

## Daftar Gambar

Gambar 2. 1 Cara kerja IDS berbasis <i>signature</i> .....	II-2
Gambar 2. 2 Cara kerja IDS berbasis <i>anomaly</i> .....	II-3
Gambar 2. 3 Cara kerja Optuna (Akiba dkk., 2019).....	II-5
Gambar 3. 1 Tahapan Penelitian .....	III-2
Gambar 3. 2 Gambaran cara kerja model.....	III-4
Gambar 3. 3 Model <i>machine learning</i> berbasis <i>anomaly</i> .....	III-6
Gambar 3. 4 Bagan proses <i>Isolation Forest</i> .....	III-8
Gambar 4. 1 <i>Pseudocode</i> model hibrida .....	IV-3
Gambar 4. 2 Contoh output model hibrida.....	IV-5
Gambar 4. 3 Analisis serangan <i>SQL Injection</i> .....	IV-6
Gambar 4. 4 Output hasil perbandingan .....	IV-7
Gambar 4. 5 Pustaka <i>machine learning</i> .....	IV-8
Gambar 4. 6 Langkah <i>preprocessing</i> .....	IV-10
Gambar 4. 7 <i>Hyperparameter</i> awal untuk melatih model.....	IV-12
Gambar 4. 8 Contoh tree yang dibentuk <i>Isolation Forest</i> .....	IV-13
Gambar 4. 9 Evaluasi awal model.....	IV-15
Gambar 4. 10 Hasil evaluasi awal model <i>machine learning</i> .....	IV-15
Gambar 4. 11 <i>Pseudocode</i> optimasi model.....	IV-17
Gambar 4. 12 Pergeseran <i>threshold</i> model .....	IV-20
Gambar 4. 13 Evaluasi IDS berbasis <i>signature</i> pada <i>Known Attack</i> .....	IV-22
Gambar 4.14 Evaluasi IDS berbasis <i>signature</i> Pada <i>Unknown Attack</i> .....	IV-23
Gambar 4. 15 Evaluasi model <i>Isolation Forest</i> .....	IV-24

Gambar 4. 16 Perbandingan penggunaan *resource* model..... IV-29