DETEKSI ANOMALI *TRAFFIC* DATA PADA *WEB SERVER* DENGAN METODE *OUTLIER* DAN *NAIVE PATTERN*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

JUNED RIANDI
09111001055

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018

HALAMAN PENGESAHAN

DETEKSI ANOMALI *TRAFFIC* DATA PADA *WEB SERVER* DENGAN METODE *OUTLIER* DAN *NAIVE PATTERN*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

Juned Riandi
09111001055

Ketua Jurusan Sistem Komputer

UNIVERSITAS SRIWIJAYA FAKULTAS ILMU KOMPUTER JURUSAN SISTEM KOMPUTER

Rossi Passarella, M.Eng.
NIP. 19780611 201012 1 004

Inderalaya, September 2018

Pembimbing

Deris Stiawan, Ph.D.
NIP. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa
Tanggal : 31 Juli 2018

Tim Penguji :

1. Ketua	**: Sutarno, M.T.**	( )
2. Pembimbing	**: Deris Stiawan, Ph.D.**	( )
3. Penguji I	**: Ahmad Heryanto, M.T.**	( )
3. Penguji II	**: Rido Zulfahmi, M.T.**	( )

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M. Eng.
NIP. 19780611 201012 1 004

Rossi Passarella, M.Eng.
NIP. 197806112010121004

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Juned Riandi

NIM : 09111001055

Judul TA : Deteksi Anomali *Traffic* Data Pada *Web Server* Dengan Metode *Outlier* Dan *Naive Pattern*

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil plagiat. Apabila ditemukan unsur plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, September 2018

METERAI TEMPEL

53B45AFF080521689

6000

ENAM RIBU RUPIAH

Juned Riandi

HALAMAN PERSEMBAHAN

“Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya”

(QS. Albaqoroh 286)

“Sesungguhnya Allah tidak akan merubah keadaan suatu kaum sebelum mereka merubah keadaan diri mereka sendiri “

(QS. Ar-Ra’d)

“Tidaklah menimpa seorang mukmin berupa rasa sakit (yang terus menerus), rasa capek, kekhawatiran (pada pikiran), sedih (karena sesuatu yang hilang), kesusahan hati atau sesuatu yang menyakiti sampai pun duri yang menusuknya melainkan akan dihapuskan dosa-dosanya.”

(HR. Bukhari dan Muslim)

Tugas Akhir ini ku persembahkan untuk:

- **Ayah, Ibu, Ayuk Febri, Dek Rerin dan Dek Purti serta Keluarga Besar**
- **Teman-teman Sistem Komputer 2011**
- **Almamater Universitas Sriwijaya**

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Allah SWT yang telah memberikan nikmat dan karunianya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul **"Deteksi Anomali *Traffic* Data Pada *Web Server* Dengan Metode *Outlier* Dan *Naïve Pattern*".** Laporan ini disusun setelah melaksanakan tugas akhir yang diajukan untuk memperoleh gelar Sarjana Komputer di jurusan Sistem Komputer, Universitas Sriwijaya.

Sholawat dan salam tidak lupa penulis kirimkan kepada Rasulullah Muhammad SAW yang menjadi panutan dan teladan bagi umat manusia sehingga kehidupan umat manusia menjadi lebih baik dalam segala bidang.

Dalam penulisan tugas akhir ini penulis menyadari bahwa penulis banyak mendapat dukungan dari berbagai pihak. Oleh karena itu dalam kesempatan ini penulis ingin menyampaikan terima kasih kepada :

1. Keluarga tercinta, Ayah dan Ibu telah membesarkan saya dengan penuh kasih sayang, Ayuk Ferbriani, adik-adiku Fajar Rerin & Putri Sepriani serta seluruh keluarga besar yang telah membantu do'a, serta dukungan baik moril maupun materil.
2. Bapak Rossi Passarella, M.Eng. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Sutarno, M.T. selaku dosen pembimbing akademik, terimakasih saya ucapkan atas nasehatnya selama penulis menempuh perkuliahan di Jurusan Sistem Komputer, Fasilkom, Universitas Sriwijaya.
4. Bapak Deris Stiawan, Ph.D. selaku Dosen Pembimbing Tugas Akhir yang telah meluangkan banyak waktu untuk membimbing penulis dalam menyelesaikan tugas akhir ini.

5. Bapak Ahmad Heryanto, M.T. & Bapak Rido Zulfahmi, M.T. selaku dosen penguji sidang TA1 & TA2
6. Bapak Ibu dosen jurusan Sistem Komputer yang telah menyalurkan ilmu dan pengalamannya.
7. Semua teman-teman seperjuangan di jurusan Sistem Komputer Angkatan 2011, kakak tingkat dan adek tingkat, terimakasih segala dukungan dan bantuannya.
8. Terkhusus untuk sahabat-sahabat yang sudah banyak membantu yang rela menemani dan memberikan waktu luangnya Agung Wahyu Buana, Ahmad Zaki, S.Kom, Amelia Desiana, Budiman, Eko Saputra, Farid Wazdi, Fitri Mareta, Inro Bernamanuel Simbolon, Maido Arfindra Putra, Satria Puja Kesuma. Semoga allah membalas segala kebaikan yang telah kalian berikan.
9. Kak Ahmad Reza & Mbak Iis Oktaria sebagai admin jurusan Sistem Komputer yang telah sering direpotkan, terima kasih sebesar-besarnya serta seluruh Civitas Fakultas Ilmu Komputer Universitas Sriwijaya

Penulis juga sadari dalam penulisan tugas akhir ini jauh dari kesempurnaan baik dari materi maupun penyajiannya karena kurangnya pengetahuan dan pengalaman penulis, maka dari itu sangat diharapkan saran dan kritik dari pembaca agar lebih baik lagi untuk hal berikutnya.

Inderalaya, September 2018

Penulis

DETEKSI ANOMALI TRAFFIC DATA PADA *WEB SERVER* DENGAN METODE *OUTLIER* DAN *NAIVE PATTERN*

Juned Riandi (09111001055)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Abstrak

Intrusion detection system (IDS) adalah sistem keamanan jaringan untuk mendeteksi adanya *intrusion* yang dilakukan oleh *intruder* pada jaringan komputer. IDS dapat dirancang dengan metode *outlier* dan *naïve pattern*. Metode *outlier* digunakan sistem IDS untuk mendeteksi *anomaly traffic* data pada *web server*. Metode *naive pattern* digunakan sistem IDS untuk mencocokan *pattern* serangan pada *rule base* sistem IDS dengan *access.log webserver*. Pada penelitian ini sistem IDS yang dirancang dengan metode *outlier* dan *naïve pattern* berhasil mendeteksi serangan dengan baik. IDS akan mengeluarkan *output* anomali level 1 ketika hanya terdeksi *outlier* pada ukuran *traffic* data, *output* anomali level 2 ketika hanya terdeteksi *pattern* serangan pada *access.log web server* dan *output* anomali level 3 ketika anomali pada ukuran *traffic* data dan *pattern* serangan pada *access.log web server* terdeteksi.

Kata kunci : *Intrusion Detection System* (IDS), *Outlier*, *Naïve Pattern*, *Traffic* data, *access.log web server*

TRAFFIC DATA ANOMALY DETECTION ON WEB SERVER WITH OUTLIER AND NAÏVE PATTERN METHODS

Juned Riandi (09111001055)

Departement of Computer Engineering, Faculty of Computer Science, Sriwijaya University

Abstract

Intrusion detection system (IDS) is a network security system to detect any intrusion which performed by the intruder on the computer network. IDS able to design with outlier and naïve pattern method. Outlier Methode is used by IDS to detect the anomaly traffic data on a web server. Naive pattern method is used by IDS to match the pattern of attacks on IDS rule base system with webserver access.log . in this Research IDS designed with outlier and naïve pattern method is succes to detect the attack well. IDS will produce level 1 anomaly output when only detected an outlier on the size of traffic data, anomaly output level 2 is when only detected pattern of attacks on access.log web server and anomaly output level 3 is output when anomalies on the size of the traffic data and pattern of attacks on access.log web server is detected.

Keywords : *Intrusion Detection System (IDS), Outlier, Naïve Pattern, Traffic data, access.log web server*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

BAB I. PENDAHULUAN

1.1. Latar Belakang

Intrusion detection system (IDS) adalah perangkat lunak yang beroperasi sebagai mekanisme keamanan jaringan untuk melindungi sistem jaringan komputer dari serangan. Dengan meningkatnya jumlah data yang ditransmisikan secara bertahap dari satu jaringan ke yang lain maka resiko penyerangan terhadap sistem akan meningkat. Teknologi IDS dapat digunakan untuk mengidentifikasi intrusi dalam kumpulan data besar secara efektif [1].

Ada dua jenis sistem IDS yaitu *host based* IDS dan *network based* IDS. Sebuah *host based* IDS hanya berfunsi untuk menganalisa area dalam *host* apakah ada anomali, penyusupan atau serangan sedangkan *network based* IDS berfungsi untuk menganalisa lalu lintas *packet* pada suatu jaringan apakah ada anomali, penyusupan atau serangan [1].

Traffic monitoring adalah topik penelitian penting dalam bidang jaringan komunikasi, yang melibatkan banyak kelompok penelitian di seluruh dunia. Monitoring dan analisis lalu lintas selalu dilihat sebagai metodologi kunci untuk memahami jaringan telekomunikasi dan teknologi internet. Evolusi jaringan dalam dekade terakhir telah terlihat dari cara pengguna menggunakan jaringan. Kategori-kategori aplikasi baru seperti *game online*, *peer to-peer*, dan layanan multimedia baru telah diperkenalkan. Aplikasi dan serangan jahat telah menjadi ancaman harian terhadap stabilitas jaringan dan keamanan. Penyedia layanan jaringan selalu berupaya untuk mengoptimalkan konsumsi sumber daya kualitas layanan, pemecahan masalah, dan mengurangi ancaman [2].

Outlier atau Pencilan merupakan data hasil pengamatan yang sangat berbeda dari data lainnya. Data *outlier* mengandung informasi yang berguna untuk mendeteksi ketidak stabilan suatu sistem. Aplikasi untuk mendeksi *outlier* memiliki fungsi penting untuk mendeteksi penipuan, analisis ketangguhan jaringan, dan sistem IDS [3].

Pattern Matching atau *string matcing* adalah teknik yang sangat penting dan popular yang digunakan pada banyak aplikasi. *String Matching* saat ini digunakan pada dunia komputer, internet dan teknologi informasi. *String matching* digunakan pada jejaring sosial, mesin pencari, situs *e-commerce*, aplikasi kamus dan juga digunakan pada aplikasi keamanan jaringan IDS [4].

Pada penelitian [1], disebutkan *Outlier* adalah pola dalam data yang tidak sesuai dengan gagasan perilaku normal yang terdefinisi dengan baik. Deteksi *outlier* bertujuan untuk menemukan pola dalam data yang tidak sesuai dengan perilaku normal. Deteksi *outlier* dapat digunakan untuk meningkatkan kemampuan teknologi sistem IDS.

Pada Penelitian [4], disebutkan *string matching* adalah suatu teknik yang berperan penting dalam dunia keamaanan jaringan. *String matching* dapat digunakan suntuk merancang sistem IDS dengan metode *signature based*.

Pada penelitian [5], disebutkan untuk melindungi jaringan dari dari *traffic* data yang berpotensi membahayakan jaringan hasus disediakan sarana untuk memonitor lalu lintas data yang melintasi jaringan dan menyediakan sarana untuk menanggapi ketika serangan terhadap jaringan terjadi.

Pada penelitian ini akan dibuat sistem IDS untuk mendeteksi anomali *traffic* data *pada web server* dengan metode *outlier* dan metode *naïve pattern string matching*.

1.2. Tujuan

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Membuat desain sistem untuk mendeteksi anomali *traffic* data pada *web server* menggunakan metode *outlier*.
2. Membuat desain sistem untuk mendeteksi anomali *traffic* data pada *web server* menggunakan metode *naïve pattern.*

3. Menganalisa tingkat keberhasilan, dan akurasi sistem dalam mendeteksi serangan pada *web server*

1.3. Manfaat

Adapun manfaat yang dapat diambil dengan dilakukannya penelitian ini adalah :

1. Dapat merancang sebuah program *Intrusion Detection System* (IDS) dengan metode *outlier* dan metode *naïve pattern* yang dapat mendeteksi anomali *traffic* data pada *web server*.
2. Dapat mendeteksi serangan anomali *traffic* data pada *web server* dengan metode *outlier*.
3. Dapat mendeteksi serangan anomali *traffic* data pada *web server* dengan metode *naïve pattern*.

1.4. Rumusan Masalah

Rumusan masalah yang muncul dalam penelitian ini adalah :

1. Bagaimana merancang suatu sistem pendeteksi anomali *traffic* data pada *web server* dengan metode *outlier*.
2. Bagaimana cara mendeteksi anomali *traffic* data pada *web server* dengan metode *outlier*.
3. Bagaimana cara mendeteksi anomali *traffic* data pada *web server* dengan metode *naïve pattern*.

1.5. Batasan Masalah

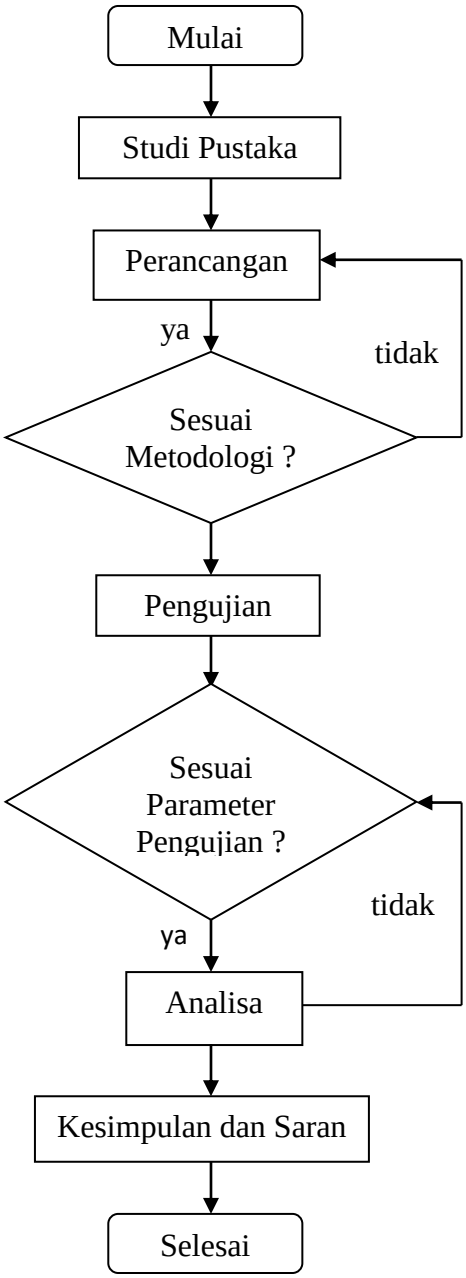
Batasan masalah dalam tugas akhir ini yaitu sebagai berikut :

1. Sistem yang dirancang hanya digunakan untuk pendeteksian anomali *traffic* data pada *web server* dengan metode *outlier* dan metode *naïve pattern.*
2. Penelitian ini menekankan penerapan metode *outlier* dan metode *naïve pattern* untuk mendeteksi anomali *traffic* data pada *web server*.
3. Pengujian hanya dilakukan untuk melihat tingkat keberhasilan IDS dalam mendeteksi anomali *traffic* data pada *web server*.

4. *Traffic* Data yang dilakukan pengecekan adalah *traffic* data berdasarkan *interface* jaringan.
5. *Traffic* Data yang dilakukan pengecekan adalah ukuran *traffic* data secara keseluruhan bukan berdasarkan protokol.

1.6. Metodologi Penelitian

Metodologi yang akan digunakan dalam penelitian ini dibagi dalam beberapa tahapan berikut ini :



Gambar 1.1 *Flowchart* Metodologi Penelitian

1. Studi Literatur dan Konsultasi

   Pada tahap ini dilakukan untuk mencari, membaca dan mengumpulkan referensi atau literatur tentang , anomali *traffic* data, *web server*, dan metode *outlier* dan metode *naïve pattern* yang dapat menunjang penyelasaian penulisan tugas akhir.

   Konsultasi dilakukan dengan cara berkonsultasi degan orang-orang yang memiliki kompetensi di bidang keamanan jaringan komputer.
2. Perancangan Sistem

   Pada tahap ini dilakukan untuk menentukan instrumen yang cocok untuk merancang dan membuat sistem deteksi anomali *traffic* data pada *web server* dengan metode *outlier* dan metode *naïve pattern.*
3. Eksperimen

   Pada tahap ini akan dibuat simulasi topologi jaringan komputer, bagaimana sistem pendeteksi deteksi anomali *traffic* data pada *web server* dengan metode *outlier* dan metode *naïve pattern* akan bekerja yang akan menunjang hasil penelitian.
4. Analisis Sistem

   Pada tahap ini hasil dari eksperimen di tahap sebelumnya akan di analisis untuk kelebihan dan kekurangan pada hasil perancangan supaya kekurangan pada hasil rancangan dapat digunakan untuk penelitian selanjutnya.

1.7. Sistematika Penulisan

Untuk memudahkan dalam penyusunan tugas akhir ini dan memperjelas isi dari setiap bab yang ada pada tugas akhir ini, maka dibuatlah sistematikapenulisan sebagai berikut

BAB I. PENDAHULUAN

Bagian pendahuluan berisi latar belakang, tujun dan manfaat penulisan, perumusan masalah, pembatasan masalah, metode penelitian yang digunakan, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi tentang pengenalan anomali, *traffic* data, *web server*, dan metode *outlier* dan metode *naïve pattern*

BAB III METODOLOGI PENELITIAN

Pada bab ini berisi tentang perencanaan tugas akhir, yang meliputi perancangan, pembuatan sistem keamanan yang dapat mendeteksi anomali *traffic* data pada *web server* dengan metode *outlier* dan metode *naïve pattern.*

BAB IV HASIL DAN ANALISA

Pada bab ini berisi tentang proses pengolahan data dari hasil pengujian sistem keamanan pendeteksi deteksi anomali *traffic* data pada *web server* dengan metode *outlier* dan metode *naïve pattern.*

BAB V KESIMPULAN

Pada bab ini berisi kesimpulan tentang apa yang diperoleh setelah melakukan analis data hasil penelitian.

DAFTAR PUSTAKA

[1] M. Ibrahim Salim and T. A. Razak, “A study on IDS for preventing denial of service attack using outliers techniques,” Proc. 2nd IEEE Int. Conf. Eng. Technol. ICETECH 2016, no. March, pp. 768–775, 2016.

[2] E. Biersack, F. Measurement, and D. Hutchison, Data Traffic Monitoring and Analysis, vol. 7754. 2013.

[3] Aggarwal, C. C. Outlier analysis. In Data mining (pp. 237-263). Springer International Publishing Switzerland, Cham. 2015.

[4] CHOI, Byungkwon, et al. DFC: Accelerating String Pattern Matching for Network Applications. In: NSDI. p. 551-565., 2016.

[5] R. D. Carpenter and K. Maloney, “(12) Patent Application Publication (10) Pub . No .: US 2006 / 0222585 A1 Figure 1,” vol. 002, no. 15, p. 354, 2015.

[6] S. P. Oriyano, Certified Ethical Hacker v9 Study Guide, vol. 0700, no. option 2, 2016.

[7] Mohanan, Vasuky, Rahmat Budiarto, and Ismat Aldmour, eds.Powering the Internet of Things With 5G Networks. IGI Global, 2017

[8] M. A. Novianta and E. Setyaningsih, “Sistem Informasi Monitoring Kereta Api Berbasis Web Server Menggunakan layanan GPRS,” Momentum, vol. 17, no. 2, pp. 58–67, 2015.

[9] D. Lukitasari and A. fali Oklilas, “Analisis Perbandingan Load Balancing Web Server Tunggal Dengan Web server Cluster Menggunakan Linux Virtual Server,” Generic, vol. 5, no. 2, pp. 31–34, 2013.

[10] Kanimozhi, R. Data analysis using box plot on electricity consumption. In Electronics, Communication and Aerospace Technology (ICECA), International conference of (Vol. 2, pp. 598-600). IEEE, 2017.

[11] Moustafa, Nour, Gideon Creech, and Jill Slay. "Anomaly Detection System Using Beta Mixture Models and Outlier Detection." Progress in Computing, Analytics and Networking. Springer, Singapore, pp. 125-135, 2018.

[12] Harshita and R. Nayyar, “Detection of ICMP Flood DDoS Attack,” International Journal of New Technology and Research (IJNTR)., vol. 5, no. 2, pp. 199–205, 2017.

[13] Sheshasayee, “A Comparitive Analysis of Single Pattern Matching Algorithms in Text Mining,” International Conference on Green Computing and Internet of Things (ICGCIoT)., pp. 1–6, 2015.

[14] K. Ritesh, M. Nishchol and P. Ravindra “A Survey and Analysis on String Matching Techniques and its Applications-text,” Int. J. Appl. or Innov. Eng. Manag., vol. 4, no. 12, pp. 67–73, 2015.

[15] E. D’Souza, “Comparitive Analysis on Efficiency of Single String Pattern Matching,” Int. J. Latest Trends Eng. Technol., pp. 221–225, 2016.