BAB VI KESIMPULAN DAN SARAN

6.1 Kesimpulan

Secara keseluruhan, implementasi *data masking* adalah langkah yang penting untuk melindungi informasi sensitif dalam data. Dengan memperhatikan performa, kesalahan klasifikasi, dan kesesuaian data, implementasi *data masking* dapat meningkatkan keamanan data dan menjaga privasi informasi secara efektif.

Kesimpulan tersebut menunjukkan bahwa implementasi *data masking* ini telah memberikan hasil yang cukup baik dalam melindungi informasi sensitif dan mengklasifikasikan data dengan benar. Namun, tetap ada ruang untuk perbaikan dan peningkatan kinerja metode *masking* yang dapat dilakukan dengan melakukan analisis dan penyesuaian lebih lanjut terhadap proses *masking* yang digunakan.

Secara keseluruhan, implementasi *data masking* memiliki beberapa kesimpulan:

1. Pemilihan metode *masking* yang tepat sangat penting untuk mencapai hasil yang diinginkan, terutama untuk proses transformasi di *ETL*. Metode *masking* yang dipilih juga harus sesuai dengan jenis data dan tingkat sensitivitasnya. Selain itu, perhatian juga perlu diberikan pada kebutuhan regulasi dan privasi yang berlaku. Dengan demikian, *data masking* dapat diimplementasikan, terutama pada proses transformasi *ETL*.

2. Implementasi *data masking* efektif dalam melindungi informasi sensitif yang ada dalam data, terutama pada proses transformasi *ETL*. Proses *masking* lebih sederhana, dibandingkan harus mengimplementasikannya di

level *database*. *Data masking* yang diimplementasikan di proses transformasi *ETL*, cukup dengan menambahkan beberapa transformasi sederhana di workflow, sehingga hal ini yang membuat efektifnya proses *data masking* di *ETL*, karena akan menghasilkan output yang sudah di*masking*, terutama untuk data *staging* dan data sebelum diload ke *database*.

3. Efektifitas implementasi *data masking* pada proses transformasi, dapat di ukur dan dievaluasi dengan cara membandingkan kompleksitas proses dan juga waktu yang dibutuhkan untuk mengolah data dari sebelum hingga menghasilkan output yang sudah di*masking*. Juga dengan cara melihat kemudahan untuk mengolah data yang dihasilkan oleh proses *masking* untuk kebutuhan proses berikutnya.
4. Dari pengujian Akurasi model mencapai sekitar 57%, menunjukkan bahwa sebanyak 57% dari semua prediksi yang dilakukan oleh model benar, baik yang positif maupun yang negatif. Meskipun akurasi tersebut tergolong cukup baik, masih ada 43% dari data yang tidak diklasifikasikan dengan benar. Oleh karena itu, perlu dilakukan evaluasi lebih lanjut terhadap klasifikasi yang kurang tepat.
5. Presisi model mencapai sekitar 87%, menunjukkan bahwa dari semua instance yang diprediksi sebagai positif oleh model, sekitar 87% di antaranya benar-benar positif. Hasil ini menandakan bahwa metode masking mampu dengan baik mengidentifikasi dan melindungi informasi sensitif yang seharusnya disembunyikan. Meskipun presisi tinggi, ada 13%

dari data yang diprediksi sebagai data masking yang sebenarnya bukan, yang mungkin merupakan False Positive.

6.2 Saran

Dari penelitian ini, didapatkan beberapa saran secara keseluruhan untuk implementasi *data masking* kedepannya:

1. Untuk keperluan masa mendatang, disarankan agar dirancang suatu spesifikasi yang memuat berbagai data masking yang dilakukan serta keamanan untuk spesifikasi tersebut, termasuk hak akses terhadap file yang berisi data masking dan aspek lainnya.
2. Ketersediaan informasi masing-masing data, dengan memberikan label berupa data sensitif dan bukan sensitif, hal ini untuk kemudahan data yang ingin di*masking*.
3. Algoritma juga rumus dari perlakuan suatu data harus tercatat dengan baik, terutama untuk data-data yang di*masking.*
4. Evaluasi menyeluruh terhadap data yang perlu dilindungi dan identifikasi resikonya. Identifikasi jenis data sensitif dan potensi dampak jika data tersebut diakses oleh pihak yang tidak berwenang.
5. Pilih teknik *masking* yang sesuai, pertimbangkan berbagai teknik *masking* yang tersedia, seperti substitusi nilai, enkripsi, atau pengaburan data. Pilih teknik yang paling cocok dengan jenis data yang ingin dilindungi dan pastikan tingkat keamanan yang diinginkan.
6. Desain dan implementasikan proses *masking* yang efektif, pastikan langkah-langkah *masking* terdokumentasi dengan baik dan dapat diulang.

Uji dan verifikasi proses *masking* secara menyeluruh untuk memastikan efektivitasnya.

7. Pertimbangkan regulasi dan kebijakan privasi yang berlaku dalam lingkungan di mana data tersebut dioperasikan. Pastikan implementasi *data masking* sesuai dengan persyaratan yang diberlakukan untuk memenuhi kepatuhan dan melindungi data secara tepat.
8. Lakukan evaluasi secara berkala terhadap kinerja metode *masking* yang diterapkan. Tinjau hasil *masking*, kesalahan klasifikasi, dan potensi kebocoran data. Identifikasi dan perbaiki kelemahan atau kegagalan *masking* yang terdeteksi selama pemantauan.
9. Berikan pelatihan kepada tim yang terlibat dalam proses *masking* untuk memastikan pemahaman yang baik tentang metode dan langkah-langkah yang diterapkan.
10. Libatkan pihak berkepentingan yang relevan, seperti tim keamanan informasi, pengelola data, dan pihak hukum, dalam proses implementasi *data masking*, agar mendapatkan masukan lebih banyak.
11. Implementasi *data masking* harus menjadi proses yang berkelanjutan. Selalu cari cara untuk meningkatkan kinerja *masking* dan mengikuti perkembangan teknologi dan persyaratan keamanan data.
12. Membangun algoritma penyamaran khusus yang dapat disesuaikan dengan kebutuhan dan karakteristik data organisasi masing-masing.
13. Beberapa masukan terkait kemungkinan pengembangan spesifikasi untuk data masking kedepannya:

- Sebaiknya dipertimbangkan penggunaan metode *masking* yang sesuai dengan kebutuhan spesifik organisasi. Sebagai contoh, apakah substitusi data, enkripsi, atau pengaburan lebih cocok untuk melindungi informasi sensitif.
- Menetapkan kriteria yang jelas untuk menentukan jenis data yang perlu di*masking*, kapan proses *masking* harus diimplementasikan, dan di lingkungan apa *masking* diperlukan. Hal ini dapat membantu memfokuskan upaya pada data yang benar-benar memerlukan perlindungan.
- Penting untuk mendefinisikan secara tepat siapa yang memiliki hak akses ke data asli dan data yang telah di*masking*. Peran pengguna dan kontrol akses perlu dirumuskan agar hanya pihak yang berwenang yang dapat mengakses data.
- Menetapkan sistem pemantauan dan audit yang efektif untuk memastikan bahwa kebijakan masking terus dipatuhi dan mendeteksi aktivitas yang mencurigakan. Ini bisa menjadi langkah krusial untuk memitigasi risiko kebocoran data.
- Merancang program pendidikan dan pelatihan, terkait untuk memahami dan menerapkan praktik data masking dengan benar. Ini akan mendukung penerapan yang konsisten dan penggunaan yang efektif.

Dari saran tersebut, diharapkan implementasi *data masking* dapat menjadi lebih efektif dalam melindungi informasi sensitif, menjaga privasi, dan meminimalkan risiko penyalahgunaan data.