SISTEM PENCEGAHAN SERANGAN USER TO ROOT (U2R) DENGAN METODE SUPPORT VECTOR MACHINE

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

MONICA ADHELIA

09011181621009

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

SISTEM PENCEGAHAN SERANGAN USER TO ROOT (U2R) DENGAN METODE SUPPORT VECTOR MACHINE

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

MONICA ADHELIA

09011181621009

Indralaya, 11 Januari 2021

Mengetahui,

Pembimbing I Tugas Akhir

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

Pembimbing II Tugas Akhir

Ahmad Heryanto, S.Kom., M.T
NIP. 198701222015041002

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis
Tanggal : 12 November 2020

Tim Penguji :

1. **Ketua** : **Rossi Passarella, S.T., M.Eng.** _____
2. **Sekretaris I** : **Deris Stiawan, M.T., Ph.D.** _____
3. **Sekretaris II** : **Ahmad Heryanto, S.Kom., M.T.** _____
4. **Anggota I** : **Huda Ubaya, S.T., M.T.** _____
5. **Anggota II** : **Sarmayanta Sembiring, S.SI., M.T.** _____

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T
NIP. 196612032006041001

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Monica Adhelia

NIM : 09011181621009

Judul : Sistem Pencegahan Serangan User To Root (U2R) dengan Metode Support Vector Machine

Hasil Pengecekan *Software iThenticate/Turnitin* : 18%

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 dari Universitas Sriwijaya sesuai dengan ketentuan yang belaku.

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

Indralaya, 12 November 2020

Yang menyatakan,

Monica Adhelia

NIM. 09011181621009

HALAMAN PERSEMBAHAN

"Sesungguhnya bersama kesulitan itu pasti ada kemudahan. Maka apabila kamu telah selesai (dari sesuatu urusan), kerjakanlah dengan sungguh-sungguh (urusan) yang lain, dan hanya kepada Tuhanmulah hendaknya kamu berharap." (QS: 94: 6-8)

"Great losses are great lessons" (Anonim)

Skripsi ini saya persembahkan khusus untuk:

- **Almarhumah Ibu (Sutati) dan Ayah (Hamid) tersayang yang tak pernah berhenti memanjatkan doa, memotivasi, mendidik dan mengorbankan segalanya kepada Putri Kembarnya agar dapat mencapai cita-cita yang diinginkan.**
- **Kedua Kakakku (Kak Panji dan Kak Ulan) yang mendoakan, memberikan materi dan semangat hingga sekarang.**
- **Dan patner ku Brigadir Satu Taruna Jihan Andrean yang selalu memotivasi serta ikut pusing mendengarkan keluh kesahku.**
- **Dosen Pembimbing terbaik pak (Deris Stiawan, M.T,. Ph.D.) dan pak (Ahmad Heryanto, S.kom., M.T.)**
- **Keluarga Besar Sistem Komputer Universitas Sriwijaya**

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji dan syukur penulis selalu panjatkan atas kehadirat Allah Swt yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis sampai pada saat ini dapat menyelesaikan penyusunan tugas akhir ini dengan judul "**Sistem Pencegahan Serangan *User To Root* (U2R) dengan Metode *Support Vector Machine***"

Pada penyusunan tugas akhir ini, tidak terlepas dari bantuan, bimbingan, ajaran serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan terima kasih kepada:

1. Allah Subhanahu Wata'ala yang telah memberikan berkah dan karunia-Nya kepada penulis dalam penyusunan tugas akhir ini.
2. Orangtua tercinta yang selalu memberikan motivasi, semangat dan do'a serta keluarga besar yang tersayang.
3. Bapak Jaidan Jauhari, S.Pd. M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya
5. Bapak Sutarno, S.T., M.T. selaku Dosen Pembimbing Akademik.
6. Bapak Deris Stiawan, M.T., Ph.D selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Bapak Ahmad Heryanto, M.T.selaku Dosen Pembimbing II Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya
8. Mbak Winda Kurnia Sari selaku Admin Jurusan Sistem Komputer.
9. My Twins yang super cerewet dan my partner Brigadir Satu Taruna Jihan Andrean yang selalu memberikan dukungan dan semangat saat mengerjakan tugas akhir.
10. Kakak tingkat sistem komputer yang memberikan masukan selama perkuliahan.
11. Derik, Ariak, Ejak, dan Ardin, sebagai teman diskusi dan membantu dalam menyelesaikan tugas akhir ini.
12. Teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2016 terkhusus kelas A, serta semua pihak yang tidak dapat penulis cantumkan satu persatu.
13. Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya.

Dalam pembuatan tugas akhir ini, tentunya penulis merasa masih terdapat kekurangan dan kesalahan. Oleh karena itu, sebagai bahan perbaikan kedepan penulis tentunya mengharapkan koreksi, saran, serta masukan terhadap isi dari tugas akhir ini.

Akhir kata, semoga dengan pembuatan tugas akhir ini akan menjadi tambahan ilmu dan pengembangan wawasan terhadap pengolahan citra digital dan dapat menjadi bahan referensi terhadap mahasiswa yang membutuhkan.

Wa'alaikumsalam Warahmatullahi Wabarakatuh

Indralaya, 11 Januari 2021

Penulis

Monica Adhelia

USER TO ROOT (U2R) ATTACK PREVENTION SYSTEM WITH SUPPORT VECTOR MACHINE METHOD

Monica Adhelia (09011181621009)
Department of Computer Systems, Faculty of Computer Science,
Sriwijaya University
Email: monicaadhelia3@gmail.com

ABSTRACT

Intrusion Prevention System (IPS) is an approach used to build a computer security system that is more advanced than the Intrusion Detection System (IDS), because this IPS can do more than just analyze traffic / logs and generate alerts. IPS responds to detected intrusion packets and will block malicious activity on the network. The dataset used is NSL - KDD which will be detected by IDS Snort so that it gets an attack pattern to perform the detection process using the support vector machine method. The results of the accuracy value of detection using a support vector machine obtained 91.75%. In this study, the IPS system will search for and block packets from Buffer Overflow attacks which have the aim of gaining root access by executing code created by the attacker, the IPS system used is the Suricata Engine which serves as IDPS and performs packet inspection on raw data using rules alert, then suricata will act as IPS and regulate which network traffic is allowed to pass through the IPS system and drop packets that have buffer overflow attacks and drop will be used only in IPS / inline mode.

Keywords : Intrusion Prevention System, Buffer Overflow, Support Vector Machine, NSL – KDD, Suricata.

Mengetahui,

Pembimbing I Tugas Akhir	**Pembimbing II Tugas Akhir**
Deris Stiawan, M.T., Ph.D	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 197806172006041002	**NIP. 198701222015041002**

Ketua Jurusan Sistem Komputer

Dr. Ir. H Sukemi, M.T.
NIP. 196612032006041001

SISTEM PENCEGAHAN SERANGAN USER TO ROOT (U2R) DENGAN METODE SUPPORT VECTOR MACHINE

Monica Adhelia (09011181621009)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email: monicaadhelia3@gmail.com

ABSTRAK

Intrusion Prevention System (IPS) merupakan pendekatan yang digunakan untuk membangun suatu system keamanan komputer yang lebih advance dari *Intrusion Detection Sytem (IDS)*, karena IPS ini dapat melakukan lebih dari sekedar menganalisis *traffic / log* dan menghasilkan *alert*. Dataset yang digunakan adalah NSL – KDD yang akan dideteksi oleh IDS Snort sehingga mendapatkan pola serangan untuk melakukan proses deteksi menggunakan metode support vector machine. Hasil nilai akurasi dari deteksi menggunakan support vector machine diperoleh 91,75%. Dalam penelitian ini system IPS akan mencari dan memblokir paket dari Serangan *Buffer Overflow* yang memiliki tujuan untuk mendapatkan akses *root* dengan mengeksekusi *code* yang dibuat oleh *attacker*, System IPS yang digunakan adalah Suricata Engine yang bertugas sebagai IDPS dan melakukan inspeksi paket pada *raw data* dengan menggunakan rules alert, Selanjutnya suricata akan bertindak sebagai IPS dan mengatur lalu lintas jaringan mana saja yang diperbolehkan untuk melewati sistem IPS dan melakukan drop paket yang terdapat serangan buffer overflow dan drop akan digunakan hanya pada mode IPS / inline saja.

Kata Kunci : Intrusion Prevention System, Buffer Overflow, Support Vector Machine, NSL – KDD, Suricata.

Mengetahui,

Pembimbing I Tugas Akhir	**Pembimbing II Tugas Akhir**
Deris Stiawan, M.T., Ph.D	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 197806172006041002	**NIP. 198701222015041002**

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

DAFTAR ISI

Halaman

BAB IV HASIL DAN PEMBAHASAN

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Intrusion Detection System IDS [1] merupakan kombinasi dari hardware dan *software* yang memiliki fungsi untuk melakukan monitoring sistem atau jaringan dari aktifitas *malicious* yang dilakukan oleh *attacker*. Secara umum, banyak teknik yang digunakan untuk mendeteksi. Menurut [2] IDS dibagi menjadi dua kategori berdasarkan metode deteksi yaitu, *anomaly detection* dan misuse detection. Anomaly detection merupakan metode yang diambil berdasarkan *behaviour* yang jarang dan berbeda dari *behaviour* normal, sedangkan *misuse detection* yang mengidentifikasi serangan dengan melakukan pencocokan data yang dapat dilihat dari behavior.

Dari kedua metode deteksi tersebut masih memiliki kelemahan, pada IDS yang berdasarkan metode *signature based* tidak dapat mendeteksi tipe serangan baru (serangan yang belum dikenali) yang tidak ada di dalam *database.* Sedangkan untuk IDS [3] dengan metode *anomaly based* dapat mendeteksi beberapa variasi terhadap serangan baru, namun masih sangat sering menimbulkan nilai *false alarm* yang besar.

Intrusion Prevention System [4] merupakan pendekatan yang digunakan untuk membangun system keamanan komputer yang lebih *advance* dari *Intrusion Detection* System, karena IPS ini dapat melakukan lebih dari „sekedar“ menganalisis *traffic / log* dan menghasilkan *alert.* IPS memberikan respon terhadap paket *intrusi* yang terdeteksi dan akan memblokir aktivitas yang berbahaya dalam jaringan.

Setiap hari ditemukan kerentanan dan *eksploitasi* baru [5]. Sehingga kerugihan akibat serangan *cyber* meningkat sangat pesat. Berdasarkan penelitian [6] yang dilakukan pada *University of Texas at Dallas*, didapatkan 100 versi bug *buffer overflow* (jenis serangan *user to root*) dari 63 proyek dunia nyata dengan total 28 Mloc berdasarkan laporan di *Common Vulnerabilities and Exposures* (CVE). *User to Root* [7] adalah suatu serangan dimana *user* normal secara illegal mendapatkan akses ke *root* atau *superuser* yang memiliki tujuan tertentu, Hal ini dapat terjadi dikarenakan suatu sistem tersebut masih terdapat celah berupa *bug* dari sistem yang masih dapat dieksploitasi.

Pada penelitian sebelumnya [8] membahas tentang cara mendeteksi serangan *buffer overflow* menggunakan *algoritma machine learning* yaitu *string matching* dan *Algoritma Aho – Corrasickv* yang berhasil mendeteksi dengan rata – rata akurasi 99%.Pada penelitian lainnya [9] dengan menambahkan metode *Support Vector Machine (SVM)* untuk melakukan deteksi dan mendapatkan tingkat akurasi yang baik.

Support Vector Machine merupakan metode dari data mining yang terbukti memiliki akurasi yang tinggi dalam mengklasifikasikan pola – pola paket data jaringan. Yang dibuktikan oleh beberapa penelitian menggunakan Dataset NSL-KDD adalah revisi dari KDD‟99. Dan data ini juga masih mengalami beberapa masalah yang dibahas oleh McHuh [10]. SVM juga dapat membedakan serta memisahkan antara data serangan dan data normal dengan cara pembagian antar *class.*

Pada penelitian ini akan membahas dan mengimplementasikan metode *Support Vector Machine* terhadap IPS untuk mendeteksi dan memblokir lalu lintas jaringan komputer yang terindikasi sebagai serangan *buffer overflow*

1.2 Rumusan Masalah

Berikut adalah rumusan masalah dalam penulisan Proposal Tugas Akhir ini:

1. Bagaimana cara pengamanan serangan dari *buffer overflow*?
2. Mendeteksi dan memblokir akses traffic buffer overflow
3. Menganalisis output yang dihasilkan dari penanganan serangan *buffer overflow* menggunakan *algoritma support vector machine*?
4. Bagaimana cara membandingkan hasil dari serangan *buffer overflow* yang didapatkan oleh Snort dan dengan yang didapatkan oleh *Support Vector Machine*

1.3 Tujuan Penelitian

Adapun tujuan dari penulisan Proposal Tugas Akhir ini adalah :

1. Mendeteksi serangan dari *buffer overflow.*
2. Mengklarifikasi dan menerapkan metode *Support Vector Mechine.*
3. Menganalisa keakurasian metode yang digunakan untuk mendeteksi dan mencegah serangan *buffer overflow*.
4. Memblokir akses buffer overflow pada jaringan komputer yang digunakan pada penelitian.

1.4 Manfaat Penelitian

Adapun manfaat dari penulisan Proposal Tugas Akhir ini adalah :

1. Dapat mengetahui mana paket normal dan paket serangan.
2. Dapat memberi kemudahan dalam mendeteksi serangan *buffer overfllow*.
3. Dapat memberikan keamanan pada server dari serangan *user to root* karena jika terdapat paket serangan maka sistem akan memblok.
4. Dapat mengetahui nilai akurasi dari serangan *buffer overflow* menggunakan metode (SVM)

1.5 Batasan Masalah

Adapun ruang lingkup dan perumusan masalah dalam penulisan Proposal Tugas Akhir ini adalah :

1. Menggunakan Dataset NSL-KDD adalah revisi dari KD”99
2. Mengklasifikasikan serangan *buffer overflow* menggunakan algoritma *Support Vector Machine.*
3. Mengklasifikasikan lalu lintas jaringan normal dan abnormal yang disebabkan oleh *buffer overflow*
4. Serangan yang dideteksi hanya serangan *buffer overflow*
5. Support Vector Machine hanya untuk memecahkan klasifikasi Deteksi saja
6. Memblokir atau mencegah akses *User To-Root (buffer overflow)* pada jaringan dan menyimpan pola lalu lintas yang telah di klasifikasi untuk digunakan di kemudian hari.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini yaitu melewati beberapa tahapan sebagai berikut :

1.6.1 Tahap Pertama yaitu (Studi Pustaka/Literatur) Pada Tahap pertama ini yaitu diawali dengan mencari informasi dan masalah yang sesuai danrelevan untuk diangkat sebagai penelitian. Lalu mencari beberapasumber seperti artikel, jurnal ilmiah, buku, internet dan lainnya yang mendukung dan berhubungan langsung dengan proposal tugas akhir ini serta mencari dataset yang terdapat di website – website, pada penelitian ini saya menggunakan Dataset NSL-KDD adalah revisi dari KDD‟99.

1.6.2 Tahap Kedua yaitu (Perancangan Sistem) Tahap kedua ini merupakan tahap yang membahas masalah proses bagaimana cara membangun metode atau pendekatan tertentu, perangkat lunak maupun perangkat keras yang digunakan untuk konfigurasi sistem beserta penerapan metode dan untuk melakukan penanganan terhadap serangan *buffe*

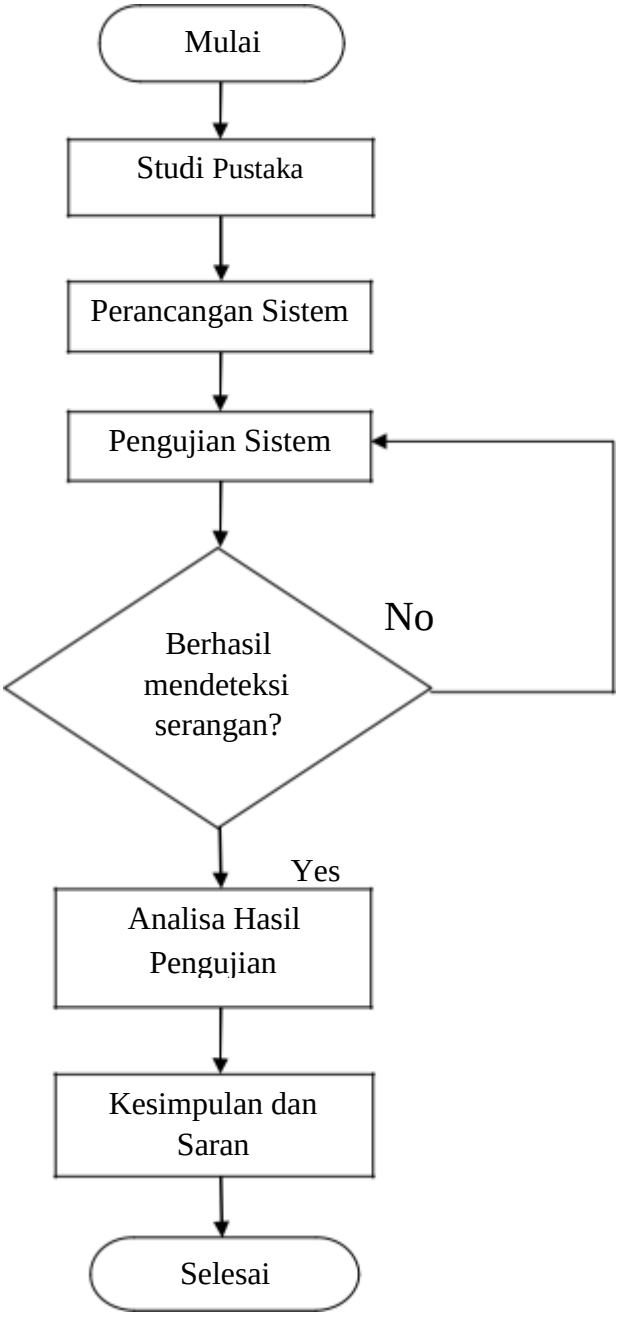
overflow menggunakan algoritma *Support Vector Machine* menggunakan bahasa pemrograman Python.

Tahap Ketiga yaitu (Pengujian) Pada tahap ketiga ini merupakan tahap lanjutan dari perancangan sebuah sistem dimana pada tahap ini melakukann pengujian berdasarkan metodologi penelitian dari penelitian sebelumnya sehingga didapatan hasil uji yang sesuai dan tepat secara konsep ataupun praktis.

Tahap Keempat yaitu (Analisa) Pada tahap keempat ini dilakukan pengolahan dan analisi sementara data yang diperoleh dari hasil pengujian berdasarkan pendekatan tertentu untuk mendapatkan data yang objektif, serta mengamati, mencatat dan menganalisa terdapat data yang diperoleh.

Tahap Kelima yaitu (Kesimpulan dan saran) Pada tahapan ini, akan dirumuskan suatu kesimpulan sementara yang diperoleh dari tahapan sebelumnya, serta untuk mengetahui kekurangan pada hasil perancangan dan factor penyebabnya.

Pada Gambar 1.1 ini menampilkan metodologi penelitian secara visual dalam bentuk diagram alir yang mempresentasikan proses pelaksanaan penelitian ini :



Gambar 1.1 Diagram Alir Metodologi Peneli

1.7 Sistematika Penulisan

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

BAB I. PENDAHULUAN

Pada bab ini merupakan isi dari penjelasan secara sistematis mengenai landasan topic penelitian yang meliputi latar belakang, tujuan, manfaat, rumusan masalah, dan batasan masalah kemudian metodologi penelitian serta sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada bab ini berisi tentang dasar teori dari *Intrusion Prevention System*, *Buffer Ovrflow*, algoritma *Support Vector Machine* dll, yang berhubungan dengan penelitian ini

BAB III. METODOLOGI PENELITIAN

Bab ini akan menjelaskan bagaimana proses penelitian ini, yang penjelasannya meliputi tahapan perancangan sistem design dan penerapan metode *Support Vector Machine* pada penelitian ini.

BAB IV. HASIL DAN ANALISA

Pada bab ini menjelaskan hasil dari pengujian yang dilakukan serta analisis dari setiap data yang diperoleh dari hasil pengujian menggunakan metode *Support Vector Machine*.

BAB V. KESIMPULAN

bab ini berisi kesimpulan dari bab yang telah dicantumkan dari penelitian yang dilakukan, bab ini juga akan berisi saran yang diharapkan dapat digunakan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] V. No and C. A. Winanto, "Deteksi Serangan Denial of Service Menggunakan Artificial Immune System," vol. 2 no. 1, pp. 456–459, 2016.

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

[3] R. Jamar, A. Sogani, S. Mudgal, Y. Bhadra, and P. Churi, "E-shield: Detection and prevention of website attacks," *RTEICT 2017 - 2nd IEEEInt. Conf. Recent Trends Electron. Inf. Commun. Technol. Proc.*, vol. pp.706–710, 2017.

[4] R. F. Pratama, N. A. Suwastika, and M. A. Nugroho, "Design and implementation adaptive Intrusion Prevention System (IPS) for attack prevention in software-defined network (SDN) architecture," *2018 6th Int.Conf. Inf. Commun. Technol. ICoICT 2018*, vol. no. c, pp. 299–304, 2018.

[5] A. Sawant, "A Comparative Study of Different Intrusion Prevention Systems," *Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom.ICCUBEA 2018*, vol. pp. 1–5, 2018.

[6] T. Ye, L. Zhang, L. Wang, and X. Li, "An Empirical Study on Detecting and Fixing Buffer Overflow Bugs," *Proc. - 2016 IEEE Int. Conf. Softw.Testing, Verif. Validation, ICST 2016*, vol. pp. 91–101, 2016.

[7] S. Revathi and A. Malathi, "Detecting User-To-Root (U2R) Attacks Based on Various Machine Learning Techniques," *Ijarcce.Com*, vol no. 4, pp. 6322–6324.

[8] A. Hidayat, "Deteksi serangan buffer overflow dengan metode string matching," vol., 2019.

[9] M. Edy Susanto, "Deteksi Serangan R2L dengan Metode Support VectorMachine," *J. Chem. Inf. Model.*, vol. 53 no. 9, pp. 1689–1699, 2019.

[10] I.Ahmad,M.Basheri,M.J.Iqbal,andA.Rahim, "PerformanceComparison of Support Vector Machine, Random Forest, and Extreme learning Machine for Intrusion Detection," *IEEE Access*, vol. no. c, pp. 33789–33795, 2018.

[11] S. Das and M. J. Nene, "A survey on types of machine learning techniques in intrusion prevention systems," *Proc. 2017 Int. Conf. Wirel. Commun.*

[12] M. A. Ajay Kumara and C. D. Jaidhar, "Hypervisor and virtual machine dependent Intrusion Detection and Prevention System for virtualized cloud environment," *2015 Int. Conf. Telemat. Futur. Gener. Networks, TAFGEN2015*, vol., pp. 28–33.

[13] Z. Jin, Y. Cui, and Z. Yan, "Survey of intrusion detection methods based on data mining algorithms," *ACM Int. Conf. Proceeding Ser.*, vol., no. 2, pp. 98–106, 2019.

[14] J. A. Goncalves, V. S. Faria, G. B. Vieira, C. A. M. Silva, and D. M. Mascarenhas, "WIDIP: Wireless distributed IPS for DDoS attacks," *20171st Cyber Secur. Netw. Conf. CSNet 2017*, vol. pp. 1–3, 2017.

[15] A. Alharbi, "Denial-of-Service , Probing , User to Root (U2R) & Remote to User (R2L) Attack Detection using Hidden Markov Models," vol. 07 no. 05, pp. 204–210, 2018.

[16] D. Kim and K. Y. Lee, "Detection of DDoS attack on the client side using support vector machine," *Int. J. Appl. Eng. Res.*, vol. no. 20, pp. 9909– 9913, 2017.

[17] P. M, V. V, F. Al-Turjman, M. Hamdi, and M. Maode, "Intrusion Prevention System for DDoS attack on VANET with reCAPTCHA Controller using Information based metrics," *IEEE Access*, vol. pp. 1–1, 2019.

[18] B. Xu *et al.*, "A Security Design for the Detecting of Buffer Overflow Attacks in IoT Device," *IEEE Access*, vol., no. c, pp. 72862–72869, 2018.

[19] M. N. Ali, M. M. Saudi, T. Bhuiyan, and A. A. Bakar, "Comparative study of traditional and next generation IPS," *Int. J. Eng. Technol.*, vol. no. 4, pp. 55–58.

[20] S. Kurnaz and I. A. Obaid, "Support Vector Machine (SVM) Based on Wavelet Transform (WT) for Intrusion Detection System (IDS)," vol. 8 , no. 2, pp. 13–19, 2019.

[21] J. Hu, “Network intrusion detection algorithm based on improved support vector machine,” *Proc. - 2015 Int. Conf. Intell. Transp. Big Data SmartCity, ICITBS 2015*, vol., pp. 523–526, 2016.

[22] P. G. Jeya, M. Ravichandran, and C. S. Ravichandran, “Efficient Classifier for R2L and U2R Attacks,” *Int. J. Comput. Appl.*, vol., no. 21, p. 29, 2012.

[23] O. Of, “An Overview of Buffer Overflow and Network Intrusion Detection and Prevention Systems,” vol., no. 2, 2019.

[24] B. Wang and L. Gu, “Detection of network intrusion threat based on the probabilistic neural network model,” *Inf. Technol. Control*, vol. no. 4, pp. 618–625, 2019.

[25] X. U. Xiaolong, G. A. O. Zhonghe, and H. A. N. Lijuan, “Intrusion Detection System Based on Integration of Artificial Neural Network and Support Vector Machine,” vol. 9, no. 2, pp. 39–43, 2016.

[26] T. A. Wibisono and F. Y. Al-Irsyadi, “Analisa pendeteksian dan pencegahan serangan buffer overflow terhadap achat,” vol. 2016.

[27] W. Bul‟ajoul, A. James, and S. Shaikh, “A New Architecture for Network Intrusion Detection and Prevention,” *IEEE Access*, vol, pp. 18558–18573, 2019.

[28] H. Kilic, N. S. Katal, and A. A. Selcuk, “Evasion Techniques Efficiency over the IPS/IDS Technology,” *UBMK 2019 - Proceedings, 4th Int. Conf.Comput. Sci. Eng.*, vol., pp. 542–547, 2019.

[29] N. Harale and B. B. Meshram, “Network Based Intrusion Detection and Prevention Systems : Attack Classification , Methodologies and Tools,” *Int.J. Eng. Sci.*, vol., no. 5, pp. 1–12, 2016.

[30] G. Mullen and L. Meany, “Assessment of buffer overflow based attacks on an IoT operating system,” *Glob. IoT Summit, GIoTS 2019 - Proc.*, vol., pp. 1–6, 2019.