SISTEM PENCEGAHAN SERANGAN *MALWARE REMOTE ACCESS TROJAN* (RATs) DENGAN METODE *SUPPORT VECTOR MACHINE* DI *SMALL BOARD COMPUTER*

OLEH:

DERI ANDANY
09011181621001

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

SISTEM PENCEGAHAN SERANGAN *MALWARE REMOTE ACCESS TROJAN* (RATs) DENGAN METODE *SUPPORT VECTOR MACHINE* DI *SMALL BOARD COMPUTER*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer (S1)

OLEH :

DERI ANDANY
09011181621001

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

SISTEM PENCEGAHAN SERANGAN *MALWARE*
***REMOTE ACCESS TROJAN* (RATs) DENGAN**
METODE *SUPPORT VECTOR MACHINE*
DI *SMALL BOARD COMPUTER*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh
DERI ANDANY
090111816210001

Inderalaya, Januari 2021

Pembimbing I Tugas Akhir

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

Pembimbing II Tugas Akhir

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

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis

Tanggal : 05 November 2020

Tim Penguji:

1. Ketua : Rendyansyah. S.Kom. M.T. :.....
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 : Rahmat Fadli Isnanto, S.Si., M.Sc. :.....

APPROVED

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Deri Andany

Nim : 09011181621001

Program Studi : Sistem Komputer

Judul skripsi : Sistem Pencegahan Serangan *Malware Remote Access Trojan* (RATs) dengan *Metode Support Vector Machine* di *Small Board Computer*

Hasil pengecekan software ithenticate / Turnitin : 13%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri bukan hasil penjiplakan / *plagiat.* Apabila di temukan unsur penjiplakan / *plagiat* dalam laporan ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

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

Indralaya, Januari 2021

ndany

NIM.09011181621001

HALAMAN PERSEMBAHAN

Dan sungguh akan Kami uji kamu dengan sedikit ketakutan, kelaparan, kekurangan harta, jiwa dan buah-buahan. Dan sampaikanlah kabar gembira kepada orang-orang yang bersabar (155), Yaitu orang-orang yang apabila ditimpa musibah, mereka mengucapkan: "Inna lillahi wa inna ilaihi raji'un (Sesungguhnya kami milik Allah, dan kepadanya kami akan kembali)" (156)." (Q.S Al-Baqarah: 155-156).

"Jangan banyak mengeluh, hidup memang tidak selalu indah"

Skripsi ini terutama saya persembahkan untuk :

1. Diri sendiri, terima kasih sudah menjadi sosok yang kuat dan tidak pernah menyerah dalam berjuang.
2. Orangtua tercinta, yang tidak pernah letih memberikan dukungan moral dan finansial.
3. Ayuk Intary Doamry, yang tidak pernah bosan memberikan dukungan finansial saat saya sedang terpuruk.
4. Kakak Andry Voku Badra yang selalu memberikan dukungan dan tempat berbagi cerita.
5. Dosen Pembimbing I: Pak Deris Stiawan, M.T., Ph.D yang selalu saya repotkan pada proses perjuangan yang amat Panjang ini. Terima kasih pak.
6. Dosen Pembimbing II: Kak Ahmad Heryanto, S.Kom., M.T selaku dosen pembimbing II dan juga kepala Lab Jaringan Komputr Inderalaya yang banyak memberikan support khususnya untuk perangkat yang saya butuhkan pada riset ini. Terima kasih, Terima kasih.
7. Semua rekan-rekan yang terlibat langsung maupun tidak langsung yang tidak dapat saya sebutkan satu per satu.

KATA PENGANTAR

Puji syukur atas kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan judul **"Sistem Pencegahan Serangan *Malware Remote Access Trojan* (RATs) dengan Metode *Support Vector Machine* di *Small Board Computer*"**.

Penulisan Proposal Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan proposal ini. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Proposal Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

- Orang Tua serta keluarga penulis tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama mengikuti dan melaksanakan perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya hingga dapat menyelesaikan Proposal Tugas Akhir ini.

- Bapak Deris Stiawan, M.T., Ph.D selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

- Bapak Ahmad Heryanto, M.T. selaku Dosen Pembimbing II Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

- Bapak Dr. Ir. Sukemi., M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
- Bapak Ir. Bambang Tutuko, M.T. selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
- My Venus yang selalu memberikan dukungan dan semangat saat mengerjakan tugas akhir.
- Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
- Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
- Almamater.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Proposal Tugas Akhir ini. Karena sesungguhnya tak ada yang sempurna didunia ini. Untuk itu, segala saran dan kritik sangatlah penting bagi penulis. Akhir kata, semoga Proposal Tugas Akhir ini dapat bermanfaat dan berguna bagi khalayak.

Indralaya, Januari 2021
Penulis

Deri Andany
NIM. 09011181621001

SISTEM PENCEGAHAN SERANGAN *MALWARE REMOTE ACCESS TROJAN* (RATs) DENGAN METODE *SUPPORT VECTOR MACHINE* DI *SMALL BOARD COMPUTER*

DERI ANDANY (09011181621001)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

E-mail : deriandhany@gmail.com

Abstrak

Remote Access Trojan (RATs) menjadi salah satu masalah yang serius yang perlu diselesaikan. RATs berjalan secara diam-diam pada latar belakang sehingga sulit dideteksi oleh pengguna. *Intrusion Detection and Prevention System* (IDPS) biasanya diterapkan untuk mengatasi hal ini. Telah banyak beredar perangkat NIDPS dari berbagai vendor, akan tetapi perangkat ini sulit dijangkau *Small Office and Home Office* (SOHO) karena memiliki nilai jual yang cukup *expensive*. Untuk mengatasi masalah tersebut, peneliti merancang IDPS *pada Small Board Computer* untuk meningkatkan efisiensi sumber daya. Untuk meningkatkan performa sistem yang akan dibangun, peneliti menambahkan algoritma *Support Vector Machine* untuk dilakukan *training data* yang diambil dari log IDPS. Hasil yang didapatkan dari proses *training* ini akan digunakan untuk update *rules* pada *engine* IDPS. Pengujian pada penelitian ini dilakukan secara *realtime* dalam menganalisa traffic jaringan. Traffic yang terindikasi serangan RATs akan langsung di drop dan sistem IDPS akan mengeluarkan *alert* yang ditulis pada *drop log*. Dari penelitian ini, metode SVM memiliki hasil yang baik dalam mendeteksi serangan RATs.

Kata Kunci: *Intrusion Prevention System, Intrusion Detection System, Small Board Computer, Support Vector Machine.*

INTRUSION PREVENTION SYSTEM FOR MALWARE REMOTE ACCESS TROJAN (RATs) ATTACK USING SUPPORT VECTOR MACHINE METHOD ON SMALL BOARD COMPUTER

DERI ANDANY (09011181621001)
Department of Computer Systems, Faculty of Computer Science, Sriwijaya University
E-mail : deriandhany@gmail.com

Abstract

Remote Access Trojans (RATs) are a serious problem that needs to be resolved. RATs run silently in the background making them difficult to detect by users. Intrusion Detection and Prevention System (IDPS) is usually applied to solved this. Many NIDPS devices have been distributed from various vendors, but these devices are difficult to reach Small Office and Home Office (SOHO) because they have quite expensive selling price. To solve this problem, researchers designed IDPS on a Small Board Computer to improve resource efficiency. To improve the performance of the system to be built, the researcher added the Support Vector Machine algorithm for training data taken from the IDPS log. The results obtained from this training process will be used to update rules on the IDPS engine. Testing in this study was carried out in real time analyzing network traffic. Traffic indicated that RATs attacks will be immediately dropped and the IDPS system will issue an alert written in the drop log. From this research, the SVM method has good results in detecting RATs attacks.

Keyword: *Intrusion Prevention System, Intrusion Detection System, Small Board Computer, Support Vector Machine.*

DAFTAR ISI

Daftar Gambar

Daftar Tabel

BAB I. PENDAHULUAN

1.1. Latar Belakang

Ada peningkatan besar dalam keamanan siber sejak beberapa dekade terakhir. Kerugian organisasi akibat serangan *cyber* ini telah meningkat pesat [1]. Setiap hari ditemukan kerentanan dan eksploitasi baru. Menurut [2] basis data *Common Vulnerabilities and Exposures* (CVE) pada 2018 sekitar 16.556 kerentanan dicatat dibandingkan dengan 2016 sekitar 6.447 kerentanan sistem diseluruh dunia.

Network Intrusion Detection System (NIDS) semakin menarik perhatian sebagai solusi untuk mengatasi ancaman keamanan pada internet [3]. *Intrusion Detection System* (IDS) adalah perangkat lunak yang otomatis melakukan deteksi intrusi pada jaringan yang di monitoring. Sementara *Intrusion Prevention System* (IPS) [4] adalah perangkat lunak yang memiliki kemampuan IDS dan juga yang menghentikan kemungkinan insiden.

Di era internet, *malware* (seperti *virus, trojan, ransomware*, dan *bot*) telah menjadi ancaman serius dan terus berevolusi bagi pengguna Internet. *Malware* telah digunakan oleh *hacker* sebagai senjata dalam mencapai tujuan mereka [5]. Malware menjadi ancaman yang sangat potensial untuk membuat keamanan komputer lebih rentan [6].

Remote Access Trojan (RATs) [7] adalah *malware* yang dirancang untuk mengontrol komputer target dengan tujuan tertentu. Peran utama *RATs* adalah untuk memberikan kontrol atas mesin korban, yang dapat dicapai dengan menyuntikkan dirinya ke dalam program yang sah untuk menyembunyikan kegiatan jahat mereka, mesin yang terinfeksi ini akan menjadi *botnet*.

Pada penelitian sebelumnya [8] membahas tentang cara mendeteksi RATs *Botnet* menggunakan empat algoritma *machine learning*, yaitu *Random Forest* (RF), *Naïve Bayes* (NB), *Naïve Bayes Tree* (NBTree), dan *k-Nearest Neighbor* (*Lazy Classifier*). Pada penelitian lain [7], ditambahkan algoritma *Support Vector Machine* (SVM) untuk melakukan deteksi, dan mendapatkan akurasi yang cukup baik. *Support Vector Machine* adalah algoritma *supervised learning* pada *machine learning* yang digunakan untuk analisa data klasifikasi dan regresi [4]. *Support Vector Machine* memisahkan dua kelas data dalam dataset menggunakan *hyperlane* [9].

Saat ini telah banyak beredar perangkat NIDPS dari berbagai vendor, akan tetapi perangkat ini masih memiliki harga jual dan biaya perawatan yang *expensive*, sehingga sulit untuk menjangkau *Small Office and Home Office* (SOHO). Dengan adanya *Small Board Computer* (SBC) memungkinkan individu untuk mendapatkan akses yang terjangkau, portabel, dan hemat daya [10].

Pada penelitian ini akan mengimplementasikan metode *Support Vector Machine* pada IPS untuk mendeteksi dan memblokir lalu lintas jaringan komputer yang terindikasi sebagai RATs yang akan di *embeded* ke *Small Board Computer* (SBC) *Banana Pi* R1. IPS dengan metode *Support Vector Machine* ini diharapkan akan dapat mewujudkan sistem yang lebih selektif dan responsif dalam menentukan mana yang merupakan *normal traffic* dan mana yang merupakan akses *malicious traffic*, dan mewujudkan system yang memiliki efisiensi sumber daya.

1.2. Rumusan Masalah

Rumusan masalah dalam penelitian ini yaitu sebagai berikut :

1. Bagaimana merancang IPS pada SBC Banana Pi.
2. Bagaimana melakukan *packet sniffing* pada jaringan dan mengolah data pcap yang akan dijadikan data *training* untuk model SVM.
3. Bagaimana mendeteksi dan memblokir akses *traffic Malware* RATs

4. Apakah IPS yang dirancang dapat mendeteksi dan memblokir paket berbahaya pada sistem secara *realtime*.

1.3. Batasan Masalah

Batasan masalah dalam penelitian ini yaitu sebagai berikut :

1. Algoritma SVM akan digunakan untuk menyelesaikan masalah klasifikasi data. Pada penelitian ini menggunakan dataset CTU120 Skenario 1 dari *Stratosphere IPS.*
2. Mengklasifikasikan lalu lintas internet normal dan abnormal yang disebabkan oleh RATs.
3. Memblokir akses *malware* RATs pada jaringan dan menyimpan pola lalu lintas RATs yang telah di klasifikasi untuk digunakan di kemudian hari.
4. Pada penelitian ini hanya RATs yang akan digunakan pada serangan.
5. Sistem akan berjalan secara realtime, namun hanya sampel trafik dalam kurun waktu tertentu yang akan dilakukan analisa.

1.4. Tujuan

Adapun tujuan yang hendak dicapai dari penelitian ini adalah :

1. Mengimplementasikan metode *Support Vector Machine* pada IPS yang di *embedded* pada SBC.
2. Mendeteksi *traffic malware* RATs pada jaringan komputer menggunakan *Rules Based Suricata* dan *Anomaly Based*.
3. Mengklarifikasi serangan RATs menggunakan Algoritma *Machine Learning Support Vector Machine*.
4. Memblokir akses *malware* RATs pada jaringan komputer yang digunakan pada penelitian.
5. Melakukan analisa akurasi metode yang digunakan untuk mendeteksi dan memblokir serangan RATs.

1.5. Manfaat

Adapun manfaat yang dapat diambil dari penelitian ini adalah :

1. Dapat digunakan sebagai alternatif metode keamanan pada suatu sistem ke depannya.
2. Dapat mengklasifikasikan *traffic* tidak biasa pada jaringan komputer yang disebabkan oleh aktivitas RATs.
3. Menghasilkan klasifikasi *traffic* normal dan tidak normal.
4. Memberikan informasi mengenai keakurasian metode *Support Vector Machine* pada pendeteksian RATs.

1.6. Metodologi Penelitian

Penelitian ini akan melewati beberapa tahapan :

1. Tahap Pertama (Studi Pustaka / Literatur)

   Tahap ini adalah proses mencari referensi dari beberapa sumber kajian ilmiah seperti paper, jurnal, dan buku yang berhubungan dengan penelitian yang akan dilakukan.
2. Tahap Kedua (Perancangan IPS menggunakan metode SVM)

   Pada tahap kedua, sistem akan di desain dan dirancang sedemikian rupa, seingga sistem (*software*) dapat digunakan untuk mengklasifikasi dan melakukan penanganan serangan RATs menggunakan algoritma *Support Vector Machine* menggunakan bahasa pemrograman python. Tahap ini dibagi menjadi dua skenario, yaitu skenario deteksi intrusi dan skenario prevensi intrusi.
3. Tahap Ketiga (Eksperimen)

   Pada tahap ini dilakukan pengujian serangan RATs pada node. Semua traffic akan diteruskan melalui server Banana Pi R1 dan akan diterapkan metode SVM untuk mendeteksi anomali pada traffic jaringan. Kemudian akan diamati bagaimana sistem IPS ini mendeteksi *intrusion* dalam jaringan, sehingga nantinya *traffic* yang tidak normal dan terindikasi sebagai *malicious traffic* akan di drop.

4. Tahap Keempat (Analisis sistem)

   Hasil dari pengujian pada tahap sebelumnya kemudian dianalisis, dengan tujuan untuk mengetahui performa dari system yang telah dibuat serta menganalisis apakah terdapat kekurangan pada hasil perancangan dan faktor penyebabnya sehingga dapat digunakan untuk pengembangan pada penelitian selanjutnya.

5. Tahap Kelima (Penarikan Kesimpulan dan Saran)

   Pada tahap ini akan ditarik kesimpulan dari hasil analisis pada tahap keempat dan saran yang mungkin berguna untuk penelitian selanjutnya.

1.7. Sistematika Penulisan

Sistematika penulisan dibuat untuk memperjelas dan mempertegas setiap bab yang akan dibuat pada penelitian ini. Adapun sistematika penulisan yang akan digunakan adalah sebagai berikut

BAB I. PENDAHULUAN

Pada bab I akan berisikan latar belakang masalah, tujuan dan manfaat serta metodologi penelitian dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada Bab II akan berisi dasar teori *Machine Learning*, Kelas *Malware*, *Remote Access Trojan*, *Botnet*, *Intrusion Detection System*, *Intrusion Prevention System*, *Suricata Engine*, *Feature Extraction*, *Feature Selection*, dan algoritma *Support Vector Machine* , *Banana Pi* R1 *Board*, *Bananian Linux*.

BAB III. METODOLOGI

Pada Bab III akan membahas analisis dan perancangan sistem klasifikasi dan penanganan serangan RATs menggunakan algoritma *Support Vector Machine* (SVM).

BAB IV. HASIL DAN ALANISIS

Pada Bab IV membahas tentang penerapan sistem yang di desain pada BAB III di *Banana Pi* R1 *Board*, dan membahas hasil pengklasifikasian dan penanganan serangan RATs menggunakan algoritma *Support Vector Machine*.

BAB V. KESIMPULAN DAN SARAN

Pada bab V berisi kesimpulan yang ditarik dari setiap bab yang telah dibuat, dan juga membahas mengenai hasil dari penerapan algoritma *Support Vector Machine* untuk penanganan serangan RATs. Pada bab ini juga akan berisi saran yang diharapkan dapat digunakan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] A. Sawant, "A Comparative Study of Different Intrusion Prevention Systems," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018, pp. 1–5, doi: 10.1109/ICCUBEA.2018.8697500.

[2] Cvedetails.com, "Browse cve vulnerabilities by date," 2019. https://www.cvedetails.com/browse-by-date.php (accessed Dec. 01, 2019).

[3] H. Jianhong, "Network Intrusion Detection Algorithm Based on Improved Support Vector Machine," in *2015 International Conference on Intelligent Transportation, Big Data and Smart City*, 2015, pp. 523–526, doi: 10.1109/ICITBS.2015.135.

[4] S. Das and M. J. Nene, "A survey on types of machine learning techniques in intrusion prevention systems," *Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017*, vol. 2018-Janua, pp. 2296–2299, 2018, doi: 10.1109/WiSPNET.2017.8300169.

[5] Y. Ye, L. Tao, A. Donald, and I. S. S, "A Survey on Malware Detection Using Data Mining Techniques," vol. 50, no. 3, 2017.

[6] D. Deka, N. Sarma, and N. J. Panicker, "Malware Detection Vectors and Analysis Techniques : A Brief Survey," 2016.

[7] A. A. Awad, S. G. Sayed, and S. A. Salem, "Collaborative Framework for Early Detection of RAT-Bots Attacks," *IEEE Access*, vol. 7, pp. 71780–71790, 2019, doi: 10.1109/ACCESS.2019.2919680.

[8] A. A. Awad and S. A. Salem, "A Network-based Framework for RAT-Bots Detection," pp. 128–133, 2017.

[9] C. Chio and D. Freeman, *Machine Learning and Security Protecting System with Data and Algorithm*, Firts Rele. California: O'Reilly Media, Inc, 2018.

[10] S. J. Matthews, R. W. Blaine, and A. F. Brantly, "Evaluating single board computer clusters for cyber operations," *2016 IEEE Int. Conf. Cyber Conflict, CyCon U.S. 2016*, vol. 2, no. February, 2017, doi: 10.1109/CYCONUS.2016.7836622.

[11] N. Vaidya and P. Godbole, "Hardware implementation of key functionalities of NIPS for high speed network," in *2015 International Conference on Computing and Network Communications (CoCoNet)*, 2015, pp. 892–897, doi: 10.1109/CoCoNet.2015.7411296.

[12] R. M. Yousufi, P. Lalwani, and M. B. Potdar, "A network-based intrusion

detection and prevention system with multi-mode counteractions," in *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 2017, pp. 1–6, doi: 10.1109/ICIIECS.2017.8276023.

[13] R. T. Gaddam and M. Nandhini, "An analysis of various snort based techniques to detect and prevent intrusions in networks: Proposal with code refactoring snort tool in Kali Linux environment," *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2017*, no. Icicct, pp. 10–15, 2017, doi: 10.1109/ICICCT.2017.7975177.

[14] D. Mudzingwa and R. Agrawal, "A study of methodologies used in intrusion detection and prevention systems (IDPS)," *Conf. Proc. - IEEE SOUTHEASTCON*, 2012, doi: 10.1109/SECon.2012.6197080.

[15] T. I. U. of B. Saad Hafeez B.Eng. and A, "Deep Packet Inspection using Snort," *Deep Pack. Insp. using Snort*, p. 24, 2017, [Online]. Available: http://on-demand.gputechconf.com/gtc/2017/presentation/s7468-wenji-wu-network-traffic-analysis-using-gpus.pdf.

[16] Banana-pi, "Banana Pi BPI-R1 - Banana Pi Wiki." http://wiki.banana-pi.org/Banana_Pi_BPI-R1 (accessed Dec. 15, 2019).

[17] Banana-pi, "BPI-R1 Specification." http://www.banana-pi.org/r1.html (accessed Dec. 15, 2019).

[18] D. D. Bhavani, A. Vasavi, and P. T. Keshava, "Machine Learning: A Critical Review of Classification Tehnique," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 3, no. 11, pp. 17–23, 2014, doi: 10.17148/ijarcce.

[19] Techterms, "Malware Definition." https://techterms.com/definition/malware (accessed Dec. 15, 2019).

[20] S. A. R. Shah and B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to Snort system," *Futur. Gener. Comput. Syst.*, vol. 80, pp. 157–170, 2018, doi: 10.1016/j.future.2017.10.016.

[21] M. C. Belavagi and B. Muniyal, "Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection," *Procedia Comput. Sci.*, vol. 89, pp. 117–123, 2016, doi: 10.1016/j.procs.2016.06.016.

[22] S. Pahwa and D. Sinwar, "Comparison Of Various Kernels Of Support Vector Machine," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. Volume 3 I, no. July, 2015.

[23] S. García, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," *Comput. Secur.*, vol. 45, pp. 100–123, 2014, doi: 10.1016/j.cose.2014.05.011.

[24] B. S. Raghuwanshi and S. Shukla, “SMOTE based class-specific extreme learning machine for imbalanced learning,” *Knowledge-Based Syst.*, vol. 187, p. 104814, 2020, doi: 10.1016/j.knosys.2019.06.022.

[25] W. P. Chawla, N. V. and Bowyer, K. W. and Hall, L. O. and Kegelmeyer, “SMOTE: Synthetic Minority Over-sampling Technique Nitesh,” *J. Artif. Intell. Res.*, vol. 16, no. 2, pp. 321–357, 2002, doi: 10.1613/jair.953.

[26] D. Jiang and K. Omote, “An approach to detect remote access trojan in the early stage of communication,” *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 2015-April, pp. 706–713, 2015, doi: 10.1109/AINA.2015.257.

[27] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, “Malware traffic classification using convolutional neural network for representation learning,” *Int. Conf. Inf. Netw.*, pp. 712–717, 2017, doi: 10.1109/ICOIN.2017.7899588.

[28] A. Bansal and S. Mahapatra, “A Comparative Analysis of Machine Learning Techniques for Botnet Detection,” *ACM Int. Conf. Proceeding Ser.*, pp. 91–100, 2017, doi: 10.1145/3136825.3136874.

[29] P. A. A. Resende and A. C. Drummond, “Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling,” *Secur. Priv.*, vol. 1, no. 4, p. e36, 2018, doi: 10.1002/spy2.36.

[30] E. Beckhauser, V. A. Petrolini, A. Savaris, J. M. Alves, and A. V. Von Wangenheim, “Are single-board computers an option for a low-cost multimodal telemedicine platform?: First tests in the context of Santa Catarina state integrated telemedicine and telehealth system,” *Proc. - IEEE Symp. Comput. Med. Syst.*, vol. 2016-Augus, pp. 163–168, 2016, doi: 10.1109/CBMS.2016.57.

[31] Fgrehl, “Homeserver – ESXi on HPE ProLiant MicroServer Gen10 | Virten.net.” https://www.virten.net/2017/11/homeserver-esxi-on-hpe-proliant-microserver-gen10/ (accessed Feb. 03, 2020).