Deteksi Serangan *Remote to Local* (R2L) Menggunakan Metode *Support Vector Machine* (SVM)

TUGAS AKHIR

OLEH :

MUHAMMAD FACHRURROJI ILHAM SAPUTRA

09011181320025

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2019

Deteksi Serangan *Remote to Local* (R2L) Menggunakan Metode *Support Vector Machine* (SVM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

MUHAMMAD FACHRURROJI ILHAM SAPUTRA

09011181320025

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2019

LEMBAR PENGESAHAN

DETEKSI SERANGAN REMOTE TO LOCAL (R2L) MENGGUNAKAN METODE SUPPORT VECTOR MACHINE (SVM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

MUHAMMAD FACHRURROJI ILHAM SAPUTRA
09011181320025

Palembang, Desember 2019

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng.
NIP. 197806112010121004

Pembimbing

Deris Stiawan, M.T,. Ph. D
NIP. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :
Hari : Selasa
Tanggal : 10 Desember 2019

Tim Penguji :

1. **Ketua** : **Aditya Putra Perdana, M.T.**
2. **Anggota I** : **Ahmad Fali Oklilas, M.T.**
3. **Anggota II** : **Sarmayanta Sembiring, M.T.**

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng.
NIP. 197806112010121004

HALAMAN PERNYATAAN

Yang bertandatangan dibawah ini :

Nama	: Muhammad Fachrurroji Ilham Saputra
NIM	: 09011181320025
Program Studi	: Sistem Komputer
Judul Skripsi	: Deteksi Serangan *Remote to Local* (R2L) Menggunakan Metode *Support Vector Machine* (SVM)

Hasil Pengecekan *Software iThenticate/Turnitin* : 6%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik yang diberikan oleh Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Demikian Pernyataan ini saya buat dengan sebenar-benarnya.

Palembang,

Yang menyatakan,

Muhammad Fachrurroji Ilham Saputra
NIM. 09011181320025

HALAMAN PERSEMBAHAN

"Hanya kamu dan kamu sendiri yang bisa mengubah situasimu, jangan menyalahkannya kepada siapapun atau apapun."

وَلِكُلِّ أُمَّةٍ أَجَلٌ ۖ فَإِذَا جَاءَ أَجَلُهُمْ لَا يَسْتَأْخِرُونَ سَاعَةً ۖ وَلَا يَسْتَقْدِمُونَ

Artinya : *"Tiap-tiap umat mempunyai batas waktu; maka apabila telah datang waktunya mereka tidak dapat mengundurkannya barang sesaatpun dan tidak dapat (pula) memajukannya."*

(QS. Al-A'raaf :34).

Dengan mengucap syukur Alhamdulillah atas rahmat Allah Subhanahu wa Ta'ala, kupersembahkan karya kecil ini untuk . . .

Kedua orang tua tercinta

(Bapak Bambang Sutrisno dan Ibu Mauli Diana)

Kedua Adik ku

(Khairil Arya Ramadhan dan Feby Nur Khotimah)

Kekasih tercinta

(Aila Askanah Embun)

Teman-teman seperjuangan jurusan,

(Sistem komputer angkatan 2013)

Almamater perjuangan

(Universitas Sriwijaya)

23 Desember 2019

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan rahmat, hidayah serta ijin-Nya sehingga penulis dapat menyelesaikan penulisan tugas akhir dengan judul **"Deteksi Serangan Remote to Local (R2L) Menggunakan Metode Support Vector Machine (SVM)".** Penulisan tugas ahir ini dibuat dalam rangka memenuhi persyaratan untuk menyelesaikan pendidikan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya untuk memperoleh gelar strata 1.

Selama penyusunan laporan ini, penulis mendapatkan banyak bantuan dari berbagai pihak yang berupa bimbingan, saran, dan petunjuk. Oleh karena itu, pada kesempatan kali ini penulis menyampaikan terimakasih yang tak terhingga kepada semua yang membantu penulis dalam menyelesaikan laporan tugas akhir ini. Semoga apa yang telah diberikan oleh mereka mendapatkan balasan yang berlimpah dari Tuhan Yang Maha Esa. Penulis juga ingin mengucapkan terima kasih kepada : Orang-orang tercinta, Kedua orang tua saya (Bapak Bambang Sutrisno dan Ibu Mauli Diana), terimakasih atas kasih sayang, semangat, ridha dan segalanya yang telah bapak ibu berikan serta adik saya Khairil Arya Ramadhan dan Feby Nur Khotimah selalu membantu dan memberikan semangat, yang telah menjadi penyemangat saya dalam mengerjakan skripsi ini.

1. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
2. Bapak Rossi Passarella, M.Eng. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Deris Stiawan, M.T., Ph.D selaku Dosen Pembimbing Tugas Akhir
4. Bapak Huda Ubaya, M.T. selaku Pembimbing Akademik.
5. Kak Aditya Putra P Prasetyo,S.Kom., MT. selaku Ketua Tim Penguji
6. Bapak Ahmad Fali Oklilas, M.T. dan bapak Sarmayanta Sembiring, M.T. selaku Anggota Tim Penguji Tugas Akhir.
7. Bapak dan Ibu dosen jurusan Sistem Komputer yang telah memberikan pelajaran selama perkuliahan.

8. Kedua Orang Tua-ku Bambang Sutrisno dan Mauli Diana yang sangat aku sayangi yang selalu memberikan kasih sayang, dukungan, do'a, dan nasehat yang sangat berguna, serta tak kenal lelah untuk mendidik-ku menjadi lebih baik
9. Kakak ku Rizqie Aras Perdana dan kedua adik ku Khairil Arya Ramadhan, Feby Nur Khotimah yang selalu mendukung dan peduli dalam menggapai cita-cita.
10. Teruntuk teman-teman satu angkatan, khususnya Sistem Komputer kelas A dan B, Andhika Riski Perdana, S.Kom (ketua Angkatan 2013), Eko Pratama, S.Kom (ketua kelas), Erick Okvanty Haris, S.Kom, Tri Atmoko Malik Kurniawan, Imam Mustofa, S.Kom, Ahmad Kuswandi, S.Kom, Yoppy Prayudha, Ryan Fitrah Perdana, S.Kom, Dwi Kurnia Putra, S.Kom, Dede Tri Septiawan, S.Kom, Faris Abdul Aziz, S.Kom, Sandi Sarfani, Agus Juliansyah, Indah Sari, S.Kom, Fahrul Rozi, Yayang Paryoga, Kholil Anggara, SKom, Rio Astani, Adi Suryan, Sri Suryani, S.Kom, Fepiliana, S.Kom, Leny Novita Sari, S.Kom, Meilinda Eka Suryani, S.Kom, Ulan Purnamasari, S.Kom, Umi Yanti, S.Kom, Riki Andika, S.Kom, Nova Dyati Pradista, S.Kom, Lisa Mardaleta, S.Kom, Nur Rahma Dela, S.Kom, Saros Sakiana, Kusuma Dwi Indriani, Elfa Purnamasari, S.Kom, Suci Anggraini, S.Kom. Edy, Amir, Bely, Yoga, Diah, Sukses untuk kita semua.
11. Sahabat-Sahabat ; M Ihsan F, Rasyid Kurniawan, Aziz Cahya, Agung Setyo Nugroho, Agung Wicaksono, Fajar Adriansyah, Niko Wijaya, Agung Erlangga, Agung BW, Tomi Kurniawan, Revian, Andre Ngolo, Vinco, Nanda, Yogi Gautama, Aldo, Ramadhan Alfalah, Randy Blek, Redo Saputra, Agus Harley.
12. Kakak dan Adik Tingkat Sistem Komputer; kak Candra Adi Winanto, S.Kom, kak Eko Adi Winanto, S.Kom, mas bram, kak Mamat, kak Agus wahyudi, kak Imam suganda, kak Erick lamdompak, kak Edoy, kak Tahta, kak Bio, Kadapi, Novit, Nina, Ajran, Rido, Atma.
13. Serta semua pihak yang telah membatu baik moril maupun materil yang tidak dapat disebutkan satu persatu dalam penyelesaian tugas ahir ini. Terima kasih semuanya.

Semoga dengan terselesainya tugas ahir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua dalam mempelajari tentang Deteksi Serangan Remote to Local (R2L) Menggunakan Metode Support Vector Machine (SVM).

Dalam Penulisan laporan ini penulis juga sangat menyadari bahwa masih banyak terdapat kekurangan dan ketidak sempurnaan, oleh karena itu penulis mohon saran dan kritik yang membangun untuk Perbaikan Laporan Tugas Akhir ini, agar menjadi lebih baik dimasa yang akan datang.

Palembang, Desember 2019

Penulis

DAFTAR ISI

Halaman

BAB III. METODOLOGI PENELITIAN

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

Attack Detection Remote to Local *(R2L) Use Method* Support Vector Machine *(SVM)*

Muhammad Fachrurroji Ilham Saputra (09011181320025)
Departement of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email : mfilhamsaputra@gmail.com

Abstrak

Detection is a process by which to examine or conduct an examination of something using certain means and techniques. The remote to local attack was a local incursion to get access to an account into a system that didn't have an account into that system before. The r2l attack patterns on darpa databases are identifiable with such parameters as source address, destination address, flags, IP addresses, and TCP claims. It USES vector support technology where SVM produces a classification of offensive and normal files separated by hyperlane line, purple class 1 for attack and -1 for normal yellow file. Results from my classification used SVM in evaluation with confusion matrix to find out how great the accuracy level of detection of attack and normal file and SVM. From this research we obtained a 99.99% accurate rate which is a very good result of accuracy.

Keywords : Detection, *Remote to Local, Snort IDS, Support Vectror Machine*

Palembang, Desember 2019

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng.
NIP. 197806112010121004

Pembimbing

Deris Stiawan M.T., Ph.D.
NIP. 197806172006041002

Deteksi Serangan *Remote to Local* (R2L) Menggunakan Metode *Support Vector Machine* (SVM)

Muhammad Fachrurroji Ilham Saputra (09011181320025)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : mfilhamsaputra@gmail.com

Abstrak

Deteksi adalah suatu proses untuk memeriksa atau melakukan pemeriksaan terhadap sesuatu dengan menggunakan cara dan teknik tertentu. Serangan *remote to local* adalah serangan yang dilakukan oleh *attacker* untuk mendapatkan akses akun ke sebuah sistem yang sebelumnya tidak memiliki akun ke sistem tersebut. Pola serangan R2L pada dataset DARPA dapat dikenali dengan beberapa parameter seperti *source address, destination address, flags, ip length,* dan *tcp length.* Penelitian ini menggunakan metode *Support Vector Machine dimana* SVM menghasilkan klasifikasi antara serangan dan normal file yang dipisahkan berdasarkan garis hyperlane, *class* 1 berwarna ungu untuk serangan dan -1 untuk normal file dengan warna kuning. Hasil dari Klasifikasi menggunakan SVM di evaluasi dengan *confusion matrix* untuk mengetahui seberapa besar tingkat akurasi dari deteksi serangan dan normal file dan SVM. Dari penelitian ini diperoleh tingkat akurasi sebesar 99.99% yang merupakan hasil akurasi yang sangat baik.

Kata Kunci : Deteksi, *Remote to Local, Snort IDS, Support Vectror Machine*

Palembang, Desember 2019

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng.
NIP. 197806112010121004

Pembimbing

Deris Stiawan M.T., Ph.D.
NIP. 197806172006041002

BAB I. PENDAHULUAN

1. LATAR BELAKANG

Intrusion Detection System (IDS) merupakan sistem yang sangat penting dalam keaman jaringan, dimana IDS berguna untuk mendeteksi kemungkinan adanya serangan. Banyak teknik yang digunakan namun secara umum untuk mendeteksi pada IDS adalah dengan menggunakan *rule base* seperti *attack anomaly* dan *attack signature*, tetapi teknik ini masih mempunyai kelemahan. Pada *attack signature* tidak bisa mendeteksi tipe serangan baru yang tidak ada pada *database* serangan. Sedangkan mekanisme dengan *attack anomaly* dapat mendeteksi beberapa varian serangan baru, tetapi sangat sering menimbulkan *false alarm* [1].

Dengan cara pendekatan yang dapat digunakan untuk mengatasi kelemahan tersebut ialah memvisualisasikan keadaan yang kompleks dan sederhana [2]. Manusia bisa dengan mudah mengenali dan menyimpulkan pola dari gambar visual. Untuk mendapatkan gambar dari grafik menggunakan teknik dan algoritma komputer grafik yang diambil dari data mentah. *Support vector machine* adalah tehnik yang paling cocok digunakan untuk analysis data. SVM dapat membantu membedakan dan memisahkan antara serangan dan data normal dengan cara pembagian antar *class* [3][4].

Jenis serangan dapat dibedakan menggunakan layanan, protokol, serta jenis serangan. Salah satu jenis serangan yang lumrah digunakan pada internet adalah *Remote to Local* [5]. Serangan *Remote to Local* (*R2L*) adalah serangan yang terjadi ketika penyerang melakukan pengiriman paket kesebuah mesin melalui jaringan, dimana penyerang tidak memiliki hak akses di mesin tersebut. Terdapat beberapa serangan dari *Remote to Local* salah satunya yaitu *bruteforce* [6].

Penelitian lainnya [7], penerapan *data mining* untuk mendeteksi intrusi dapat menjadi jalan keluar dari permasalahan meningkatnya jumlah data yang besar karena memiliki kelebihan dalam memproses *system logs. Data mining* bisa membantu mengintegrasikan dua teknik pendeteksian intrusi yaitu *anomaly* dan *misuse*. *Data mining* juga bisa menemukan suatu pola dalam *dataset* yang besar dan mempermudah bagi analis untuk mengidentifikasi data kemudian memberikan analisis yang lebih efisien.

Support vector machine (SVM) adalah metode dari *data mining* yang terbukti memiliki akurasi yang tinggi dalam mengklasifikasikan pola-pola paket data jaringan, ini dibuktikan oleh beberapa penelitian yang mempergunakan *dataset* DARPA KDD'99 yang dibuat oleh Lincoln Lab[8]. Dari hasil penelitian tersebut maka *Support Vector Machine* dinilai tepat untuk diimplementasikan dalam penelitian ini.

Dari beberapa ulasan diatas penelitian ini akan menganalisa deteksi serangan *Remote to Local* (R2L) dengan tipe serangan *bruteforce*. Untuk meningkatkan tingkat akurasi dalam pendeteksian serangan diperlukan teknik yang tidak hanya bertumpu pada satu parameter. Oleh karena itu, pada penelitian ini berfokus pada penerapan metode algoritma *Support Vector Machine* (SVM) agar tingkat akurasi yang baik.

II. Tujuan

Adapun tujuan yang akan dicapai pada penelitian ini adalah:

1. Melakukan pengenalan pola *bruteforce*.
2. Menerapkan metode *Machine Learning* dengan *Algoritma Support Vector Machine* untuk mendeteksi serangan *bruteforce.*
3. Menghitung akurasi deteksi serangan *bruteforce.*

III. MANFAAT

Adapun manfaat yang didapatkan dalam penelitian ini adalah:

1. Dapat memberikan kemudahan dalam mengenali pola serangan *bruteforce* pada layanan *telnet*.
2. Dapat memberikan peringatan serangan brutforce pada layanan *telnet*.

IV. RUMUSAN MASALAH

Berdasarkan latar belakang masalah yang ada, permasalahan yang akan dibahas pada penelitian ini ada dua yaitu:

1. Bagaimana algoritma *Support Vector Machine* (SVM) ini dapat mengenali pola paket serangan *bruteforce* atau paket data normal.
2. Bagaimana notifikasi sedini mungkin sebagai peringat dini.

V. BATASAN MASALAH

Batasan masalah tugas akhir ini yaitu sebagai berikut :

1. Dalam penelitian ini digunakan serangan R2L dengan jenis serangan *bruteforce.*
2. Metode yang digunakan untuk mendeteksi serangan menggunakan SVM.
3. Pengujian bersifat *offline.*
4. Menggunakan *Dataset Darpa* 1999.
5. Tidak membahas cara pencegahan serangan tersebut.
6. Tidak diujikan pada lalu lintas jaringan yang terenkripsi.

VI. METODOLOGI PENELITIAN

Metode yang akan digunakan pada penelitian ini yaitu sebagai berikut :

1. Tahap Pertama (Studi Pustaka/Literatur)

   Pada Tahap pertama ini diawali dengan mencari masalah yang sesuai dan relevan untuk diangkat sebagai penelitian. Setelah itu, mencari

beberapa sumber seperti artikel, jurnal, buku, dan yang lainnya yang berhubungan langsung dengan tugas akhir.

2. Tahap Kedua (Perancangan Sistem)

   Tahap kedua ini merupakan tahap yang membahas masalah proses bagaimana membangun metode atau pendekatan tertentu, perangkat lunak maupun perangkat keras apa saja yang digunakan dan konfigurasi system beserta penerapan metode.

3. Tahap Ketiga (Pengujian)

   Pada tahap ketiga ini merupakan tahap lanjutan dari perancangan system dimana pada tahap ini dilakukan pengujian berdasarkan metodologi penelitian dan penelitian sebelumnya sehingga didapatan hasil uji yang sesuai dan tepat secara konsep ataupun praktis.

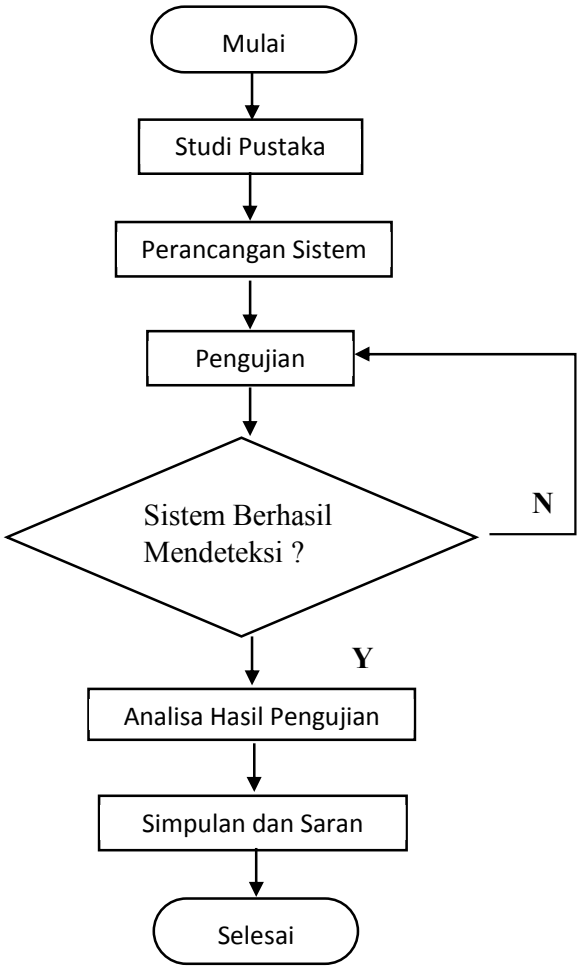
4. Tahap Keempat (Analisa)

   Pada tahap keempat ini dilakukan pengolahan dan analisi data yang diperoleh dari hasil pengujian berdasarkan pendekatan tertentu untuk mendapatkan data yang objektif.

5. Tahap Kelima (Kesimpulan dan saran)

   Pada tahapan ini, akan dirumuskan suatu kesimpulan yang diperoleh dari tahapan –tahapan sebelumnya. Selain itu, ditambahkan beberapa saran yang dapat dijadikan sebagai landasan untuk penelitian selanjutnya.

Pada Gambar 1.1 berikut ditampilkan metodologi penelitian secara visual dalam bentuk diagram alir yang merepresentasikan proses pelaksanaan penelitian:



Gambar 1.1 Diagram Alir Metodologi Penelitian

VII. SISTEMATIKA PENULISAN

Untuk memudahkan dalam proses penyusunan tugas akhir dan memperjelas isi dari setiap bab maka dibuat sistematika penulisan sebagai berikut :

BAB 1. PENDAHULIAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi latar belakang, tujuan, manfaat, rumusan masalah, dan batasan masalah kemudian metodologi penelitian sistematika penulisan.

BAB 2. TINJAUAN PUSTAKA

Pada bab ini berisi dasar teori dari *Intrusion Detection System, Root to Local, Bruteforce, Machine Learning, Support Vector Machine* yang berhubungan dengan penelitian.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini meliputi tahapan perancangan sistem (*System Design*) dan penerapan metode penelitian.

BAB IV. HASIL DAN ANALISA

Pada bab ini menjelaskan hasil pengujian yang dilakukan serta analisis dari tiap data yang diperoleh dari hasil pengujian.

BAB V. KESIMPULAN

Pada bab ini berisi kesimpulan tentang penelitian yang dilakukan, serta menjawab tujuanyang hendak dicapai pada BAB I (Pendahuluan).

DAFTAR PUSTAKA

[1] C. Adi Winanto, "Deteksi serangan Denial of Service mengunakan Artificial Immune System," vol. 2, no. 1, pp. 1–67, 2017.

[2] E. A. Winanto, A. Heryanto, and D. Stiawan, "Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means," *Annu. Res. Semin. 2016*, vol. 2, no. 1, pp. 359–362, 2016.

[3] S. Mukkamala and A. H. Sung, "Feature Selection for Intrusion Detection with Neural Networks and Support Vector Machines," *Transp. Res. Rec. J. Transp. Res. Board*, vol. 1822, no. 1, pp. 33–39, 2007.

[4] T. I. U. of B. Saad Hafeez B.Eng. and A, "Deep Packet Inspection using Snort," *Deep Pack. Insp. using Snort*, p. 24, 2017.

[5] S. Revathi and A. Malathi, "Effective Analysis on Remote to User (R2L) Attacks Using Random Forest Algorithm," *Int. J. Eng. Sci. {&} Res. Technol.*, vol. 3, no. 5, p. 3, 2014.

[6] D. Dey, A. DInda, P. P. Kundapur, and R. Smitha, "Warezmaster and Warezclient: An implementation of FTP based R2L attacks," *8th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2017*, pp. 6–11, 2017.

[7] A. Jacobus and E. Winarko, "Penerapan Metode Support Vector Machine pada Sistem Deteksi Intrusi secara Real-time," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 8, no. 1, p. 13, 2017.

[8] A. Agathou and T. Tzouramanis, "The Role of Data Mining in Intrusion Detection Technology," *Handb. Res. Public Inf. Technol.*, pp. 463–473, 2011.

[9] Dr.J.A.Chandulal, D. K. N. Rao, and S. Akbar, "Intrusion Detection System Methodologies Based on Data Analysis," *Found. Comput. Sci.*, vol. 5, no. 2, pp. 10–20, 2010.

[10] A. Jamdagni, "Payload-based Anomaly Detection in HTTP Traffic," no. November, p. 172, 2012.

[11] D. M. Reeves and G. M. Jacyna, “Support vector machine regularization,” *Wiley Interdiscip. Rev. Comput. Stat.*, vol. 3, no. 3, pp. 204–215, 2011.

[12] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das, “Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation,” pp. 162–182, 2007.

[13] D. Stiawan, S. Sandra, E. Alzahrani, and R. Budiarto, “Comparative analysis of K-Means method and Naïve Bayes method for brute force attack visualization,” *2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017*, no. 09121001005, pp. 177–182, 2017.

[14] D. A. N. Tunneling, “Meningkatkan keamanan port knocking dengan kombinasi special features icmp, source port, dan tunneling,” pp. 187–194, 2016.

[15] G. Hill, “Cable and Telecommunications Professionals’ Reference, 3rd ed. Oxford: Elsevier’s Science & Technology, 2007.”

[16] S. X. Wu and W. Banzhaf, “The use of computational intelligence in intrusion detection systems: A review,” *Appl. Soft Comput. J.*, vol. 10, no. 1, pp. 1–35, 2010.

[17] S. Andrews, I. Tsochantaridis, and T. Hofmann, “Support Vector Machines for Multiple-Instance Learning,” *Adv. Neural Inf. Process. Syst. (NIPS ’02)*, vol. 53, no. 9, pp. 1689–1699, 2002.

[18] H. Zhang, C. He, M. Yu, and J. Fu, “Texture Feature Extraction and Classification of SEM Images of Wheat Straw/Polypropylene Composites in Accelerated Aging Test,” *Adv. Mater. Sci. Eng.*, vol. 2015, no. September 2015, pp. 1–10, 2015.