. Literature Skunder Penelitian ini memanfaatkan berbagai sumber literature yang relevan, termasuk artikel jurnal ilmiah, buku, dan publikasi online lainnya. Studi literatur ini bertujuan untuk memahami tantangan yang telah diidentifikasi sebelumnya dan solusi yang telah diusulkan dalam konteks anonimisasi dan pseudonimisasi data. Literatur yang dikaji mencakup topik-topik seperti teknik anonimisasi, teknik pseudonimisasi, regulasi privasi data, dan teknologi kriptografi. Sumber literatur ini memberikan dasar teoritis yang kuat untuk penelitian dan membantu dalam merumuskan hipotesis serta desain eksperimen
ii. Eksperimen Langsung, data eksperimental dikumpulkan dengan menerapkan teknik anonimisasi dan pseudonimisasi pada set data yang dipilih. Eksperimen ini dilakukan untuk menguji kinerja dan efektivitas solusi yang diusulkan dalam mengatasi tantangan yang telah diidentifikasi. Set data yang digunakan mencakup berbagai jenis informasi sensitif yang umum ditemukan dalam sistem operasi Windows, seperti data kesehatan, data keuangan, dan informasi pribadi lainnya.
iii. Desain Eksperimen desain eksperimen melibatkan tahapan yang sitematis, dengan melakukan penentuan set data yang akan digunakan dalam eksperimen ditentukan dengan mempertimbangkan berbagai jenis informasi sensitif yang umum dalam konteks sistem operasi Windows. Data ini mencakup informasi seperti data pasien dalam konteks kesehatan, data transaksi dalam konteks keuangan, dan informasi pribadi lainnya.kemudian mengidentifikasi tekninya seperti teknik anonimisasi dan pseudonimisasi yang akan diuji diidentifikasi berdasarkan studi literatur yang telah dilakukan. Teknik-teknik yang diuji mencakup hashing kriptografis (sepertiSHA256), K-anonymity, L-diversity, T-closeness, dan metode enkripsi. Dan yang terahir mengenai pengembagan skrip/program yang dikembangkan untuk menrapkan teknik-teknik yang telah diidentifikasi pada set data yang dipilih. Pengembangan ini melibatkan penulisan kode untuk menerapkan algoritma hashing, enkripsi, dan metode anonimisasi lainnya.
iv. Analisis data dan validasi hasil data yang dikumpulkan dari eksperimen dianalisis mengunakan analisis kualitatif. Analisis ini mengevaluasi kesesuaian teknik yang

P-ISSN : 2502-3357
E-ISSN : 2721-284X

digunakan dengan persyaratan regulasi seperti GDPR dan CCPA, serta dampak teknik terebut terhadap kegunaan data. Analisis kuatitatif juga melibatkan penilaian terhadap kemudahan iplementasi dan potensi risiko yang terkait dengan penggunaan teknik tersebut. Sedangkan untuk memastikan validasi dan relibilitas penelitian dilakukan beberapa langkah validasi seperti uji joba tambahan, eksperimen tambahan dengan dilakukan dengan mengunak dengan menggunakan set data yang berbeda untuk memastikan koneksistensi hasil. Uji coba ini membantu mengidentifikasi potensi variabilitas dalam hasil dan memastikan bahwa temuan penelitian dapat digeneralisasikan ke berbagai jenis data. Dan terahir melakikan preer review terhadapa ahli bidang privasi data dan keamanan informasi yang membantu mengidentifikasi kelemahan dalam desain eksperimen dan analisi data dan saran pengembangan.

3) Hasil Penelitian dan Pembahasan

Pseudomimisasi/penyamaran adalah perlindungan yang mengurangi keterhubungan data dengan subjek data. Artinya, Anda melakukan de-identifikasi data sedemikian rupa sehingga data tersebut tidak dapat lagi mengarah pada identifikasi tanpa informasi tambahan. Secara teori, menghapus informasi tambahan ini akan menghasilkan data yang dianonimkan. Dalam makalah "Teknik Anonimisasi Data di Sistem Operasi Modern" menekankan pentingnya teknika anonimisasi dalam menjaga kerahasiaan data pribadi di sistem operasi terkini. Mereka menjelaskan berbagai metode, termasuk generalisasi, perturbasi, dan penerapan algoritma kriptografi. Studi ini juga mencakup tantangan implementasiteknik-teknik tersebut dalam hal kinerja sistem dan kebutuhan untuk mengurangi risiko identifikasi ulang individu (smith dan Doe,2019)

Namun dibalik itu semua perlu memperhatikan bagaiaman tantaganya dalam penerapannya dalam penelitian yang dilakukan oleh (Brown, 2020) berjudul "Tantangan dalam Pseudonimisasi Data: Sebuah Perspektif Teknis," dia mengidentifikasi beberapa tantangan teknis dalam proses pseudonimisasi. Penelitian tersebut menyoroti kesulitan dalam menjaga kegunaan data setelah dilakukan proses pseudonimisasi serta risiko reidentifikasi melalui teknik de-anonimisasi. Brown juga menekankan pentingnya menjaga keseimbangan antara privasi dan kegunaan data, serta perlunya pendekatan teknis yang inovatif untuk mengatasitantangan tersebut, dalam artikel yang berjudul "Implementing GDPR Compliance through Data Pseudonymization," Garcia dan (Lopez,2021 membahas bagaimana pseudonimisasi dapat digunakan untuk memenuhi persyaratan kepatuhan GDPR. Mereka mengungkapkan bahwa pseudonimisasi adalah metode yang efektif untuk meningkatkan perlindungan data pribadi. Artikel ini menyajikan contoh-contoh implementasi praktis serta analisis efektivitas teknik ini di berbagai industri. Selain itu, Garcia dan Lopez menekankan pentingnya regulasi dalam mendorong adopsi praktik pseudonimisasi secara lebih luas.

Pseudonimisasi sering diartikan sebagai penggantian pengenal langsung (misalnya nama) dengan nama samaran , dan menyimpan hubungan antara pengenal dan nama samaran dalam file kunci, terpisah dari data penelitian. Meskipun ini merupakan praktik yang baik (hal ini memastikan bahwa data tidak lagi dapat diidentifikasi secara langsung), penafsiran nama samaran ini tidak memperhitungkan informasi yang dapat diidentifikasi secara tidak langsung , sehingga tidak serta merta memenuhi definisi nama samaran GDPR Anonimisasi adalah proses de-identifikasi yang menghasilkan data "dijadikan anonim sedemikian rupa sehingga subjek data tidak atau tidak lagi dapat diidentifikasi", baik secara langsung maupun tidak langsung, dan oleh siapa pun. Jika data dianonimkan, data tersebut bukan lagi data pribadi, sehingga tidak lagi tunduk pada GDPR. Namun perlu diperhatikan bahwa semua yang lakukan sebelum data dianonimkan (termasuk anonimisasi itu sendiri) tunduk pada GDPR!

3.1 Pseudonimisasi Dalam Sistem Operasi Windows

Pseudonimisasi adalah salah satu metode perlindungan data yang efektif, di mana informasi yang dapat mengidentifikasi individu digantikan dengan pengenal atau kode fiktif. Dalam konteks sistem operasi Windows, penerapan pseudonimisasi memerlukan pendekatan yang komprehensif dan teknis untuk memastikan keamanan data pribadi. Windows sebagai sistem operasi yang kompleks menyimpan data di berbagai lokasi, termasuk registry, file sistem, dan aplikasi. Tantangan utama dalam penerapan pseudonimisasi pada Windows melibatkan identifikasi lokasi data sensitif, penggantian informasi dengan kode fiktif, dan pengelolaan hubungan antara data asli dan data pseudonimisasi.

P-ISSN : 1858-3938
E-ISSN : 2721-284X

3.1.1. Kompleksitas Teknikal dalam Pseudonimisasi

Pseudonimisasi di Windows memerlukan pemahaman mendalam tentang struktur data dan bagaimana data tersebut digunakan oleh sistem dan aplikasi. Registry Windows, misalnya, menyimpan konfigurasi sistem dan aplikasi yang dapat berisi informasi sensitif. Selain itu, file sistem Windows yang berfungsi sebagai repositori utama untuk penyimpanan data juga dapat berisi informasi pribadi yang perlu disamarkan. Pseudonimisasi harus dilakukan dengan hati-hati agar tidak merusak integritas data atau mempengaruhi kinerja aplikasi yang mengandalkan data tersebut

1) AlgoritmaEfisien untuk Pseudonimisasi: Salah satu solusi untuk menangani kompleksitas teknikal adalah denganmengembangkan algoritma yang efisien untuk pseudonimisasi. Algoritma ini harus mampu menangani volume datayang besar dengan cepat dan tanpa mengorbankan kinerja sistem. Contoh algoritma yang dapat digunakan termasukhashing kriptografis seperti SHA-256, yang menggantikan informasi sensitif dengan hash yang tidak dapat diubah kembali ke data asli.
2) Penggunaan Teknologi Kriptografi: Teknologi kriptografi berperan penting dalam pseudonimisasi. Dengan menggunakan teknik seperti hashing dan enkripsi, data yang sensitif dapat digantikan dengan token yang aman. Misalnya, penggunaan hash kriptografis untuk menggantikan nama, alamat, dan nomor telepon dalam dataset dapatmeningkatkan keamanan data.

3.1.2. Dampak pada kinerja Sistem

Proses pseudonimisasi dapat mempengaruhi kinerja sistem operasi, terutama jika dilakukan secara realtime atau pada data dalam jumlah besar. Pseudonimisasi memerlukan sumber daya komputasi yang signifikan, seperti CPU dan memori, yang dapat mempengaruhi kinerja aplikasi lain yang berjalan disistem yang sama. Oleh karena itu, perlu adanya strategi untuk mengurangi dampak ini diantaranya

Automasi Proses: Automasi dalam proses pseudonimisasi dapat membantu mengurangi beban kerja manual dan memastikan konsistensi dalam penerapan teknik ini di seluruh sistem. Misalnya, penggunaan skrip atau program otomatis yang dapat menjalankan pseudonimisasi pada data baru secara berkala dapat mengurangi beban pada sumber daya komputasi.

Pemantauan dan Audit: Implementasi sistem pemantauan dan audit yang efektif dapat membantu mengidentifikasi dan mengatasi masalah kinerja yang muncul selama proses pseudonimisasi. Sistem ini juga dapat memastikan bahwa proses pseudonimisasi dilakukan sesuai dengan standar yang ditetapkan dan tidak menyebabkan kebocoran data pribadi.

3.2. Anonimisasi dalam Sistem Operasi Windows

Anonimisasi adalah proses yang lebih ketat dibandingkan pseudonimisasi, di mana informasi yang dapat mengidentifikasi individu dihapus sepenuhnya sehingga data tersebut tidak lagi dapat digunakan untuk mengidentifikasi seseorang, baik secara langsung maupun tidak langsung. Anonimisasi data dalam sistem operasi Windows menghadirkan tantangan teknis yang signifikan karena kompleksitas data yang ada di berbagai lokasi.

3.2.1. Metode Anonimisasi yang Digunakan

Berbagai metode anonimisasi dapat diterapkan untuk menghapus informasi yang dapat mengidentifikasi individu. Metode yang umum digunakan meliputi generalisasi, di mana data yang spesifik diubah menjadi data yang lebih umum, dan perturbasi, di mana data asli dimodifikasi dengan menambahkan noise atau nilai acak. Implementasi metode ini dalam Windows memerlukan pemahaman mendalam tentang struktur dan penggunaan data di sistem operasi.

1) **Generalisasi dan Perturbasi**: Dalam konteks Windows, generalisasi dapat diterapkan dengan menggantikan informasi spesifik seperti alamat rumah dengan informasi yang lebih umum seperti nama kota atau kode pos. Perturbasi dapat diterapkan dengan memodifikasi nilai-nilai dalam dataset sehingga data tersebut tidak lagi dapat digunakan untuk mengidentifikasi individu secara langsung.
2) **K-anonymity, L-diversity, dan T-closeness**: Metode-metode ini dapat digunakan untuk meningkatkan tingkat anonimisasi data. K-anonymity memastikan bahwa setiap record dalam dataset tidak dapat dibedakan dari setidaknya K-1 record lainnya berdasarkan informasi identitas yang tersamar. L-diversity memastikan bahwa setiap grup anonim mengandung setidaknya L nilai yang berbeda untuk atribut sensitif. T-closeness memperluas konsep ini dengan memastikan bahwa distribusi atribut sensitif dalam setiap grup anonim mendekati distribusi dalam seluruh dataset.

P-ISSN : 2502-3357
E-ISSN : 2721-284X

3.2.2. Tantangan Kepatuhan terhadap Regulasi

Kepatuhan terhadap regulasi privasi seperti GDPR di Eropa dan CCPA di Amerika Serikat memerlukan mekanisme yang dapat menjamin bahwa data yang dianonimkan sesuai dengan standar yang ditetapkan. Regulasi ini menetapkan persyaratan yang ketat untuk perlindungan data pribadi dan memberikan panduan tentang bagaimana data harus dianonimkan.

1) **Implementasi Regulasi GDPR dan CCPA**:Untuk memastikan kepatuhan terhadap GDPR dan CCPA, proses anonimisasi harus dirancang sedemikian rupa sehingga data yang telah dianonimkan tidak lagi dapat digunakan untuk mengidentifikasi individu, baik secara langsung maupun tidak langsung. Ini memerlukan penggunaan metode anonimisasi yang kuat dan audit berkala untuk memastikan bahwa data tetap anonim.
2) **Pemantauan dan Audit**: Sistem pemantauan dan audit yang efektif dapat membantu memastikan bahwa proses anonimisasi dilakukan sesuai dengan persyaratan regulasi. Pemantauan ini juga dapat mendeteksi kebocoran data pribadi dan memungkinkan tindakan korektif segera.

3.2.3. Implementasi Pseudonimisasi dan Anonimisasi dalam Berbagai Bidang

Pseudonimisasi dan anonimisasi data adalah teknik yang sangat penting dalam menjaga privasi dan keamanan informasi pribadi dalam berbagai bidang. Implementasi teknik ini memiliki tantangan dan kebutuhan khusus di setiap bidang, seperti kesehatan, keuangan, dan pemerintahan. Dalam penjelasan ini, akan dibahas secara mendetail bagaimana teknik-teknik ini diterapkan di masing-masing bidang, dengan contoh kode dan penjelasan yang rinci.

3.2.3.1. Implementasi dalam Bidang Kesehatan

Pseudonnimisasi dalam Rekam Medis Elektronik(EMR) yang menyimpan informasi penting tentang pasien, termasuk data identifikasi pribadi seperti nama, alamat, dan nomor telepon, serta informasi medis seperti riwayat penyakit dan hasil tes. Perlindungan data ini sangat penting untuk mematuhi regulasi seperti Health Insurance Portability and Accountability Act (HIPAA) di Amerika Serikat. Pseudonimisasi dapat digunakan untuk menggantikan informasi identifikasi pribadi dengan token atau hash yang aman.

```python
import hashlib

def pseudonymize_patient_data(patient_data):
    """Menggantikan data pasien sensitif dengan hash SHA-256"""
    pseudonymized_data = {}
    for key, value in patient_data.items():
        if key in ['nama', 'alamat', 'nomor_telepon']:
            hash_object = hashlib.sha256(value.encode())
            pseudonymized_data[key] = hash_object.hexdigest()
        else:
            pseudonymized_data[key] = value
    return pseudonymized_data

# Contoh data pasien
data_pasien = {
    'nama': 'Widya Putri',
    'alamat': 'Suppa',
    'nomor_telepon': '1234-5678',
    'riwayat_penyakit': 'Demam'
}

# Menerapkan pseudonimisasi pada data pasien
data_pseudonim = pseudonymize_patient_data(data_pasien)

print("Data Pseudonimisasi Pasien:")
for key, value in data_pseudonim.items():
    print(f"{key}: {value}")
```

Output:

```
Data Pseudonimisasi Pasien:
nama: 85df00e9484ead3fb07a6abdb0330f725698d977a43f405b21e6c6e12ccb2a6f
alamat: 0438db34d72590c816c5872c7b5f85bc6865b12528213fbb3d8ddc2c2fb0b50e
nomor_telepon: e5957e85064b1fe6de6a4e54ef2f50e4024a48a40ff17711e740d6c119e9d796
riwayat_penyakit: Demam
```

Gambar 1. Contoh penerapan Pseudonimisasi data pasien (Sumber : Visual Studio Code)

Pada contoh di atas, data pasien seperti nama, alamat, dan nomor telepon digantikan dengan hash SHA-256, yang merupakan bentuk pseudonimisasi. Hash ini unik untuk setiap input dan sulit untuk dikembalikan ke bentuk aslinya tanpa mengetahui input aslinya dan adapun Riwayat penyakitnya Tetap tidak berubah karena tidak mengandung informasi identifikasi pribadi.

Anonimisasi dalam Data Penelitian Kesehatan: Data penelitian kesehatan seringkali memerlukan anonimisasi lengkap untuk memastikan bahwa data tersebut tidak dapat dikaitkan kembali ke individu tertentu. Metode seperti generalisasi dan perturbasi digunakan untuk menghapus atau menyamarkan informasi identifikasi.

```python
import random

def anonymize_research_data(research_data):
    """Menganonimkan data penelitian dengan menghapus informasi identifikasi"""
    anonymized_data = []
    for record in research_data:
        anonymized_record = {key: value for key, value in record.items() if key not in ['nama', 'alamat', 'nomor_telepon']}
        anonymized_record['usia'] = random.randint(20, 80)  # Menambahkan noise pada data usia
        anonymized_data.append(anonymized_record)
    return anonymized_data

# Contoh data penelitian
data_penelitian = [
    {'nama': 'Ayu Anugra', 'alamat': 'Barru', 'nomor_telepon': '5678-1234', 'usia': 19, 'riwayat_penyakit': 'Asam Lambung'},
    {'nama': 'Widya Putri', 'alamat': 'Suppa', 'nomor_telepon': '1234-5678', 'usia': 18, 'riwayat_penyakit': 'Demam'}
]

# Menerapkan anonimisasi pada data penelitian
data_anonim = anonymize_research_data(data_penelitian)

print("Data Anonimisasi Penelitian:")
for record in data_anonim:
    print(record)
```

Output:

```
Data Anonimisasi Penelitian:
{'usia': 20, 'riwayat_penyakit': 'Asam Lambung'}
{'usia': 50, 'riwayat_penyakit': 'Demam'}
```

Gambar 2. Contoh penerapan Anonimisasi data pasien (Sumber : Visual Studio Code)

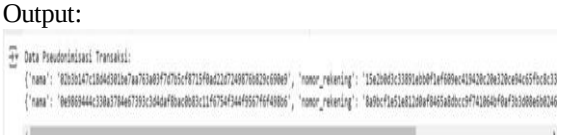
P-ISSN : 1858-3938
E-ISSN : 2721-284X

Pada contoh di atas, informasi identifikasi seperti nama, alamat, dan nomor telepon dihapus dari data penelitian, dan noise ditambahkan pada data usia untuk mengurangi risiko identifikasi kembali.

3.2.3.2. Implementasi dalam Bidang Keuangan

Dalam industri keuangan, melindungi data pelanggan merupakan hal yang sangat penting untuk mencegah penipuan dan pencurian identitas. Denngan demikian pseudonimisasi dapat digunakan untuk melindungi data transaksi keuangan dengan menggantikan informasi identifikasi seperti nama serta nomor rekening dengan token yang aman.

Output:



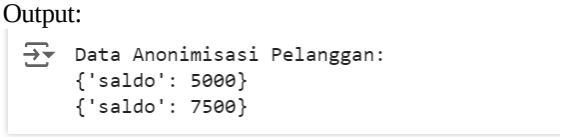
Gambar 3. Contoh penerapan Pseudonimisasi data keuangan (Sumber : Visual Studio Code)

Pada contoh diatas, menerapkan bagaimana teknik pseudonimisasi mentikan nama, dan nomor rekening pelangan demgam hash SHA-256, sehinga data transaksi tetap dapat dianalisis tampa mengungkap identitas pelangan.

3.2.3.3. Anonimisasi Dalam Transaksi Keuangan

Anonimisasi data pelanggan memastikan bahwa informasi pribadi seperti nama, alamat, dan rekening dihapus atau disamarkan sehinga tidak dapat diidentifikasi kembali. Inilah pentingnya untuk melindungi privasi pelanggan dan mematuhi regulasi privasi data.

Output:



Gambar 4. Contoh penerapan Anonimisasi Data Transaksi (Sumber : Visual Studio Code)

Pada contoh di atas, informasi pribadi seperti nama, alamat dan nomor rekening dihapus sehingga daata pelanggan dapat digunakan unutuk analisis resiko mengungkap identitas individu.

3.2.3.4. Implementasi Dalam Bidang Pemerintah

Data sensus mengandung informasi pribadi yang sangat sensitif dan perlu dilindungi untuk menjaga privasi warga negara. Pseudonimisasi dapat digunakan untuk menggantikan informasi identifikasi dengan token yang aman, sehingga data sesus tetap dianalisis tampa mengunakan identitas individu.

Output:

Gambar 5. Contoh penerapan Pseudonimisasi Data sensus (Sumber : Visual Studio Code)

Pada contoh di atas , nama warga Negara dalam data sensus diganti dengan hash SHA-256, sehingga informasi identifikasi pribadi terlindungi.

3.2.3.5. Anonimisasi Dalam Data Kriminal

Anonimisasi dalam data kriminal untuk menghapus atau menyamarkan informasi identifikasi pribadi, sehinga data tidak dapat dikaitkan kembali ke individu tertentu. Ini penting untuk melindungi privasi privasi individu yang terlibat dalam kasus kriminal

P-ISSN : 2502-3357
E-ISSN : 2721-284X

```python
def anonymize_criminal_data(criminal_data):
    """Menganonimkan data kriminal dengan menghapus informasi identifikasi"""
    anonymized_data = []
    for record in criminal_data:
        anonymized_record = {key: value for key, value in record.items() if key not in ['nama', 'alamat']}
        anonymized_data.append(anonymized_record)
    return anonymized_data

# Contoh data kriminal
data_kriminal = [
    {'nama': 'Paulus Jimi', 'alamat': 'NTT', 'kejahatan': 'Pencurian', 'hukuman': '3 tahun'},
    {'nama': 'Farah Diyanah', 'alamat': 'Parepare', 'kejahatan': 'Penipuan', 'hukuman': '2 tahun'}
]

# Menerapkan anonimisasi pada data kriminal
data_anonim = anonymize_criminal_data(data_kriminal)

print("Data Anonimisasi Kriminal:")
for record in data_anonim:
    print(record)
```

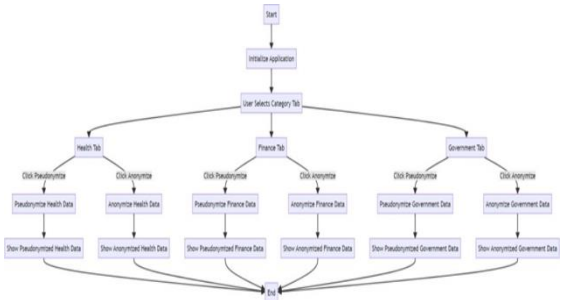
Output:

```
Data Anonimisasi Kriminal:
{'kejahatan': 'Pencurian', 'hukuman': '3 tahun'}
{'kejahatan': 'Penipuan', 'hukuman': '2 tahun'}
```

Gambar 6. Contoh penerapan Anonimisasi Data Kriminal (Sumber : Visual Studio Code)

Pada contoh di atas identitas pelaku kriminal seperti nama serta alamat dapat di lindungi dengan metode anonimisasi data diatas.

Pada penerapan yang dilakukan tentunya melalui model diagram alur yang menjadi dena ritem yang dilakukan sistem seperti dalam penjelasan diagram alur berikut ini:



Gambar 7. Diagram Alur Sistem

Dalam diagram alur sistem di atas menyajikan :

1) **Start**: Awal dari alur aplikasi.
2) **Initialize Application**: Membuat jendela utama aplikasi dan menyiapkan tab untuk berbagai kategori data (Kesehatan, Keuangan, Pemerintahan).
3) **User Selects Category Tab**: Pengguna memilih salah satu tab (Kesehatan, Keuangan, Pemerintahan).
4) **Click Pseudonymize**: Pengguna mengklik tombol untuk pseudonimisasi data di kategori yang dipilih.
5) **Pseudonymize Health Data**: Proses pseudonimisasi untuk data kesehatan.
6) **Pseudonymize Finance Data**: Proses pseudonimisasi untuk data keuangan.
7) **Pseudonymize Government Data**: Proses pseudonimisasi untuk data pemerintahan.
8) **Show Pseudonymized Data**: Menampilkan hasil pseudonimisasi kepada pengguna.
9) **Click Anonymize**: Pengguna mengklik tombol untuk anonimisasi data di kategori yang dipilih.
10) **Anonymize Health Data**: Proses anonimisasi untuk data kesehatan.
11) **Anonymize Finance Data**: Proses anonimisasi untuk data keuangan.
12) **Anonymize Government Data**: Proses anonimisasi untuk data pemerintahan.
13) **Show Anonymized Data**: Menampilkan hasil anonimisasi kepada pengguna.
14) **End**: Akhir dari alur aplikasi

4) Kesimpulan

Penelitian ini bertujuan utuk mengidentifikasi tantangan serta solusi dala penerapan teknik anonimisasi dan peseudonimisasi data pada sistem operasi *windows*, dengan harapan dapat mengembangkan langkah-langkah efektifit untuk melindungi data pribadi dari penyalagunaan dan memastikan kepatuhan terhadapa regulasi privasi seperti GDPR dan CCPA.

Dari hasil penelitian ini dapat disipulkan bahwa teknik anonimisasi dan pseudonimisasi secara signifikan meningkatkan perlindungan data pribadi. Pseudonimisasi, yang menggantikan informasi dengan pengenal fiktif, memerlukan penerapan algoritma yang efesisen seperti hashing kriptografi dab teknologi enkripsi untuk menjaga keamanan data tampa mengorbankan kinerja sistem. Di sisi lain, anonimisasi, yang menghapus seluru informasi identifikasi, tentunya memanfaatkan metode seperti generalisasi dan perturbasi untuk memastikan bahwa data tidak dapat dikaitkan kembali kepada individu tertentu .

Implemntasi teknik-teknik ini diterapkan dalam berbagai sektor, seperti kesehatan, dan keuangan menunjukan bahwa meskipun terdapat sejumlah tantangan teknis dan regulasi, solusi yang komprehensif dapat dihasilkan melalui pendekatan sistemtis serta penerapan teknologi yang tepat. Contoh nyata penerapan pseudonimisasi dalam penelitian kesehatan menegaskan efektifitas teknik-teknik ini dalam melindungi privasi individu.

Terkait pengembangan selanjutnya, disarankan agar penelitian lebih difokuskan pada pengembangan algoritma yang lebi inovatif dan metode yang lebih efesien untuk anonimisasi dan

P-ISSN : 1858-3938
E-ISSN : 2721-284X

pseudonimisasi. Serta pengembanngan sistem pemantauan dan audit yang lebih canggih juga sngat diperlukan untuk memastikan efektifitas dan kepatuhan terhadap regulasi privasi yang terus berkembang. Selain itu, ekplorasi terhadap integrasi teknologi kecerdasan buatan dan pembelajarasan mesin dapat meningkatkan otomasi serta akurasi dalam proses perlindungan data. Dengan mengatasi berbagai tantangan ini, diharapkan organisasi dapat meningkatkan keamanan data pribad, mematuhi standar privasi yang ketat, dan melindungi data dari potensi penyalagunaan dalam era digital yang semakin kompleks.

5) Referensi

Narayana, S., & Shmatikov, V. (2010). Myths and Fallacies of "Personally Identifiable Information". _Communications of the ACM, 53(6), 24-26.

El Emam, K., Jonker, E., Arbuckle, L., & Malin, B. (2011). *_A Systematic Review of Re-Identification Attacks on Health Data_ . _PLOS ONE_* , 6(12), e28071.

Fung, B. C. M., Wang, K., Chen, R., & Yu, P. S. (2010). *_Privacy-preserving Data Publishing_ : _A Survey of Recent Developments_ . _ACM Computing Surveys (CSUR)_* , 42(4), 1-53.

Brown, D. (2020). Challenges in Data Pseudonymization: *A Technical Perspective. Journal of Information Security and Applications*, 52, 102487.

Garcia, M., & Lopez, M. (2021). *Implementing GDPR Compliance through Data Pseudonymization. Data & Knowledge Engineering_* , 130, 101895.

Pfitzmann, A., & Hansen, M. (2010). *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management A Consolidated Proposal for Terminology. In Proceedings of the 1st German Conference on IT-Security* (IT-Security), 1-28.

Sweeney, L. (2002). k-Anonymity: *A Model for Protecting Privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5), 557-570.

O'Flaherty, R. (2015). *The Role of Pseudonymization in Data Protection. Journal of Data Protection & Privacy*, 1(1), 62-74.

Rannenberg, K., & Gollmann, D. (2006). *The Role of Data Pseudonymization in Privacy Protection. Privacy and Identity Management for Life*, 215-234.