`

BAB V
PENUTUP

Pada bab ini akan membahas kesimpulan dari keseluruhan penelitian yang dilakukan, serta terdapat saran untuk pengembangan penelitian selanjutnya.

5.1. Kesimpulan

Berdasarkan keseluruhan pembahasan mengenai kontribusi PSO dalam mengoptimalkan parameter SVM untuk meningkatkan kemampuan WAF dalam mendeteksi pola serangan pada aplikasi web, serta penerapan PSO-SVM dalam pendekatan *hybrid signature* dan *anomaly based* pada WAF, berikut kesimpulan yang didapatkan:

1. Kontribusi PSO dalam mengoptimalkan parameter SVM terletak pada kemampuannya untuk menemukan kombinasi optimal dari parameter *C* dan *gamma* yang mempengaruhi kinerja WAF. Optimasi yang baik dari pemilihan *hyperparameter* yang tepat dari PSO meningkatkan deteksi pola serangan, khususnya serangan baru yang belum terdeteksi sebelumnya. Dari berbagai skenario pengujian, model paling optimal mendapatkan nilai rata-rata akurasi dari dua dataset sebesar 97,80%. Hal ini yang menunjukkan kemampuan WAF dalam mendeteksi pola serangan yang lebih akurat.
2. Penerapan PSO-SVM pada WAF dengan pendekatan *hybrid* melibatkan penggabungan dua metode: *signature-based*, yang mendeteksi serangan berdasarkan pola serangan yang sudah dikenal, dan *anomaly-based*, yang mendeteksi perilaku mencurigakan menggunakan metode *machine learning*. PSO-SVM digunakan untuk mengoptimalkan deteksi pada metode *anomaly-based*, yang umumnya lebih lambat dibandingkan dengan *signature-based*. Hasil evaluasi menunjukkan bahwa PSO-SVM dapat meningkatkan kecepatan deteksi hingga 11,99 ms pada metode *anomaly-based* dan 3,01 ms pada metode *signature-based*. Meskipun metode *signature-based* memiliki kecepatan deteksi yang lebih baik, *anomaly-based* dengan optimasi PSO-SVM lebih efektif dalam menangani pola

`

serangan baru dan tidak lazim. Hal ini membuat sistem lebih unggul dalam mendeteksi serangan baru dan kompleks dengan akurasi yang tinggi.

5.2. Saran

Berdasarkan keseluruhan pembahasan tentang penggunaan PSO dalam optimisasi SVM berikut saran yang dirumuskan:

1. Mengembangkan teknik *hybrid* yang mengintegrasikan pendekatan *signature-based* dan *anomaly-based* dengan metode *clustering* atau *ensemble learning* untuk meningkatkan sensitivitas terhadap serangan baru dan mengoptimalkan deteksi.
2. Melakukan pengujian dan validasi mendalam terhadap PSO-SVM dengan berbagai dataset dan skenario berbeda untuk memastikan keandalan dan generalisasi model dalam mendeteksi serangan di lingkungan aplikasi web yang beragam.