BAB I. PENDAHULAN

1.1. Latar Belakang

Laju perkembangan ilmu pengetahuan dan teknologi terjadi semakin cepat dan masif. Perkembangan tersebut membentuk interkoneksi yang saling mereaksi dan mendukung satu sama lain. Sebagai dampak dari reaksi tersebut, implementasi dan pengembangan teknologi dapat dilakukan lebih cepat. Ketersediaan *software* dan *hardware* saat ini telah menghasilkan berbagai teknologi baru, suatu teknologi yang dulunya sulit untuk dihasilkan, karena memerlukan *software* dan *hardware* dengan spesifikasi tinggi, dapat lebih mudah ditemukan pada era ini. Adapun beberapa tren teknologi pada tahun 2022 adalah *Intelegent Process Automation (IPA), Internet of Things, Blockchain, Big Data Analytics (BDA), Human Augmentation, Metaverse, Artificial Intelegence, 5G,* dan *Cyber Security* [1-2].

Salah satu isu menarik terkait perkembangan teknologi adalah *cyber security* atau keamanan siber. Keterbukaan akses informasi, *big data,* IoT, 5G, AI, dan ke-hadiran berbagai macam teknologi saat ini seharusnya diimbangi oleh peningkatan sistem dan pengelolaan keamanan, sehingga data atau informasi dapat terlindungi. Sesuai dengan kutipan "*IoT without security equals to The Internet of threats*" [3]. Dengan kata lain, efektivitas keamanan siber seharusnya semakin meningkat dan jumlah serangan semakin menurun. Berbagai metode dan teknik serangan juga semakin sulit atau bahkan tidak dapat dilakukan, baik pada skala kecil, menengah, maupun *enterprise*. Kasus *data breached* atau akses data secara ilegal, apalagi dengan jumlah data yang sangat besar, seharusnya tidak lagi terjadi.

Pada kenyataannya, kasus serangan siber justu semakin meningkat, baik pada skala dunia maupun Indonesia. Secara global, berdasarkan data dari PacketLabs, terjadi peningkatan serangan siber sangat signifikan pada tahun 2021, dan serangan tersebut terjadi pada banyak negara di dunia [4]. Google bahkan mencatat 18 juta upaya serangan berupa *malware* per harinya [5]. Tidak hanya itu, upaya peretasan *website* juga mencapai 30.000 kali setiap harinya, dan sebanyak 64% perusahaan di dunia mengalami sedikitnya satu kali upaya serangan. Pada Maret 2021, tercatat 20 juta data diakses secara ilegal dan serangan siber terus terjadi setiap 39 detik [6]. Berdasarkan laporan dari Purplesec, sekitar 18 juta *website* terinfeksi *malware* setiap minggunya [7]. Secara ekonomi atau *cost*, berdasarkan laporan IBM *Security*, kerugian akibat serangan siber mencapai rata-rata $4.25 juta selama 30 hari dan diperlukan sekitar 197 hari untuk mendeteksi serangan tersebut [8]. Berdasarkan fakta-fakta tersebut, serangan siber merupakan ancaman nyata bagi setiap negara dan risikonya tergantung dengan bagaimana tingkat keamanan di negara tersebut.

Beralih pada skala lokal atau Indonesia, berdasarkan laporan tahunan Badan Siber dan Sandi Negara (BSSN) Republik Indonesia, tercatat sebanyak 316.167.753 serangan siber terjadi sepanjang tahun 2020 di Indonesia. Ditinjau dari sumbernya, serangan siber tersebut berasal dari dalam dan luar Indonesia. Jumlah serangan siber yang berasal dari dalam mencapai 1.136.689. Sementara itu, jumlah serangan yang berasal dari luar Indonesia mencapai 7.511.692. Jumlah serangan terbanyak berasal dari negara India, yaitu 2.935.769 serangan, kemudian diikuti oleh Ireland, Vietnam, dan Rusia. Peringkat lima negara sumber serangan ke Indonesia terbesar, baik dari dalam dan luar, dapat dilihat pada tabel 1.1 berikut ini.

Tabel 1.1 Lima Negara Sumber Serangan ke Indonesia Tahun 2020

Peringkat	Nama Negara	Jumlah Serangan
1	India	2.935.769
2	Ireland	2.125.343
3	Vietnam	1.545.650
4	Indonesia	1.136.689
5	Rusia	904.930

Berdasarkan aspek potensi serangan dari dalam (*internal attack)*, Indonesia terbilang memiliki potensi atau risiko serangan internal yang cukup tinggi. Selain jumlah yang tinggi, serangan siber di Indonesia juga menargetkan berbagai sektor dan teknik serangannya juga tidak mudah diidentifikasi. Terdapat lebih dari 5 juta teknik serangan dengan label *unknown* [9]. Sebagai dampak dari fakta tersebut, pada skala global, Indonesia menempati peringkat kedua sebagai negara sumber serangan tertinggi, dengan lebih dari 38 juta serangan (tabel 1.2). Hal tersebut tentunya semakin meningkatkan potensi serangan dari dalam. Oleh karena itu, upaya taktis yang preventif, defensif, dan sistematis perlu dilakukan, apalagi jika berkaitan dengan stabilitas keamanan negara. Dalam hal ini, upaya tersebut dapat dimulai dengan pengembangan metode deteksi dan mitigasi serangan yang baik.

Tabel 1.2 Negara Sumber Serangan Tertinggi Tahun 2020

Peringkat	Nama Negara	Jumlah Serangan
1	India	50.320.126
2	**Indonesia**	**38.787.054**
3	Irlandia	35.759.925
4	Vietnam	25.754.306
5	Rusia	18.694.813

Peringkat	Nama Negara	Jumlah Serangan
6	Pakistan	18.418.184
7	Cina	12.524.213
8	Bandladesh	11.725.434
9	Amerika Serikat	8.429.676
10	Venezuela	7.726.159

Teknologi yang digunakan untuk melakukan serangan siber saat ini semakin canggih dan beragam. Jumlah kasus atau statistik serangan yang meningkat setiap

tahunnya merupakan salah satu indikasi bahwa eksekusi serangan dapat lebih mudah dilakukan. Dengan teknologi otomatisasi (*bot*) misalnya, proses serangan dapat dilakukan secara cepat, tanpa memerlukan banyak intevensi dan tindakan. Secara umum, penggunaan teknologi maju dalam serangan siber dapat menyebabkan dua masalah, yaitu (1) teknik atau metode serangan yang digunakan semakin sulit untuk diidentifikasi dan (2) pengembangan sistem keamanan dan mitigasi serangan memerlukan upaya yang lebih rumit dan kompleks.

BSSN menyebutkan bahwa terdapat 5.934.058 teknik yang belum teridentifikasi pada serangan tahun 2020 [9]. Keragaman teknologi, teknik, dan strategi serangan yang digunakan mempengaruhi tingkat identifikasi. Selain itu, deteksi gejala serangan juga tidak mudah dilakukan, karena tergantung pada teknologi (*software* dan *hardware*) yang tersedia atau digunakan oleh komputer server. Tanpa teknologi deteksi serangan yang baik, proses mitigasi juga secara otomatis menjadi sulit untuk dilakukan. Oleh karena itu, keduanya harus berjalan secara sinergi, sehingga dapat membentuk sistem keamanan siber yang kokoh, stabil, dan handal.

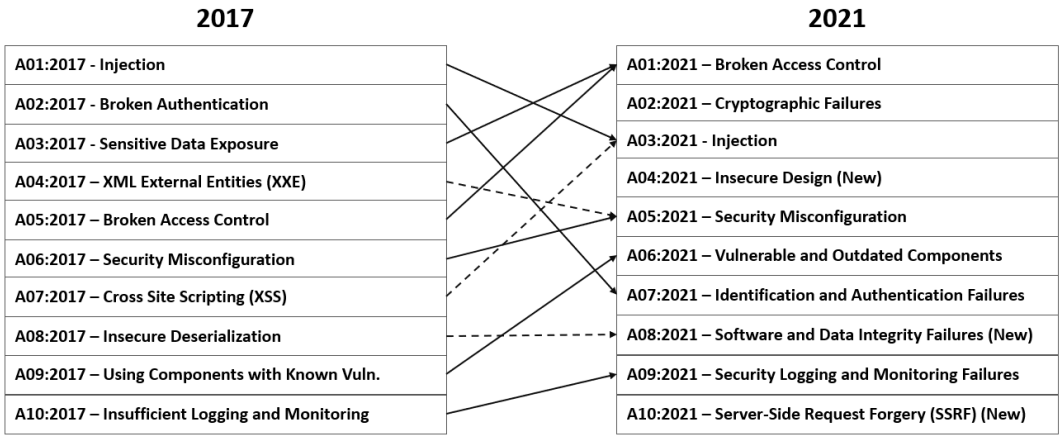
Keamanan siber merupakan komponen penting dalam suatu ekosistem teknologi. Peningkatan jumlah dan kemajuan teknologi serangan harus juga diimbangi dengan peningkatan sistem dan tata kelola keamanan, sehingga terbentuk ekosistem teknologi yang aman digunakan. Namun, pada kenyataannya, kasus serangan siber yang cukup fenomenal, terutama terkait jumlah data yang besar, masih ditemukan di Indonesia. Ironisnya, serangan tersebut menyerang perusahaan dan institusi ternama, seperti Tokopedia, BukaLapak, KPU, BPJS dan seterusnya. Bahkan, kebocoran data BPJS kesehatan disebut merugikan negara Rp 600 triliun [10].

Merujuk pada meningkatnya statistik serangan siber dan kebocoran data yang terjadi, tingkat efektivitas mitigasi juga dipertanyakan. Upaya mitigasi sebaiknya dilakukan secara berlapis (*multi-layer*), sehingga peretasan lebih sulit dilakukan. Keamanan berlapis juga tidak hanya menjamin keamanan *website* tunggal, tetapi beberapa *website* yang berada pada area arsitektur yang sama. Dengan deteksi yang akurat dan keamanan yang berlapis, serangan siber diharapkan dapat tertangani atau dapat diminimalisasi. Namun, pengembangan sistem deteksi dan mitigasi yang baik bukan sesuatu yang mudah untuk dilakukan. Keduanya memerlukan solusi dan strategi, sehingga menarik untuk dikaji dan diteliti.

Berdasarkan pada fakta dan masalah yang telah dijelaskan sebelumnya, penelitian ini menggunakan metode deteksi dan mitigasi untuk mengatasi serangan siber pada *multi-websites.* Dengan kata lain, penelitian ini mengukur seberapa baik tingkat akurasi deteksi dan seberapa efektif tingkat mitigasi terhadap serangan siber yang dilakukan pada *multi-websites*. Metode deteksi penelitian ini menggunakan *machine learning* dan metode mitigasi menggunakan *multi-layer security.* Untuk mendapatkan metode deteksi dengan tingkat akurasi yang tinggi, penelitian ini mengujikan lima algoritma. *Support Vector Machine* menjadi algoritma yang mampu menghasilkan tingkat akurasi tertinggi.

Secara parsial, terdapat sejumlah penelitian yang pernah membahas perihal beberapa sub-kajian dalam penelitian ini, seperti metode deteksi berbasis *machine learning* dan metode mitigasi berbasis *single-layer security*. Namun, penelitian tersebut masih memiliki beberapa kelemahan di antaranya: (1) masih ada metode serangan yang belum bisa diatasi [11-12]; (2) penggunaan data uji coba yang terbatas

[12-13]; dan (3) implementasi uji efektivitas metode mitigasi yang kurang komprehensif sehingga kurang representatif [14-15]. Oleh karena itu, berdasarkan pada kelemahan tersebut, salah satu tujuan penelitian ini adalah mengimplementasikan metode deteksi dan mitigasi yang lebih akurat dan efektif dari yang sebelumnya. Karena jenis metode serangan siber yang beragam dan kompleks, metode serangan yang diujikan merujuk pada *OWASP Top-10 Common Web Application Vulnerabilities* yang dipublikasikan oleh *Open Web Application Security Project* (OWASP). Penelitian ini menggunakan publikasi celah keamanan OWASP tahun 2021 yang diambil berdasarkan survey sehingga lebih relevan dengan situasi terbaru. Adapun daftar 10 celah keamanan yang kebanyakan terjadi pada aplikasi berbasis *website* menurut OWASP dapat dilihat pada gambar 1.1 berikut ini.



Gambar 1.1 Daftar Peringkat 10 Celah Kemanan *Website* Menurut OWASP

OWASP *Top-10 vulnerabilities* adalah daftar celah keamanan yang paling sering ditemukan pada kebanyakan aplikasi berbasis *website*. Dengan kata lain, celah keamanan tersebut menjadi komponen yang paling sering dijadikan sebagai target serangan. Terkait dengan hal tersebut, metode serangan yang digunakan untuk mengeksploitasi *common vulnerabilities* tersebut dapat beragam. Sebagai

gambaran, pada celah keamanan *injection*, metode serangan yang dapat digunakan adalah *SQL Injection* atau XSS. Contoh lainnya, metode serangan IDOR (*Insecure Direct Object Reference*) dapat digunakan untuk mengeksploitasi celah keamanan *broken authentication* dan *identification and authentication failures*, dan seterusnya. Oleh karena itu, istilah celah keamanan *(web vulnerabilities*) berbeda dengan metode serangan. Metode berkaitan dengan cara atau skenario penyerangan sedangkan celah keamanan berkaitan dengan target serangan.

Ditinjau dari jenis serangannya, penelitian ini berfokus pada serangan siber. Serangan ini merupakan sub-jenis ancaman siber *(cyber threat*). Dalam hal ini, ancaman siber dibagi menjadi tiga, yaitu serangan siber (*cyber attack*), kejahatan siber *(cyber crime*), dan terorisme siber (*cyber terrorism*). Berbeda dengan motif yang mendasari kejahatan dan terorisme siber, serangan siber lebih ditujukan untuk melakukan upaya-upaya destruktif seperti perusakan dan penyalahguaan data dan perusakan perangkat keras. Sementara itu, kejahatan siber lebih ditujukan untuk tujuan komersial atau pencarian keuntungan dengan memanfaatkan dunia siber, dan terorisme siber lebih ditujukan untuk menciptakan suatu kepanikan. Semakin besar dampak kepanikan, semakin berhasil serangan tersebut.

1.2. Identifikasi Masalah

Berdasarkan latar belakang masalah yang telah diungkapkan pada sub bab sebelumnya, daftar masalah dalam penelitian ini adalah sebagai berikut.

1. Metode atau teknik serangan siber saat ini semakin beragam dan menggunakan teknologi maju, sehingga semakin sulit dideteksi dan diidentifikasi.
2. Kebanyakan metode deteksi belum bekerja secara optimal, sehingga tidak

dapat mendeteksi gejala-gejala serangan secara akurat;

3. Metode mitigasi serangan masih menerapkan prinsip *single-layer security* sehingga dinding pertahanan keamanan dapat dilumpuhkan penyerang.
4. Metode mitigasi serangan belum dilakukan secara efektif dan menyeluruh, sehingga penyerang dapat melakukan eksploitasi celah keamanan pada *website* yang memiliki tingkat keamanan rendah.
5. Metode deteksi dan mitigasi serangan tidak diintegrasikan, keduanya berdiri secara terpisah, sehingga tidak dapat saling mendukung.
6. Metode mitigasi yang ditawarkan pada penelitian sebelumnya belum terbukti belum mampu mengatasi serangan secara optimal.
7. Serangan siber tidak hanya berdampak pada infrastrukur teknologi, tetapi juga pada segi bisnis dan pembiayaan atau *cost factor*.

1.3. Rumusan Masalah

Merujuk pada pemaparan yang telah disampaikan melalui latar belakang dan identifikasi masalah, rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Seberapa akurat impelementasi metode deteksi berbasis *machine learning* dalam mendeteksi serangan siber pada *multi-websites*?
2. Seberapa efektif implementasi metode mitigasi berbasis *multi-layer security* dalam mengatasi serangan siber pada *multi-websites?*
3. Bagaimana implementasi metode deteksi menggunakan *machine learning* dan mitigasi menggunakan *multi-layer security* untuk mengatasi *cyber attack* pada *multi-websites*?

1.4. Batasan Masalah

Untuk lebih memfokuskan masalah yang diuji dan diteliti, batasan masalah dalam penelitian ini dijelaskan pada tabel 1.3 berikut ini.

Tabel 1.3 Komponen dan Kriteria Batasan Masalah Penelitian

No	Komponen Pembatasan	Kriteria/Spesifikasi Pembatasan
1	Metode deteksi	Metode deteksi serangan menggunakan algoritma *machine learning* yang diseleksi berdasarkan tingkat akurasi yang berhasil dicapai. Oleh karena itu, penelitian ini mengujikan lima algoritma *machine learning*.
2	Metode mitigasi	Metode mitigasi serangan menggunakan *multi-layer security*, yang terdiri dari lima lapisan keamanan, bertugas untuk mengatasi serangan pada *website* yang berjalan di dalam area kerja *web-server* yang sama.
3	Serangan siber	Teknik serangan siber yang diteliti mengacu pada tiga celah keamanan OWASP *Top-10 Common Web Vulnerabilities* pada tahun 2021 yaitu *Cross Site Scripting, SQL Injection*, dan *Remote Code Execution.*
4	*Multi-websites*	*Multi-website* adalah beberapa atau > 1 *website* yang berada pada satu lingkungan kerja *web-server* yang sama, dan *webserver* yang akan digunakan pada penelitian ini adalah Apache2.
5	Pengujian akurasi dan efektifitas metode	Untuk menguji seberapa besar tingkat akurasi metode deteksi dan tingkat efektivitas metode mitigasi, penelitian ini menggunakan OWASP ZAP (*Zed Attack Proxy*) dan Arachni untuk melakukan simulasi serangan terotomatisasi.

1.5. Tujuan Penelitian

Secara umum, tujuan pelaksanaan penelitian ini adalah untuk mengetahui bagaimana tingkat akurasi metode deteksi berbasis *machine learning* dan tingkat efektivitas metode mitigasi guna mengatasi *cyber-attack* pada *multi-websites*. Selain itu, penelitian ini juga memiliki beberapa tujuan khusus yaitu sebagai berikut.

1. Secara luaran atau *output* penelitian**:** menghasilkan metode deteksi dan mitigasi serangan yang akurat dan efektif dalam mengatasi serangan dan melakukan pengamanan *multi-website* pada suatu *webserver*.
2. Secara teoritis: membuktikan bahwa metode deteksi dan mitigasi yang diusulkan peneliti dapat bekerja lebih baik dari metode deteksi dan mitigasi yang telah diimplementasikan pada penelitian sebelumnya.
3. Secara praktis: menghasilkan metode deteksi dan mitigasi serangan yang bersifat menyeluruh, karena dapat memberikan perlindungan tidak hanya pada satu *website*, tetapi juga pada banyak *website*.
4. Secara praktis: memberikan kontribusi berupa metode deteksi dan mitigasi serangan sebagai upaya peningkatan keamanan siber.
5. Secara praktis: memberikan gambaran atau deskripsi terkait bagaimana mengimplementasikan suatu metode deteksi dan mitigasi secara baik.

1.6. Manfaat Penelitian

Penelitian ini diharapkan akan bermanfaat bagi banyak pihak. Secara rinci, target penerima manfaat penelitian ini adalah sebagai berikut:

1. **Bagi *web developer* dan *system administrator***: memberikan gambaran dan pertimbangan terkait bagaimana mengimplementasi metode deteksi

dan mitigasi untuk mengatasi serangan siber pada *multi-websites*.

2. **Bagi *penetration tester*:** memberikan informasi dan data terkait tingkat akurasi deteksi dan efektivitas mitigasi dalam mengatasi serangan siber.
3. **Bagi pemilik *website***: memberikan pertimbangan dalam merancang dan menyampaikan kebutuhan, memilih ekosistem teknologi, dan menyiapkan sumber daya untuk membangun *website* yang aman;
4. **Bagi peneliti selanjutnya**: memberikan referensi atau bahan komparasi terkait metode deteksi berbasis *machine learning* dan mitigasi berbasis *multi-layer security* untuk mengatasi *cyber-attack*.
5. **Bagi peneliti**: meningkatkan kemampuan peneliti pada bidang keamanan siber, terutama pada implementasi metode deteksi dan mitigasi serangan.

1.7. Sistematika Penulisan

Sistematika penulisan proposal penelitian ini didasarkan pada buku panduan penulisan atau gaya selingkung tesis IBI Darmajaya dengan susunan berikut ini.

1. **Pendahuluan (Bab I)**

   Bab ini membahas tentang latar belakang atau urgensi masalah yang diteliti, identifikasi, rumusan, dan batasan masalah, lalu diikuti dengan penjelasan terkait tujuan, manfaat, dan sistematika penulisan penelitian.

2. **Tinjauan Pustaka (Bab II)**

   Bab ini membahas tentang teori dan fakta yang menjelaskan dan mendukung pelaksanaan penelitian ini seperti terkait metode deteksi dan mitigasi, jenis dan teknik serangan siber, OWASP Top-10 *common web vulne-*

rabilities, *machine learning*, *multi-layer security*, dan sebagainya.

3. **Metodologi Penelitian (Bab III)**

   Bab ini membahas metodologi penelitian yang digunakan. Mulai dari objek penelitian, alat dan bahan, sumber data, metode eksperimen, prosedur pelaksanaan penelitian, dan teknik analisis yang digunakan.

4. **Hasil dan Pembahasan (Bab IV)**

   Bab ini menyajikan hasil dan pembahasan penelitian. Pada pembahasan penelitian, peneliti menyampaikan secara rinci hal-hal yang dilakukan dalam penelitian. menyampaikan berbagai temuan penelitian, serta menyampaikan relevansi dan komparasi dengan penelitian sebelumnya.

5. **Kesimpulan dan Saran (Bab V)**

   Bab ini berisi tentang kesimpulan dan saran. Kesimpulan adalah jawaban singkat terkait rumusan masalah dan saran terkait dengan rekomendasi yang ingin disampaikan peneliti kepada pihak terkait.