BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melakukan penelitian dan mendapatkan hasil serta analisis data yang telah dilakukan, kami menemukan bahwa::

1. **Efektivitas GPT-4 dalam Menciptakan Email Phishing yang Realistis**: Alat AI Generatif berbasis GPT-4 terbukti efisien dalam menghasilkan simulasi serangan phishing yang tampak nyata. Dimana dari 50 responses, mayoritas 40 responden mencakup 80% dari total partisipan, menganggap email phishing yang dihasilkan oleh GPT-4 sangat realistis. Tingginya tingkat respons terhadap simulasi ini menandakan bahwa, meskipun kecanggihan teknologi ini, masih ada keperluan mendesak untuk memperkuat kesiagaan dalam menghadapi serangan siber yang semakin maju.
2. **Formula Prompting Optimal untuk GPT-4 dalam Pembuatan Email Phishing**: Pendekatan prompting yang ideal untuk GPT-4 berfokus pada analisis perilaku target untuk menghasilkan pesan phishing yang lebih autentik. Formula yang ditemukan dalam studi ini meliputi: Penerapan Teknik Dorking, Analisis Profil Pengguna, Analisis Penyalahgunaan, Penerapan Prompting pada GPT-4, Peluncuran Serangan (blast email), Pembentukan Persepsi, dan Penerimaan Respons.
3. **Efektivitas Email Phishing Hasil Prompting ChatGPT-4**: Penggunaan teks yang dihasilkan oleh AI GPT-4 terbukti efektif dan memberikan kontribusi positif dalam mengidentifikasi dan merespons ancaman siber, mendukung peningkatan kesadaran dan keamanan siber. Model ini, ketika dikombinasikan dengan kerangka kerja Analisis Penyalahgunaan atau pemodelan ancaman MISUSE, berpotensi tidak hanya memperkuat pertahanan siber tetapi juga mengurangi risiko penyalahgunaan teknologi AI di masa yang akan datang.

5.2 Saran

Dari hasil analisis, temuan, dan simpulan, studi ini menyarankan perlunya memperluas dan mengeksplorasi teknik-teknik lanjutan guna meningkatkan validitas dan reliabilitas hasil yang lebih kompleks, baik dalam hal kebaruan, ketangguhan,

dampak, inovasi dan implementasi. Adapun saran untuk penelitian selanjutnya sebagai berikut:

1) Peningkatan Program Edukasi dan Pelatihan: Mengingat efektivitas AI dalam menciptakan phishing yang realistis, disarankan untuk mengembangkan dan melaksanakan program edukasi yang lebih komprehensif. Program ini harus mencakup pelatihan tentang AI generatif dan phishing AI, serta menyediakan simulasi serangan phishing untuk meningkatkan kemampuan deteksi dan respons terhadap ancaman siber. Ini akan membantu individu dan organisasi lebih memahami dan mengantisipasi taktik serangan yang semakin canggih.

2) Pengembangan Alat Deteksi Phishing yang Lebih Lanjut: Mengingat kemampuan GPT-4 dalam menghasilkan email phishing yang meyakinkan, ada kebutuhan mendesak untuk pengembangan alat deteksi phishing yang lebih canggih. Penelitian selanjutnya harus fokus pada pengembangan teknologi yang dapat mengidentifikasi nuansa bahasa dan taktik persuasi yang digunakan dalam email phishing, sehingga meningkatkan efektivitas deteksi.

3) Penelitian tentang Penerapan AI dalam Konteks Pertahanan Negara: Dianjurkan untuk melakukan penelitian lebih lanjut tentang bagaimana teknologi AI, khususnya dalam konteks pertahanan negara, dapat dioptimalkan untuk kegunaan yang ramah pengguna. Penelitian ini harus mengeksplorasi bagaimana AI dapat diintegrasikan dalam operasi pertahanan negara, tidak hanya untuk meningkatkan efisiensi tetapi juga untuk memastikan bahwa teknologi tersebut dapat diakses dan digunakan dengan mudah oleh personel yang relevan.

4) Kolaborasi Lintas Sektor: Mengingat kompleksitas ancaman siber yang dihasilkan oleh AI, disarankan untuk mempromosikan kolaborasi antara akademisi, industri, dan pemerintah. Kolaborasi ini dapat memfasilitasi pertukaran pengetahuan dan sumber daya, serta pengembangan solusi inovatif yang dapat menangani ancaman siber yang berkembang.

5) Kajian Etika dan Regulasi AI: Penting juga untuk mengeksplorasi aspek etika dan regulasi penggunaan AI dalam serangan siber. Penelitian selanjutnya harus menilai dampak sosial dan etika dari penggunaan AI dalam serangan phishing dan mengembangkan kerangka kerja regulasi untuk mengendalikan penggunaan teknologi ini.