

## DAFTAR ISI

PERNYATAAN .....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN .....	iii
RIWAYAT HIDUP .....	iv
HALAMAN PERSEMBAHAN .....	v
MOTTO .....	vi
ABSTRAK.....	vii
ABSTRACT.....	viii
KATA PENGANTAR .....	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR .....	xv
<b>BAB I PENDAHULUAN</b>	
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	3
1.6 Sistematika Penulisan .....	4
<b>BAB II LANDASAN TEORI</b>	
2.1 Aplikasi .....	5
2.2 Deteksi.....	5
2.3 Cyber .....	5
2.4 Cyber Attack .....	5
2.5 SQL Injection .....	6
2.6 Python.....	7
2.7 Linux .....	8

2.8	Support Vector Machine .....	9
2.9	Rapid Application Development (RAD).....	10
2.10	Flowchart.....	11
2.11	Penelitian Terkait .....	12

### BAB III METODELOGI PENELITIAN

3.1	Metode Penelitian.....	14
3.2	Metode Pengumpulan Data .....	15
3.2.1	Riset .....	15
3.2.2	Collecting .....	16
3.2.3	Studi Pustaka .....	16
3.3	Alat Pembuatan .....	16
3.3.1	Perangkat keras .....	16
3.3.2	Perangkat Lunak .....	16
3.4	Analisis.....	16
3.4.1	Analisis Kebutuhan Fungsional .....	17
3.4.2	Analisis Kebutuhan Non - Fungsional .....	17
3.5	Flowchart.....	18
3.6	Konsep.....	19

### BAB IV PENELITIAN DAN PEMBAHASAN

4.1	Hasil Pengumpulan Data .....	21
4.2	Tahap Implementasi Perangkat .....	21
4.2.1	Instalasi GIT .....	22
4.2.2	Instalasi Python & Framework.....	22
4.2.3	Instalasi Anaconda .....	23
4.2.4	Install Jupyter Notebook .....	23
4.2.5	Instalasi Visual Studio Code .....	25

4.3	Tahap Implementasi Project .....	25
4.3.1	Data Collecting .....	25
4.3.2	Model Selection .....	26
4.3.3	Training .....	27
4.3.4	Detection .....	27
<b>BAB V PENUTUP</b>		
5.1	Kesimpulan.....	31
5.2	Saran.....	31
5.3	Penutup .....	31
<b>DAFTAR PUSTAKA .....</b>		<b>32</b>
<b>LAMPIRAN .....</b>		<b>34</b>

## DAFTAR TABEL

Tabel 2.1 Simbol dan Fungsi Flowchart .....	11
Tabel 2.2 Penelitian Terkait .....	12
Tabel 3.1 Sumber Dataset .....	14
Tabel 3.2 Payloads Dataset .....	15
Tabel 3.3 Analisis Perangkat .....	18
Tabel 3.4 Konsep dan Tujuan Penggunaan Aplikasi .....	19
Tabel 4.1 Hasil Akurasi .....	30

## DAFTAR GAMBAR

Gambar 2.1 Types of Cyber Attack .....	6
Gambar 2.2 SQL Injection Attack .....	7
Gambar 2.3 Python Language .....	8
Gambar 2.4 Linux .....	8
Gambar 2.5 RBF SVM Parameters .....	9
Gambar 3.1 RAD Methodologies .....	15
Gambar 3.2 Flowchart .....	19
Gambar 4.2 Git Tools .....	22
Gambar 4.3 Git Running.....	23
Gambar 4.4 Anaconda Website .....	24
Gambar 4.5 Anaconda App .....	24
Gambar 4.6 Jupyter Running.....	24
Gambar 4.7 Visual Studio Code .....	25
Gambar 4.8 Print Dataset dan library .....	25
Gambar 4.9 Print Dataset .....	26
Gambar 4.10 Menampilkan statistic dataframe .....	26
Gambar 4.11 Memastikan Objek Data .....	26
Gambar 4.12 Model Selection .....	27
Gambar 4.13 Training Model .....	28
Gambar 4.14 Proses Deteksi dan implementasi pertama .....	28
Gambar 4.15 Proses Deteksi dan implementasi kedua .....	29
Gambar 4.16 Evaluasi Sistem.....	29
Gambar 4.17 Peningkatan Akurasi .....	30

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Keamanan merupakan salah satu aspek yang sangat penting dari sebuah sistem informasi. Keamanan komputer adalah sebuah tindakan pencegahan yang dilakukan untuk melindungi sebuah sistem dari serangan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Tanpa keamanan yang baik, maka data-data pengguna belum dapat dikatakan aman. Hal tersebut pastinya akan mempengaruhi kepercayaan pengguna dalam menggunakan sistem tersebut.

Di era teknologi informasi saat ini, sistem memiliki peran yang besar bagi perusahaan ataupun institusi, baik untuk mendapatkan keuntungan secara finansial maupun untuk memberikan pelayanan yang baik kepada pengguna sistem. Hal tersebut membuat perusahaan-perusahaan maupun instansi bersaing dalam menyediakan layanan terbaik. Namun, seringkali yang menjadi prioritas mereka adalah tampilan sistem dan layanan yang dapat memikat pengguna dengan cepat, sedangkan masalah keamanan berada di urutan bawah atau tidak dianggap begitu penting.

Padahal keamanan data sangat dibutuhkan untuk menjaga dan melindungi privasi pengguna. Ketika data privasi pengguna bocor atau jatuh ke tangan pihak-pihak yang tidak bertanggung jawab, maka rasa kepercayaan pengguna terhadap penyedia layanan pun akan runtuh. Banyak peristiwa yang telah terjadi terkait peretasan atau pembobolan sistem karena minimnya perhatian penyedia layanan terhadap keamanan sistem tersebut, seperti kasus peretasan yang terjadi pada situs Komisi Pemilihan Umum (KPU) Kota Yogyakarta yang terjadi pada bulan Februari 2017 dan kasus peretasan situs Telkomsel yang terjadi beberapa bulan lalu.

Salah satu sistem yang umumnya menjadi sasaran hacker dan cracker adalah aplikasi berbasis website. Hal tersebut dikarenakan pemanfaatan aplikasi mengalami pertumbuhan yang sangat pesat saat ini. Hacker adalah