BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi selalu meningkat dikarena teknologi banyak memberikan keuntungan terutama dalam hal mempermudah pekerjaan manusia (Mansoori *et al*., 2012).Penggunaan teknologi yang sesuai tujuan dan tepat dapat membantu masyarakat banyak seperti dengan adanya jaringan telekomunikasi sehingga setiap orang dapat terhubung satu sama lain dengan jarak yang tanpa batas. Selain itu terciptanya internet yang dapat membantu setiap orang dalam ilmu pengetahuan yang luas dan dapat juga saling terhubung dengan menggunakan identitas unik atau disebut dengan IP *Address*. Dengan perkembangan yang semakin pesat ini setiap pengguna dapat terbantu dalam mendapatkan dan mengelola setiap informasi yang bisa diakses secara luas karena seluruh komponen perangkat keras dan perangkat lunak terhubung menjadi satu ke dalam jaringan internet yang dapat menghubungkan seluruh sumber informasi. Pada jaringan internet setiap Informasi yang berada pada sebuah website tidak dapat menjamin bahwa data tersebut dapat aman untuk diakses dikarenakan adanya risiko jika terdapat beberapa celah pada keamanan di sisi server tersebut sehingga dapat disalah gunakan oleh pihak yang tidak berwewenang atau bertanggung jawab. Informasi berdasarkan sifatnya dibagi menjadi 2 yaitu ada yang bersifat terbuka dan pribadi atau *private*. Dalam menjaga infomasi tersebut, sistem keamanan harus mempunyai tingkat keamanan yang tinggi dan tidak adanya . Jika sistem keamanan masih rendah, dapat membuat celah bagi para *attacker* melancarkan tindakan *cybercrime* maka diperlukan sistem keamanan yang aman baik dari sisi aplikasi maupun komputer server (Hartawan & Desnanjaya, 2018).

Server merupakan sebuah perangkat yang paling penting dalam suatu sistem jaringan yang berfungsi sebagai penyedia layanan atau *service* dalam jaringan yang telah ada di suatu organisasi, perusahaan dan instansi lainnya. Dalam melakukan tugasnya sebagai penyedia layanan, server harus bisa berjalan secara terus menerus karena bersifat memonitoring. Untuk memonitoring terhadap jaringan yang ada komputer server sangat diperlukan karena dapat melakukan pencatatan dalam bentuk *log service* secara *real-time* untuk mencatat aktivitas layanan yang sedang berlangsung pada server. Fungsi dari pencatatan *log* ini adalah agar setiap aktivitas memiliki catatan atau riwayat akses yang berupa *log* ke sebuah sistem pelayanan yang dijalankan oleh sebuah server seperti adanya akses untuk memasuki server kemudian adanya pengguna yang menggunakan bandwidth yang tinggi. Komputer server sangat rentan akan serangan para *attacker* untuk itulah adanya pengamanan pada perangkat server seperti *Mikrotik* yang mengatur lalu lintas data atau bandwidth pada setiap pengguna. Untuk mengetahui serangan – serangan yang dilancarkan pada server jaringan ini dapat menggunakan metode K-means *Clustering* karena dengan metode ini dapat mengelompokkan jenis serangan pada server *mikrotik* yang bersumber dari *log mikrotik* (Zulfadhilah *et al*., 2016).

Dengan adanya Pengelompokan data yang bersumber dari *log* server *mikrotik* dapat memudahkan administrator server dalam memperoleh beberapa informasi yang terperinci. Dalam melakukan pengelompokkan data ini terdapat beberapa metode algoritma yang dapat diantaranya seperti *Fuzzy* K-Means, DBSCAN, *Hierarchical Clustering*, dan K-Means *Clustering*. Dari metode pengelompokkan ini terdapat beberapa penelitian yang sudah dilakukan sebelumnya yaitu dalam menerapkan metode K-Means *Clustering* seperti halnya penggunaan metode K-Means *clustering* dalam *log* file untuk medeteksi ketidaksinambungan trafik jaringan pada server. Penelitian yang telah disebutkan menggunakan metode K-Means *Clustering* untuk melakuakn pengelompokkan data sehingga dapat memberikan informasi berdasarkan hasil dari pendeteksian *log* dengan menentukan pola dari setiap data yang dihasilkan. Hasil dari penelitian ini menghaslkan berupa analisa data dari *log* server yang dikelompokkan berdasarkan *cluster* sehingga dapat terbentuk pola trafik data serangan. Selain itu, ada juga

penelitian berikutnya mengenai pemanfaatan dari metode K-Means *Clustering* agar dapat mengetahui setiap perilaku dalam penggunaan internet berdasarkan data *mining log* jaringan server di sebuah Lembaga Pendidikan salah universitas di Yogyakarta. Dari hasil penelitian ini menunjukkan bahwa setiap data pengguna menghasilkan waktu akses yang sering digunakan yaitu pagi sampai sore dan sore sampai malam memiliki *traffic* yang terbanyak dari *traffic* lainnya (Haris *et al*., 2020).

Tujuan dalam melakukan penelitian yaitu untuk membantu administrator jaringan dalam melakukan pemeriksaan jenis serangan *cyber* pada server jaringan menggunakan *log* pada *mikrotik*. Dalam melakukan penelitian ini penulis telah mengambil judul yaitu "**Analisis Data *Mining Log* Server *Mikrotik* Untuk Analisa Pola Serangan Dengan Teks *Clustering* Di Bekangdam II Sriwijaya**."

1.2 Perumusan Masalah

Berdasarkan dari latar belakang yang telah dipaparkan dalam penjelasan diatas, Maka didapatkan beberapa rumusan masalah, yaitu Bagaimana memberikan informasi data *mining log* server *mikrotik* untuk menganalisa pola serangan dengan *clustering* di Bekangdam II Sriwijaya.

1.3 Batasan Masalah

Terdapat beberapa batasan masalah dalam melakukan penelitian sehingga pembahasan terkait penelitian yang telah dilakukan dapat lebih terarah agar mempermudah dalam memahami terhadap penelitian yang dilakukan. Adapun batasan masalah dalam penelitian ini yaitu :

Penelitian ini yaitu mengelompokkan data yang berisi pola serangan terhadap server yang menggunakan *mikrotik* yang tercatat dalam sebuah file sistem yang berisi *Log*.

1. Pengelompokkan pola serangan yang telah diambil dari file sistem dalam sebuah server *mikrotik* akan dikelompokkan dengan menggunakan metode K-

Means *Clustering* untuk mengetahui setiap aktivitas *client* yang terhubung ke komputer server berdasarkan data *log* jaringan di di Bekangdam II Sriwijaya.

2. Data yang berisi *Log* dalam server *mikrotik* yang digunakan dalam penelitian ini yaitu data yang dilakukan selama melakukan observasi di lingkungan server di Bekangdam II Sriwijaya.

1.4 Tujuan Penelitian

Adapun beberapa tujuan peneliti dalam melakukan penelitian ini adalah sebagai berikut :

1. Melakukan Analisa Data *Mining Log* menggunakan metode *Clustering*.
2. Menganalisa pola serangan pada *log* server di Bekangdam II Sriwijaya.

1.5 Manfaat Penelitian

Penelitian yang telah dilakukan diharapkan dapat berguna dan membantu dalam hal proposal maupun skripsi yang telah dibuat oleh mahasiswa yang nantinya sehingga tidak ada lagi kesalahan dalam melakukan penulisan proposal maupun skripsi, maka manfaat dari pelaksanaan penelitian ini yaitu :

1. Bagi Akademik

   Membantu peneliti dalam memperdalam materi yang telah diberikan selama masa penerimaan pembelajaran di bangku kuliah dengan menerapkan teori yang ada ke dalam praktek langsung di lapangan. Sehingga dapat mengembangkan ilmu pengetahuan yang telah diberikan.

2. Bagi Peneliti
   a. Menerapkan beberapa teori dan metode yang telah dipelajari dari beberapa buku – buku sewaktu masa sekolah.
   b. Dapat menganalisa kelemahan pada server jaringan yang telah ada.
   c. Dapat memahami tentang metode teks *clustering*
   d. Dapat mengerti proses dalam menganalisa masalah dengan metode teks *clustering*.

e. Mengetahui dan mengidentifikasi masalah pada server dengan menggunakan *log* pada *mikrotik*.
f. Mengetahui tentang data *mining* pada sebuah server.

3. Bagi Bekangdam II Sriwijaya

Dapat memberikan sebuah informasi yang berisi pola serangan yang ada pada server *mikrotik* dengan menggunakan metode k-means teks *clustering* untuk mempermudah dalam pengelompokkannya.

1.6 Metodologi Penelitian

1.6.1. Waktu Penelitian

Waktu penelitian ini direncanakan selama 8 bulan Yaitu dimulai dari Februari 2021 sampai Oktober 2021.

1.6.2. Tempat Penelitian

Tempat dalam melakukan penelitian ini yaitu di Bekangdam II Sriwijaya yang bertempat di Jl. Sultan Mahmud Badaruddin II No.47, 19 Ilir, Kec. Bukit Kecil, Kota Palembang, Provinsi Sumatera Selatan dan Kode Pos 30113.

1.6.3. Alat dan Bahan

Penelitian yang dilaksanakan di Bekangdam II Sriwijaya ini menggunakan alat dan bahan yang meliputi Perangkat Keras dan Perangkat Lunak serta bahan-bahan penunjang lainnya agar dapat berjalan dengan baik.

1.6.4. Perangkat Keras

Perangkat keras yang digunaka dalam penelitian yaitu berupa laptop dengan spesifikasi sebagai berikut.

1. Laptop HP
2. *Processor Intel* (R) Core (TM) i5-7200U
3. CPU @2.50GHz
4. *Installed Memory* (RAM) 4.00 GB

5. *Hard disk* 931.51 GB
6. *System Type* 64-bit *Operating System*

1.6.5. Perangkat Lunak

Perangkat Lunak yang digunakan dalam proses melakukan penelitian yitu sebagai berikut :

a. Microsoft Windows 10
b. Microsoft Office 2010
c. Winbox
d. Mendeley
e. Microsoft Visio 2016
f. Aplikasi Orange

1.6.6. Metode Penelitian

Peneliti yang memutuskan untuk melakukan penelitian ini yaitu menggunakan metode penelitian deskriptif. Menurut para ahli yaitu Hidayat (2010) menyatakan bahwa metode deskriptif adalah sebuah penelitian yang lebih luas dalam penggunaan data – data yang telah didapatkan. Arti dalam kata luas maksudnya yaitu lebih condong pada setiap analisa yang panjang dari ujung awal sampai akhir sehingga hasil yang didapat dapat terperinci dan detail.

Dalam melakukan penelitian dengan menggunakan penelitian metode deskriptif. Setiap peneliti harus dituntut untuk memiliki komitmen yang kuat atas penelitian yang dilakukan. Baik dari segi teori maupun dari segi praktek karena pada saat terjun langsung di lapangan harus mengambil setiap informasi yang sangat dibutuhkan. Sebab metode penelitian ini harus membutuhkan sebuah analisa yang Panjang dan kuat.

Menurut (Sukmadinata:2006) Penelitian deskriptif adalah suatu metode penelitian yang ditujukan untuk menggambarkan fenomena-fenomena yang ada, yang berlangsung saat ini atau saat yang lampau. Penelitian ini tidak mengadakan manipulasi atau pengubahan pada variabel-variabel bebas, tetapi menggambarkan suatu kondisi apa adanya. Penggambaran kondisi bisa individual atau menggunakan angka - angka.

1.6.7. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam melakukan penelitian yaitu menggunakan beberapa macam teknik dalam pengumpulan data :

1. Metode Pustaka

pengumpulan data menggunakan metode ini yaitu mengumpulkan berbagai sumber tertulis yang berkaitan dengan pelaksanaan penelitian dengan cara membaca, mempelajari, dan mencatat hal-hal penting yang berhubungan dengan masalah yang sedang dibahas guna memperoleh gambaran secara terperinci yang dapat menunjang pada penyusunan skripsi.

2. Metode Observasi

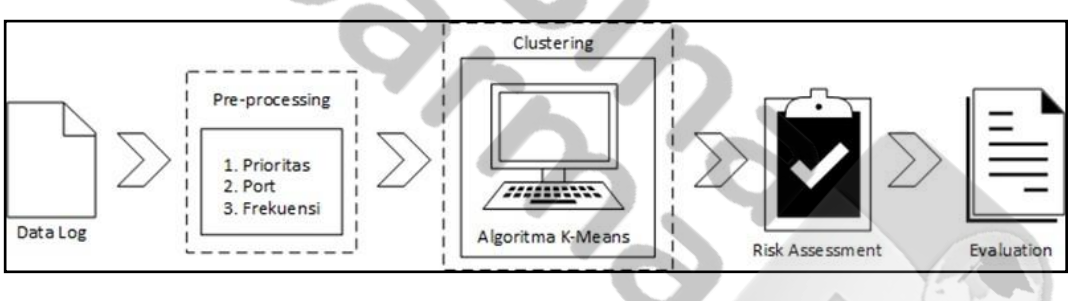
Yaitu metode pengumpulan data dengan cara mengadakan tinjauan atau pengamatan secara langsung ke objek yang diteliti. Pengumpulan data dilakukan secara langsung terhadap objek penelitian, dengan mencatat hal - hal yang berkaitan dengan penelitian yang berhubungan dengan judul skripsi, sehingga memperoleh data yang lengkap dan akurat (Pratama *et al*., 2019).

1.6.8. Metode Analisis Data

Metode pengembangan Penelitian yang duganakan dalam penelitian ini yaitu Teknik *K-Means Clustering* dengan menggunakan aplikasi *RapidMiner*. Dengan menggunakan sebuah metode K-means *Clustering* dan dibantu oleh aplikasi *RapidMiner* maka dapat mengolah data berdasarkan setiap kolom yang telah ada. Penelitian ini akan menghasilkan beberapa kelompok data yang sesuai dengan frekuensi atau jumlah berdasarkan presentase yang digunakan seperti tinggi, rendah,sedang dan cukup. Dengan menggunakan metode k – means *Clustering* merupakan sebuah algoritma klasterisasi yang banyaj digunakan dalam berbagai penelitian daritingkat kecil sampai menengah karena kemudahan implementasinya.

Adapun pengertian mengenai K- Mens *Clustering* berdasarkan Suyanto (2017), dalam bukunya yang berjudul Data *mining* : untuk klasifikasi dan klasterisasi data mengartikan bahwa metode k-means adalah sebuah algoritma klasterisasi yang mempunyai ide dasar sederhana dengan memproses seminimal mungkun *Sum of Squared Error* (SSE) antara objek data dengan sejumlah *centroid* yang ada dalam data tersebut.

Dalam melakukan penelitian ini menggunakan metode observasi langsung untuk melakukan pengumpulan data dengan melakukan pemasangan *mikrotik* pada Server di Bekangdam 2 Sriwijaya. Dengan adanya alat *Mikrotik* akan mendeteksi setiap lalu lintas jaringan yang terhubung ke server dan mengenali setiap perilaku yang mencurigakan dalam server tersebut. Setiap trafik atau lalu lintas jaringan internrt yang masuk ke server akan di deteksi dan dicatat kemudian disimpan dalam sebuah data *log mikrotik*. Data *Log* yang telah didapatkan akan dilakukan pengelompokkan data sehingga mendapatkan pengumpulan data dari penelitan. Data ini bersumber dari Data *Log mikrotik* dengan menggunakan metode K-Means *Clustering* akan dilakukan penentuan setiap resiko berdasarkan kategori serangan dari setiap data melalui perhitungan nilai. (Haris *et al*., 2020). Berikut ini gambar dalam melakukan metode K-Means *Clustering*.



Gambar 1.1 Metode Teknik *Clustering*

1.6.8.1. *Preprocessing*

Pada tahapan ini akan dilakukan beberapa penambahan parameter yang digunakan untuk memenuhi syarat dalam mengelompokkan tingkatan risiko dari suatu data dalam hal ini yaitu data *log* server *mikrotik* di Bekangdam II Sriwijaya, Parameter yang akan digunakan diantaranya Prioritas, *Port*, dan Frekuensi. Berikut ini merupakan penjelasan dari parameter yang diberikan (Haris *et al.*, 2020).

Parameter	**Penjelasan**
Prioritas	Setiap data *log* akan ditentukan berdasarkan urutan dari setiap data serangan yang harus diperhatikan. Dalam prioritas akan dibagi menjadi tiga yaitu *Low* yaitu 1 dan 2, *Medium* yaitu 3, dan *High* yaitu 4.

Port	Data *log* yang telah didapatkan akan diberikans sebuah nilai untuk menentukan *port* mana saja yang digunakan dalam pengaksesan. Dalam *Port* akan dibagi menjadi tiga diantaranya *Well-Known Port* yaitu 4, *Registered Port* yaitu 3, dan *Dynamic / Private Port* yaitu 1-2.
Frekuensi	Pada frekuensi akan menentukan berapa jumlah serangan yang telah dikirimkan. Maka pada frekuensi akan diberikan nilai parameter diantaranya adalah 1-2 yaitu *Low*, 3 yang berarti *Medium*, dan 4 adalah frekuensi tertinggi *High*.

Tabel 1.1 Parameter Nilai Risiko

1.6.8.2. *Clustering*

Setelah melakukan pengelompokkan data dengan tahapan *preprocessing* maka tahapan selanjutnya adalah tahapan *clustering* yaitu melakukan pengelompokkan data dari *data log* yang telah didapatkan melalui tahapan *preprocessing*, Hasil data yang didapatkan akan memiliki karaterisktik berdasarkan parameter yang telah disebutkan menggunakan metode K-Means *Clustering*.

1.6.8.3. *Risk Assessment*

Setelah melalui tahap *preprocessing* tahapan selanjutnya adalah Tahapan *riskassessment.* Pada tahapan ini setiap hasil dari *clustering* akan menghasilkan tiga titik pusat *centroid* akhir. Tiga titik *centroid* ini akan menghasilnya rata – rata frekuensi yang ada pada setiap *cluster*. Setiap *Cluster* akan memiliki masing – masing *centroid* dan tidak aka nada yang sama. Untuk menghitung setiaap nilai resiko serangan yang dilakukan pada server di Bekangdam II Sriwijaya akan menggunakan rumus perhitungan nilai risiko dari parameter yang telah ditentukan. Rumus dalam menentukan hasil tersebut dapat dilihat pada Tabel 1, yaitu : (Haris *et al*., 2020).

Prioritas (P) = {1-4}
Port (D) = {1-4}
Frekuensi (F) = {1-5}
MaxRA = 10

$$RA = \frac{P * D * F}{X}$$

Dari hasil penelitian yang telah dilakukan ditemukan bahwa nilai untuk parameter P memiliki rentang nilai antara 1 sampai 4,Sedangkan untuk parameter Port (D) mempunyai rentang nilai antara 1 sampai 4, Pada parameter Frekuensi (F) ditemukan bahwa nilai antara 1 sampai 5. Setiap parameter memilih nilai Maksimal yang berarti yang memiliki tingkat parameter tertinggi. Untuk mencari nilai resiko dari setiap parameter dapat menggunakan rumus sebagai berikut (Haris *et al*., 2020):

$$\text{Max}(P) = 4, \text{Max}(D) = 4, \text{Max}(F) = 5$$

$$RA = \frac{4 * 4 * 5}{X} = 10$$

$$X = \frac{80}{10} = 8$$

$$RA = \frac{P * D * F}{8}$$

Pada Parameter P memiliki nilai parameter yaitu 4, Sedangkan pada Parameter D memiliki nilai maksimal parameter (D) yaitu 4, dan Pada parameter F memiliki nilai maksimal adalah 5. Dari setiap parameter yang dihasilkan akan mendapatkan Nilai X yang diperoleh adalah 8. hasil ini didapatkan dari Persamaan 3 paramater. Untuk mencari tahu mengenai fungsi *RA* akan digunakan untuk mencari beberapa nilai risiko berdasarkan titik pusat *centroid* akhir . Dari setiap Hasil nilai risiko yang telah didapatkan akan dibagi lagi berdasarkan kategori risiko

serangan yang dapat dilihat seperti pada Tabel 1.2 (Haris *et al*., 2020).

Kategori Resiko Serangan	
Nilai Resiko	**Kategori**
1	Low
2	Medium
3	High

Tabel 1.2 Kategori resiko serangan

Pada tabel 2 yaitu mengenai Parameter yang berdasarkan kategori resiko serangan merupakan kategori risiko serangan berdasarkan hasil dari nilai risiko. Hasil dari setiap nilai risiko memiliki rentang nilai 1 sampai dengan 4. Dari nilai tesebut nilai 1 termasuk dalam kategori risiko serangan dengan tingkat *Low*, nilai 2 termasuk dalam kategori risiko serangan dengan tingkat *Medium*, dan Nilai 3 termasuk dalam kategori resiko serangan dengan tingkah *High*.

1.6.8.4. *Evaluation*

Setelah menentukan *Risk Assessment* maka akan menghasilkan hasil *clustering.* Hasil yang didapatkan harus terlebih dahulu dilakukan proses evaluasi yang akan menentukan hasil tersebut dapat dikatan sebagai hasil yang telah optimal atay tidak. Jika hasil yang didapatkan adalah optimal maka penelitian terhadap nilai resiko serangan ada benar. Jika tidak maka perlu untuk dilakukan penelitian lebih lanjut dari hasil yang didapatkan. Untuk melakukan evaluasi terhadap hasil clustering dapat menggunakan salah satu metode yaitu *Silhouette Coefficient*. Metode *Silhouette Coefficient* digunakan untuk mengetahui telah optimal atau tidak dari hasil penelitian menggunakan metode K-Means Clustering (Haris *et al*., 2020).

1.7 Sistematika Penulisan

Untuk menguraikan dan memberikan gambaran dari apa yang penulis buat, maka dibuat sistematika penulisan sebagai berikut :

BAB 1 PENDAHULUAN

Pada bab ini berisi mengenai latar belakang, rumusan masalah, Batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian dan sistematika penulisan dalam pembuatan skripsi.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi tentang tinjauan umum dari objek yang menjadi tempat penelitian dan penjelasan teori-teori yang sesuai dengan penelitian yang sedang dilakukan.

BAB III ANALISIS

Pada bab ini membahas analisis dan metode pengembangan sistem yang digunakan yaitu K-Means *Clustering* yang memberikan informasi mengelompokkan informasi data *mining log* server *mikrotik* untuk menganalisa pola serangan dengan *teks clustering* di Bekangdam II Sriwijaya.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini membahas tentang hasil dari analisa yang menggunakan metode K- Means Clustering yang mengelompokkan informasi data *mining log* server *mikrotik* untuk menganalisa pola serangan dengan *teks clustering* di Bekangdam II Sriwijaya.

BAB V KESIMPULAN DAN SARAN

Pada bab ini membahas kesimpulan dari keseluruhan penelitian yang dilakukan dan saran-saran yan diharapkan dapat berguna bagi pembaca dan instansi.


Universitas
Bina
Darma