VISUALISASI SERANGAN *MALWARE BOTNET* MENGGUNAKAN METODE *CLUSTERING K-MEANS*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer (S1)

OLEH:

NUZULA RAHMA SAFITRI

09011281722083

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

VISUALISASI SERANGAN *MALWARE BOTNET* MENGGUNAKAN METODE *CLUSTERING K-MEANS*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

NUZULA RAHMA SAFITRI

09011281722083

Indralaya, Juli 2021

Mengetahui,	
Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	: Nuzula Rahma Safitri
NIM	: 09011281722083
Judul	:Visualisasi Serangan Malware Botnet Menggunakan Metode Clustering K-Means

Hasil Pengecekan Software *iThenticate/Turnitin* : 3%

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

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksakan dari siapapun.

Indralaya, Juli 2021

Nuzula Rahma Safitri
NIM. 09011281722083

HALAMAN PERSETUJUAN

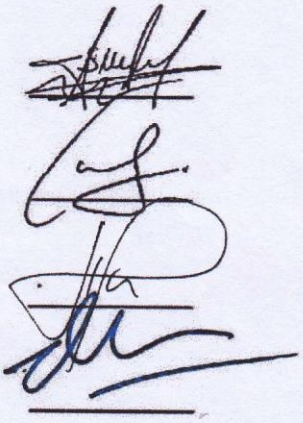
Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 15 Juli 2021

Tim Penguji :

1. **Ketua Sidang** : **Sarmayanta Sembiring, S.SI., M.T.**
2. **Sekretaris Sidang** : **Iman Saladin B.Azhar, M.MSI.**
3. **Penguji Sidang** : **Huda Ubaya, S.T., M.T.**
4. **Pembimbing** : **Deris Stiawan, M.T., Ph.D., IPU**



Mengetahui,

Ketua Jurusan Sistem Komputer

23/8/21

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

HALAMAN PERSEMBAHAN

Motto :

"Allah akan meninggikan orang-orang yang beriman di antaramu dan orang-orang yang diberi ilmu pengetahuan beberapa derajat"(surat al-mujadalah:11)

"orang yang pesimis selalu melihat kesulitan di setiap kesempatan, tapi orang yang optimis selalu melihat kesempatan dalam setiap kesulitan"(Ali bin Abi Thalib)

Dengan mengucapkan syukur alhamdulillah atas rahmat dari Allah swt, tugas akhir ini kupersembahkan untuk :

- Allah swt
- Kedua orang tua, Saudaraku dan keluarga besar.
- Sahabat serta teman – teman yang selalu membantu saat senang maupun susah.
- Rekan – rekan seperjuangan di sistem komputer 2017
- Jurusan Sistem Komputer
- Almamater Universitas Sriwijaya

KATA PENGANTAR

Segala puji bagi Allah SWT yang telah memberikan rahmat dan karuniaNya kepada penulis, sehingga penulis dapat menyelesaikan penyusunan proposal tugas akhir dengan judul "Visualisasi Serangan Malware Botnet Menggunakan Metode *Clustering K-Means*". Shalawat dan salam senantiasa tercurah kepada Rasulullah SAW yang mengantarkan manusia dari zaman kegelapan ke zaman yang terang benderang ini. Penyusunan proposal tugas akhir ini dimaksudkan untuk memenuhi sebagian syarat-syarat guna mencapai gelar Sarjana Sistem Komputer di Universitas Sriwijaya.

Dalam proposal ini penulis menjelaskan mengenai teknik visualisasi serangan malware botnet menggunakan algoritma *Clustering K-Means*. Penulis berharap tulisan ini dapat bermanfaat bagi orang banyak, dan menjadi tambahan bahan bacaan bagi yang tertarik meneliti tentang keamanan jaringan komputer.

Pada penyusunan laporan ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Tuhan Yang Maha Esa dan terimakasih kepada yang terhormat:

- Tuhan Yang Maha Esa, yang telah memberikan rahmat dan karunia-Nya sehingga pelaksanaan kerja praktek dan penulisan laporan kerja praktek ini dapat berjalan dengan lancar.
- Kedua orang tua beserta keluarga yang selalu mendoakan serta memberikan motivasi, dukungan, dan semangat.
- Bapak Jaidan Jauhari, S.Pd. M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
- Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Kompuer Fakutas Ilmu Komputer Universitas Sriwijaya.
- Bapak Deris Stiawan, Ph. D selaku Pembimbing Tugas Akhir Penulis.
- Bapak Dr. Ir. Sukemi, M.T selaku Pembimbing Akademik.

- Mbak Nurul Afifah, S.Kom, M.Kom yang telah membantu saya dalam menyelesaikan Tugas Akhir.
- Abdi Bimantara, S.Kom selaku teman yang telah membantu dalam pembuatan laporan tugas akhir.
- Taufik Qurahman, S.Kom selaku teman pergosipan.
- Taufik Hidayat terima kasih penyemangat ku dan bapak lily.
- Tia Hermita, Meutia Zamieyus, dan Ayu Melinda terima kasih atas bantuan selama perkuliahan ini.
- Lily karlina kucing kesayangan ku.
- Seluruh teman-teman Jurusan Sistem Komputer khusunya kelas A angkatan 2017 yang tidak dapat saya sebutkan satu persatu.
- Dan semua pihak yang telah membantu dalam pembuatan laporan tugas akhir ini.

Penulis menyadari bahwa Laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dikemudian hari. Akhir kata dengan segala keterbatasan, penulis berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran.

Indralaya, Juli 2021

Penulis

VISUALISASI SERANGAN *MALWARE BOTNET* MENGGUNAKAN METODE *CLUSTERING K-MEANS*

Nuzula Rahma Safitri (09011281722083)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : nuzularahma17@gmail.com

Abstrak

Visualisasi Serangan Malware bertujuan untuk mempermudah dalam mengenali jenis data malware dan normal. *Malware* atau perangkat lunak berbahaya adalah sebuah kode atau file program yang biasanya dikirimkan melalui jaringan internet, untuk mencuri, menginfeksi, atau melakukan beberapa sistem operasi bebahaya lainnya. Sedangkan *Botnet* adalah jaringan perangkat yang terinfeksi oleh perangkat lunak berbahaya dan dikendalikan oleh operator eksternal yang disebut *botmaster*. Tujuan dari penelitian ini adalah untuk mendapatkan tingkat akurasi terbaik dalam Visualisasi Serangan Malware Botnet menggunakan metode *Clustering K-Means* dengan menggunakan dataset yaitu *MedBIoT* project. Fitur ekstraksi pada penelitian ini menggunakan tools CICFlowMeters yang berasal dari *University Of New Brunswick* (UNB). Pada penelitian ini juga menggunakan *feature selection extra-tree classifier* yang bertujuan untuk memilih fitur terbaik. Hasil visualisasi menggunakan metode *Clustering K-Means* menunjukkan hasil cukup baik yaitu nilai akurasi sebesar 99,17% yang menandakan keakuratan dalam memvisualisasi serangan *malware botnet* pada penelitian ini.

Kata kunci : Visualisasi, *Malware Botnet, CICFlowMeter, Extra tree Classifier, Clustering K-Means*

Indralaya, Juli 2021

Mengetahui, 23/8/21

Ketua Jurusan Sistem Komputer	**Pembimbing**
Dr.Ir.H.Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP.196612032006041001	**NIP.197806172006041002**

VISUALIZATION OF BOTNET MALWARE ATTACKS USING K-MEANS CLUSTERING METHOD

Nuzula Rahma Safitri (09011281722083)

Department of Computer Engineering, Faculty of Computer Science,

Sriwijaya of University

Email : nuzularahma17@gmail.com

Abstrack

Malware Attack Visualization aims to make it easier to recognize the type of malware and normal data. Malware or malicious software is a code or program file that is usually sent over the internet, to steal, infect, or perform some other dangerous operating system. While the Botnet is a network of devices infected by malicious software and controlled by an external operator called a botmaster. The purpose of this study is to get the best level of accuracy in Botnet Malware Attack Visualization using clustering method K-Means by using dataset namely MedBIoT project. The extraction feature in this study uses CICFlowMeters tools from the University of New Brunswick (UNB). In this study also used feature selection extra-tree classifier that aims to choose the best feature. The visualization results using clustering method K-Means showed a fairly good result which is an accuracy value of 99.17% which indicates accuracy in visualizing botnet malware attacks in this study.

Keywords : Visualization, Malware Botnet, CICFlowMeter, Extra tree Classifier, Clustering K-Means.

Indralaya, July 2021

Head of Department Computer Engineering	**Supervisor**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Malware atau perangkat lunak berbahaya adalah sebuah kode atau file program yang biasanya dikirimkan melalui jaringan internet, untuk mencuri, menginfeksi, atau melakukan beberapa sistem operasi bebahaya lainnya. Yang ingin dilakukan penyerang merusak sistem yang ada dikomputer, mereka berkerja untuk mencapai tujuananya yaitu ingin memberikan kendali jarak jauh untuk menggunakan sistem yang terinfeksi, mengirim malware lain dari sistem yang terinfeksi ke sistem yang ditargetkan, kemudian menyelidiki jaringan lokal dari pengguna yang terinfeksi sistem untuk meluncurkan serangan *malware* lebih lanjut, dan untuk mencuri data sensitif seperti informasi kartu kredit dari sistem yang terinfeksi.[1]

Botnet telah menjadi ancaman yang signifikan bagi komputer dan jaringan komunikasi dalam dekade terakhir [2]. *Botnet* adalah jaringan perangkat yang terinfeksi oleh perangkat lunak berbahaya dan dikendalikan oleh operator eksternal yang disebut *botmaster*. Seringkali *malware* masuk ke jaringan secara diam-diam dari waktu ke waktu dengan cara mereplikasikan diri sebelum diinstruksikan oleh *botmaster* untuk memicu serangan. Tujuan dari *botnet* menyebabkan gangguan dan memimpin menyediakan layanan untuk kehilangan operasi. Jenis *botnet* sangatlah beragam yaitu seperti *bashlite, mirai, torii, okiru, kenjiro* dan lainnya. Penelitian mengenai *botnet* telah banyak dilakukan dalam beberapa tahun terakhir ini [3].

Dilihat dari penelitian sebelumnya[4], membahas bagaimana mengklasifikasikan *botnet* dengan 80 perangkat yang terkoneksi berdasarkan *Network Traffic*. Pada penelitian ini menggunakan dataset yang memiliki format *pcap*. Selanjutnya file tersebut di ekstraksi untuk kemudian akan dilakukan pengklasifikasian menggunakan tiga algoritma yaitu *k-Nearest Neighbors*, *Decision Tree* dan *Random Forest*. Dari penelitian yang telah dilakukan,

mendapatkan hasil yang cukup tinggi saat melakukan proses klasifikasi. Pada proses klasifikasi *Multi-Class* mendapatkan hasil akurasi sebesar 87,06% untuk *k-Nearest Neighbors*, 95,16% untuk *Decision Tree*, dan 97,66% untuk *Random Forest* [4]. Pada penelitian sebelumnya juga menyimpulkan bahwa pendekatan secara linear tidak cocok untuk data yang digunakan sehingga algoritma *SVM* tidak direkomendasikan untuk penelitian ini.

Selanjutnya pada penelitian ini juga membahas mengenai pendeteksian botnet berdasarkan *Network Traffic*. Selain itu penelitian ini mendekteksi dua jenis *botnet* yaitu *Mirai* dan *torii* tanpa menggunakan data yang berlebel. Data yang digunakan dalam pengklasifikasian berupa data *pcap* yang terlebih dahulu diekstraksi sebelumnya. Hasil yang didapatkan dalam mendeteksi serangan cukup bagus dibuktikan dengan nilai tingkat positif palsu yang rendah.

Pada penelitian [5], algoritma *Clustering K-Means* digunakan dalam botnet. Dataset yang digunakan pada penelitian tersebut berasal dari CTU-13. Hasil akurasi yang didapatkan pun cukup tinggi sebesar 90,65% untuk percobaan 1 dan 98,51% untuk percobaan 2.

Pada penelitian[6], membahasa tentang performa seleksi fitur untuk meningkatkan akurasi dari metode *Clustering K-Means* dan didapatkan hasil bahwa fitur seleksi terbaik untuk meningkatkan tingkat akurasi dari metode *Clustering K-Means* adalah feature *selection Extra-Tree*.

Dari beberapa ulasan diatas, penulis akan membahas mengenai visualisasi *botnet* menggunakan dataset berbentuk *pcap* yang terlebih dahulu diekstraksi sehingga menjadi *csv*. Selanjutnya hasil ekstraksi akan di visualisasi menggunakan algoritma *Clustering K-Means* [5].

1.2 Perumusan Masalah

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

1. Bagaimana cara mengelompokkan data *botnet* dan *normal* ?
2. Bagaimana cara memilih fitur terbaik pada data yang digunakan sehingga dapat mempercepat proses komputasi?

3. Bagaimana cara memvisualisasikan serangan *botnet* dalam bentuk grafik?

1.3 Batasan Masalah

Adapun batasan masalah pada tugas akhir ini, anatara lain:

1. Menggunakan dataset MedBIoT pada penelitian ini berasal dari *Talinn University of Technology.*
2. Algoritma yang digunakan dalam visualisasi *botnet* yaitu algoritma *Clustering K-means*.
3. *Feature selection* yang digunakan adalah *feature Extra-Tree.*
4. Dalam penelitian ini tidak membahas bagaimana cara pencegahan *botnet.*

1.4 Tujuan

Penelitian ini fokus pada serangan *Malware Botnet* menggunakan algoritma *clustering K-Means* untuk divisualisasikan. Adapun tujuan yang ingin dicapai dari penelitian tugas akhir ini antara lain adalah:

1. Menerapkan metode *clustering K-Means* pada penelitian ini.
2. Menerapkan *feature selection Extra-Tree* pada algoritma *clustering k-means.*
3. Memvisualisasikan dan mengelompokan data *botnet mirai*, *data botnet toriit* dan normal dalam bentuk grafik dengan metode *clustering k-means*.

1.5 Manfaat

Adapun manfaat dari penelitian tugas akhir ini yang dilakukan antara lain:

1. Dapat membedakan data *botnet* dan data *normal*.
2. *Feature selection Extra-Tree* mampu mempercepat dalam proses komputasi.
3. Memvisualisasikan data *botnet* dapat memberikan kemudahan dalam mengenali serangan *botnet* yang ada.

1.6 Metodelogi Penelitian

Pada metodologi yang digunakan pada penelitian ini akan melewati beberapa tahapan penelitian diantaranya :

1. Studi Pustaka/ Literatur

   Tahap ini dilakukan setelah masalah yang akan dibahas telah sesuai dan relevan untuk dijadikan sebagai penelitian, dengan membaca literature yang sesuai dengan topik penelitian dan mencari dataset yang akan digunakan.

2. Pengolahan Data

   Pada tahap ini membahas proses bagaimana mengolah suatu data mentah menjadi siap olah, memvisualisasikan data, serta menerapkan metode pada sistem tugas akhir.

3. Visualisasi

   Pada tahap ini dilakukan proses visualisasi data botnet dan data normal dengan menggunakan algortiman *K-Means*. Setelah proses visualisasi selesai, dilanjutkan pada proses validasi.

4. Analisa

   Setelah mendapatkan data dari tahap visualisasi, maka langkah selanjutnya adalah melakukan analisis terhadap hasil yang telah didapatkan sebelumnya sehingga didapatkan hasil yang *objektif.*

5. Kesimpulan dan Saran

   Tahap terakhir adalah membuat kesimpulan dari permasalahan, studi pustaka, metodelogi, dan analisa hasil visualisasi. Selain itu beberapa saran yang dapat dijadikan penelitian selanjutnya.

1.7 Sistematika Penulisan

Pada penyusunan tugas akhir ini dibuat sistematika penulisan untuk mempermudah dan memperjelas isi dari setiap bab sebagai berikut:

BAB I. PENDAHULUAN

Pada bab ini menjelaskan mengenai latar belakang, perumusan masalah, Batasan masalah, tujuan dan manfaat dari topik yang diangkat dari sistem visualisasi *botnet* menggunakan algoritma *K-Means*.

BAB II. TINJAUAN PUSTAKA

Bab ini berisikan mengenai beberapa *literature review* yang berhubungan dengan masalah visualisasi *botnet* dengan menggunakan algoritma *K-Means* yang mengacu pada penelitian sebelumnya.

BAB III. METODOLOGI PENELITIAN

Pada bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan mengenai bab ini meliputi tahapan-tahapan yang akan dilakukan serta mempersiapkan data *botnet* dan normal, penerapan algoritma *K-Means* serta model yang akan digunakan sehingga tujuan dari penulis tercapai.

BAB IV. ANALISA DAN PEMBAHASAN

Pada bab ini menjelaskan hasil yang telah diperoleh pada tahap sebelumnya, serta analisa data yang didapat dari hasil pengujian.

BAB V. KESIMPULAN

Bab ini berisikan kesimpulan tentang hasil pengujian yang telah dilakukan, serta merupakan jawaban yang diperoleh dari tujuan yang ingin dicapai, dan berisikan saran-saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019, doi: 10.1109/ACCESS.2019.2960412.

[2] M. J. Farooq and Q. Zhu, "Modeling, Analysis, and Mitigation of Dynamic Botnet Formation in Wireless IoT Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 9, pp. 2412–2426, 2019, doi: 10.1109/TIFS.2019.2898817.

[3] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," *Proc. Int. Jt. Conf. Neural Networks*, vol. 20, no. 8489489, pp. 8–13, 2018, doi: 10.1109/IJCNN.2018.8489489.

[4] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, and S. Nõmm, "MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network," *ICISSP 2020 - Proc. 6th Int. Conf. Inf. Syst. Secur. Priv.*, no. 72, pp. 207–218, 2020, doi: 10.5220/0009187802070218.

[5] W. N. H. Ibrahim, A. Selamat, S. Anuar, and O. Krejcar, "Clustering botnet behavior using K-means with uncertain data," *Front. Artif. Intell. Appl.*, vol. 318, no. 943, pp. 244–257, 2019, doi: 10.3233/FAIA190053.

[6] V. S. Akondi, V. Menon, J. Baudry, and J. Whittle, "Novel K-Means Clustering-based Undersampling and Feature Selection for Drug Discovery Applications," *Proc. - 2019 IEEE Int. Conf. Bioinforma. Biomed. BIBM 2019*, no. 63, pp. 2771–2778, 2019, doi: 10.1109/BIBM47256.2019.8983213.

[7] A. Naway and Y. Li, "Android malware detection using autoencoder," *IEEE Trans. Inf. Forensics Secur.*, vol. 53, no. 6, *arXiv*, pp. 1–9, 2019, doi: 10.1109/TIFS.2019.2898817.,

[8] H. Alzahrani, M. Abulkhair, and E. Alkayal, "A multi-class neural network model for rapid detection of IoT botnet attacks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 7, pp. 688–696, 2020, doi: 10.14569/IJACSA.2020.0110783.

[9] Y. Meidan *et al.*, "N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, 2018, doi: 10.1109/MPRV.2018.03367731.

[10] M. Antonakakis *et al.*, "Understanding the Mirai Botnet This paper is included in the Proceedings of the Understanding the Mirai Botnet," *USENIX Secur.*, vol. 22, no. 34, pp. 1093–1110, 2017.

[11] A. Marzano *et al.*, "The Evolution of Bashlite and Mirai IoT Botnets," *Proc. - IEEE Symp. Comput. Commun.*, vol. 11, no. 75 pp. 813–818, 2018, doi: 10.1109/ISCC.2018.8538636.

[12] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, 2020, doi: 10.1007/s11235-019-00599-z.

[13] J. Alberto and M. Galindo, "Generation of Malware Behavioral Datasets in a Medium Scale Iot Networks." *IEEE Trans. Inf. Forensics Secur.*, vol. 17, no. 5, pp. 2412–2426, 2018, doi: 10.1109/TIFS.2019.2898817.

[14] M. Austin, "IoT Malicious Traffic Classification Using Machine Learning IoT Malicious Traffic Classification Using Machine Learning," " *IEEE Trans. Inf. Forensics Secur.*, vol. 88, no. 2, pp. 2412–2426, 2020, doi: 10.1109/TIFS.2019.2898817.

[15] A. H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of tor traffic using time based features," *ICISSP 2017 - Proc. 3rd Int. Conf. Inf. Syst. Secur. Priv.*, vol. 20, no. 33, pp. 253–262, 2017, doi: 10.5220/0006105602530262.

[16] H. T. Nguyen, D. H. Nguyen, Q. D. Ngo, V. H. Tran, and V. H. Le, "Towards a rooted subgraph classifier for IoT botnet detection," *ACM Int. Conf. Proceeding vol. 7, no. 11, Ser.*, pp. 247–251, 2019, doi: 10.1145/3348445.3348474.

[17] X. Liu, J. Tang, and S. Member, "Mass Classification in Mammograms Using.pdf," *IEEE Syst. J.*, vol. 8, no. 3, pp. 910–920, 2014.

[18] S. Visalakshi and V. Radha, "A literature review of feature selection techniques and applications: Review of feature selection in data mining," *2014 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2014*, no. 19, 2014, doi: 10.1109/ICCIC.2014.7238499.

[19] J. Sharma, "Multi-layer intrusion detection system with ExtraTrees feature selection , extreme learning machine ensemble , and softmax aggregation," " *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 2412–2426, 2019, doi: 10.1109/TIFS.2019.2898817.

[20] 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*, pp. 177–182, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905286.

[21] A. A. Obeidat, "Hybrid approach for botnet detection using k-means and k-medoids with Hopfield neural network," *Int. J. Commun. Networks Inf. Secur.*, vol. 9, no. 3, pp. 305–313, 2017.

[22] R. Vinayakumar, M. Alazab, S. Srinivasan, Q. V. Pham, S. K. Padannayil, and K. Simran, "A

Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4436–4456, 2020, doi: 10.1109/TIA.2020.2971952.

[23] M. Aly and malaa caltech Edu, "Survey on multiclass classification methods," *Neural Netw*, no. 20, vol. 4, November, pp. 1–9, 2005.

[24] T. C. W. Landgrebe and R. P. W. Duin, "Efficient multiclass ROC approximation by decomposition via confusion matrix perturbation analysis," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, no. 5, pp. 810–822, 2008, doi: 10.1109/TPAMI.2007.70740.

[25] M. K. Uçar, M. Nour, H. Sindi, and K. Polat, "The Effect of Training and Testing Process on Machine Learning in Biomedical Datasets," *Math. Probl. Eng.*, vol. 22, 2020, doi: 10.1155/2020/2836236.

[26] G. V. B. M. Patil, "Query Dependant Single Document Summarization using Partitional Clustering: K-Means Clustering Approach," *Int. J. Comput. Sci. Eng. Technolo*, vol. 1, no. 5, p. 191, 2011.