VISUALISASI SERANGAN *UDP FLOOD* PADA LAYANAN *INTERNET OF THINGS* (IOT) MENGGUNAKAN METODE *K-MEANS CLUSTERING*

TUGAS AKHIR

DISUSUN OLEH :

MUHAMMAD RIFQI ABIYYU ARIQ

09011381823114

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

HALAMAN PENGESAHAN

VISUALISASI SERANGAN *UDP FLOOD* PADA LAYANAN *INTERNET OF THING* (IOT) MENGGUNAKAN METODE *K-MEANS CLUSTERING*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
Jenjang S-1

Oleh :

MUHAMMAD RIFQI ABIYYU ARIQ
09011381823114

Palembang, 10 Januari 2023

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 PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu

Tanggal : 28 Desember 2022

Tim Penguji :

1. **Ketua** : **Sarmayanta Sembiring, M.T.**
2. **Sekretaris** : **Adi Hermansyah, M.T.**
3. **Pembimbing** : **Deris Stiawan, M.T., Ph.D.**
4. **Penguji** : **Huda Ubaya, M.T.**

Mengetahui, 5/1/23

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Muhammad Rifqi Abiyyu Ariq
NIM : 09011381823114
Judul : Visualisasi Serangan *UDP Flood* Pada Layanan *Internet of Things* (IoT) Menggunakan Metode *K-Means Clustering*

Hasil Pengecekan Software iThenticate/Turnitin : 6%

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

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

Palembang, Januari 2023

Muhammad Rifqi Abiyyu Ariq
NIM. 09011381823114

HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan kepada Allah SWT yang karena karunia-nya memberikan saya kesempatan dalam menikmati keindahan dunia ini. Kepada orang orang terdekat yang senantiasa memberikan bantuan, serta Ayahanda & Ibunda saya yang tercinta, juga Adik saya tersayang.

Dengan mengucapkan Alhamdullilah sebagai rasa syukur saya terhadap rahmat yang telah diberikan Allah SWT serta ridho-nya saya sebagai penulis dapat memenuhi harapan dari keluarga besar dengan menyelesaikan program studi di FASILKOM UNSRI untuk mendapatkan gelar sarjana komputer.

"Keterlambatan bukan lah sebuah kegagalan, namun sebuah keberhasilan yang tertunda"

~Desember 2022~

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur atas kehadirat Allah SWT yang telah memberikan rahmat dan karunianya sehingga penulis dapat menyelesaikan laporan Tugas Akhir yang berjudul "**Visualisasi Serangan *UDP Flood* Pada Layanan *Internet of Things* (IoT) Menggunakan Metode *K-Means Clustering***"

Dalam laporan ini penulis akan memvisualisasikan pola serangan DDoS pada jaringan IoT yang telah diperoleh penulis selama penelitian dan pengujian. Selain itu, penulis meyakini bahwa dengan adanya laporan tersebut maka akan sangat bermanfaat kepada khalayak umum yang ingin membaca dan tertarik untuk meneruskan penelitian tentang serangan DDoS pada jaringan IoT tersebut.

Sebelumnya, penulis ingin mengucapkan terima kasih kepada beberapa pihak yang telah memberikan motivasi, ide, maupun saran kepada penulis dalam penyusunan laporan Tugas Akhir ini. Untuk itu penulis ingin mengucapkan banyak terima kasih kepada:

1. Allah SWT yang telah memberikan rahmat serta karunia-Nya sehingga penulis dapat menyelesaikan Proposal Tugas Akhir ini dengan baik.
2. Orang tua saya tercinta dan adik saya tersayang, yang senantiasa memberikan motivasi dan mendukung saya hingga seperti sekarang ini.
3. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Huda Ubaya, S.T., M.T. selaku Dosen Pembimbing Akademik.

5. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran serta motivasi untuk penulis dalam penyusunan Tugas Akhir ini.

6. Dan semua pihak yang telah membantu yang penulis tidak bisa sebutkan satu persatu.

Penulis sadar bahwa laporan yang disusun masih sangat jauh dari kata sempurna. Untuk itu penulis meminta kritik dan saran yang membangun sehingga agar penyusunan akan menjadi lebih baik untuk kedepannya serta menjadi daya tarik penelitian itu sendiri.

Palembang,..……

Penulis,

Muhammad Rifqi Abiyyu Ariq
NIM. 09011381823114

VISUALIZATION OF UDP FLOOD ATTACKS ON INTERNET OF THINGS (IOT) SERVICES USING K-MEANS CLUSTERING METHOD

MUHAMMAD RIFQI ABIYYU ARIQ (09011381823114)

Department of Computer Systems, Faculty of Computer Science, Universitas Sriwijaya

Email : muhammadrifqiabiyyuariq@gmail.com

ABSTRACT

The Internet of Things (IoT) is a system for accumulating and transferring data on a physical device that is interconnected to the internet network in order to communicate with each other between devices with any destination the user wants, so that the system will not infrequently escaped from the threat of cyber attacks such as Denial of Service (DoS) UDP floods that could reduce the performance of IoT devices. This type of attack technique can paralyze systems on IoT devices that are continuous even if the attack has been stopped. This research will visualize UDP Denial of Service (DoS) attacks using the K-Means method. In this study, the most optimal cluster was two clusters based on the results of the elbow and silhouette coefficient techniques with a score of 90.7%. The visualization results between the two clusters shows that cluster 1 has more dominant attack traffic than cluster 2.

Keyword: *Internet of Things (IoT), Denial of Service (DoS), UDP Flooding, K-Means*

VISUALISASI SERANGAN *UDP FLOOD* PADA LAYANAN *INTERNET OF THINGS* (IOT) MENGGUNAKAN METODE *K-MEANS CLUSTERING*

MUHAMMAD RIFQI ABIYYU ARIQ (09011381823114)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : muhammadrifqiabiyyuariq@gmail.com

ABSTRAK

Internet of Things (IoT) adalah sistem untuk mengumpulkan serta mentransfer data pada sebuah perangkat fisik yang saling terhubung ke dalam jaringan *internet* agar dapat saling berkomunikasi antar perangkat dengan tujuan apapun yang di inginkan pengguna, sehingga sistem tersebut tidak jarang luput dari ancaman serangan siber seperti *Denial of Service* (DoS) UDP *flood* yang dapat menurunkan kinerja perangkat IoT. Serangan ini merupakan teknik serangan yang dapat melumpuhkan sistem pada perangkat IoT yang sifatnya berkelanjutan sekalipun serangan telah dihentikan. Penelitian ini akan melakukan visualisasi pada serangan *Denial of Service* (DoS) UDP *flood* menggunakan metode *K-Means*. Pada penelitian ini *cluster* yang paling optimal sebanyak dua *cluster* berdasarkan hasil dari teknik *elbow* dan *silhouette coefficient* dengan *silhouette score*-nya sebesar 90.7%. Kemudian hasil visualisasi antara kedua *cluster* menunjukkan bahwa *cluster 1* memiliki *traffic* serangan yang lebih dominan dibandingkan *cluster 2*.

Kata Kunci : *Internet of Things* (IoT), *Denial of Service* (DoS), *UDP Flooding*, *K-Means*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Seiring pesatnya perkembangan teknologi di era industri saat ini, *Internet of Things* (IoT) telah menjadi salah satu konsep yang berperan penting dalam memajukan masa depan. IoT sendiri merupakan sistem yang sedang dikembangkan untuk dapat mengumpulkan serta mentransfer data tanpa adanya campur tangan manusia karena sistem tersebut terhubung ke sensor, perangkat lunak, dan sistem kendali [1]. Menurut [2] IoT merupakan perangkat fisik yang saling terhubung kedalam jaringan *internet* agar dapat saling berkomunikasi antar perangkat dengan tujuan apapun yang di inginkan pengguna, sehingga sistem IoT ini tidak luput dari ancaman penyerangan seperti *Denial of Service* (DoS) yang dapat menurunkan kinerja pada perangkat IoT tersebut.

Serangan DoS pada IoT akan menyerang sumber data serta platform IoT yang berperan sebagai *server*, ketika *server* menerima permintaan diluar *host* secara terus menerus akan membuat *server* sibuk sehingga komunikasi antar perangkat menjadi terhambat oleh serangan. Tidak hanya memperlambat komunikasi antar perangkat, DoS juga akan mengkonsumsi penyimpanan dan sumber daya *platform* IoT yang dapat menyebabkan kerusakan berkelanjutan [3]. Contoh serangan DoS adalah *User Datagram Protocol* (UDP) *Flood*, dimana UDP *Flood* akan membanjiri *port* dengan *packet* UDP dengan jumlah yang besar melalui IP *spoofing* sebagai alamat sumber, sehingga memberhentikan komunikasi *host* ke perangkat IoT yang mengakibatkan sistem menjadi crash. Ini dikarenakan protokol jaringan UDP bersifat *sessionless* dalam artiannya protokol UDP hanya dapat mentransmisikan data tanpa melakukan memeriksa kesalahan terlebih dahulu ketika mengirimkan data [4][5].

Pada penelitian [6], membahas tentang visualisasi serangan DoS dengan menggunakan metode *K-Means Algorithm*. Pada penelitian tersebut *K-Means* digunakan untuk membagi *cluster* dari nilai k terbaik dan menentukan titik *centroid* dari *cluster* tersebut. Kemudian *cluster* tersebut akan di visualisasikan

dengan menggunakan *Parallel Coordinate Attack Visualization* (PCAV). Penelitian tersebut menghasilkan akurasi *clustering* sebesar 97,83%, akurasi pendeteksian sebesar 98,63%, dan *false alarm* sebesar 0,2%. Lalu penelitian berikut [7][8], menjelaskan tentang dataset *UDP Flood Attack Pattern on Internet of Things Network* yang dibuat oleh *Communication Network and Information Security* (COMNETS) Universitas Sriwijaya, juga memperkenalkan pola serangan UDP *Flooding* yang terjadi pada dataset tersebut.

Berdasarkan referensi dari penelitian-penelitian sebelumnya, maka penulis mengusulkan pada penelitian tugas akhir ini akan melakukan visualisasi serangan UDP *Flooding* pada layanan *Internet of Things* (IoT) dengan menggunakan metode *K-Means Algorithm*. Penelitian ini akan menggunakan dataset *UDP Flood Attack Pattern on Internet of Things Network* dari Lab COMNETS Universitas Sriwijaya.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan diatas, rumusan masalah pada penelitian ini mengacu kepada pembagian *cluster* serta menentukan titik *centroid* dengan menggunakan algoritma *K-Means Clustering*. Lalu, menampilkannya dalam bentuk visual antar *cluster* tersebut menggunakan algoritma *Parallel Coordinates*.

1.3. Batasan Masalah

Dari rumusan masalah dan latar belakang di atas, berikut batasan masalah pada tugas akhir ini, antara lain:

1. Penelitian hanya berfokus pada serangan UDP *flooding Denial of Service* (DoS) pada layanan *Internet of Things* (IoT).
2. Hanya melakukan visualisasi serangan UDP *flooding* pada IoT, tanpa melakukan pencegahannya.
3. Visualisasi menggunakan algoritma *Parallel Coordinate Attack Visualization* (PCAV) dan algoritma *K-Means* digunakan untuk membagi *cluster* serta menentukan titik *centroid*.

1.4. Tujuan

Adapun tujuan dari penulisan tugas akhir, yaitu:

1. Mampu mengenali pola serangan UDP *flood Denial of Service* (DoS) pada layanan *Internet of Things* (IoT).
2. Mampu membagi *cluster* dan menentukan titik *centroid* menggunakan algoritma *K-Means Clustering.*
3. Mampu memvisualisasikan *traffic* serangan DoS UDP *flood* ke dalam bentuk grafik.

1.5. Manfaat

Adapun manfaat yang didapatkan dari penulisan tugas akhir ini, yaitu:

1. Dapat mempelajari pola serangan UDP *flood Denial of Service* (DoS) pada layanan *Internet of Things* (IoT).
2. Dapat menjadi referensi bagi peneliti kedepannya untuk melakukan pencegahan serangan UDP *flood* DoS pada layanan IoT.
3. Mampu mengolah data serta melakukan visualisasi terhadap data serangan UDP *flood* DoS pada layanan IoT tersebut.

1.6. Metodologi Penelitian

Adapun pada laporan penelitian tugas akhir ini menggunakan metodologi penelitian sebagai berikut:

1. Metode Studi Pustaka dan Literatur

   Metode dilakukan dengan mengumpulkan beberapa referensi literatur ilmiah yang bisa ditemukan melalui buku maupun jurnal serta melakukan validasi menggunakan *snort* terhadap dataset yang akan digunakan.

2. Metode Pengolahan Data

   Metode dilakukan dengan mengekstraksi fitur data PCAP ke dalam bentuk file CSV serta melakukan beberapa penyesuaian dengan menentukan fitur seleksi yang akan digunakan sebagai *attack pattern*.

3. Metode Visualisasi

   Metode dilakukan dengan membagi *cluster* k terbaik pada data tersebut, lalu menentukan titik *centroid* pada *n_cluster* yang telah ditentukan melalui teknik *elbow* dan *silhouette coefficient*. Setelah itu, dapat melakukan visualisasi dengan menggunakan metode *parallel coordinates* berbasis data *cluster*.

4. Metode Analisa dan Kesimpulan

   Metode dilakukan dengan menganalisa hasil yang telah didapat sebelumnya lalu menarik kesimpulan dari permasalahan, studi pustaka, metodologi, dan analisis hasil visualisasi.

1.7. Sistematika Penulisan

Adapun sistematika penulisan dalam penulisan tugas akhir ini, sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan topik yang akan diusung pada penelitian tugas akhir ini. Penjelasan tersebut meliputi latar belakang, batasan & rumusan masalah, tujuan & manfaat, dan sistematika penulisan tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan tentang *literature review* beberapa jurnal yang menjadi referensi penulisan tugas akhir dan teori-teori dasar yang berkaitan dengan topik penelitian tugas akhir ini. Bab ini akan menjadi landasan pada penelitian tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan tahapan tahapan selama proses penelitian berlangsung yang dirangkum ke dalam diagram alir. Pada bab ini juga membahas mengenai dataset serta spesifikasi perangkat keras maupun perangkat lunak yang digunakan selama penelitian tugas akhir ini.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas hasil pengujian dataset yang digunakan pada penelitian tugas akhir. Hasil pengujian tersebut disajikan kedalam bentuk visual grafik dengan menggunakan metode *parallel coordinates*.

BAB V KESIMPULAN DAN SARAN

Bab ini akan menarik kesimpulan pada hasil akhir yang didapatkan dari pengujian *dataset* selama penelitian tugas akhir berlangsung serta memberikan saran yang kemungkinan dapat membantu penelitian kedepannya.

DAFTAR PUSTAKA

[1] N. Mishra and S. Pandya, “Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review,” *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[2] D. Stiawan *et al.*, “Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network,” *IEEE Access*, vol. 9, pp. 116475–116484, 2021, doi: 10.1109/ACCESS.2021.3105517.

[3] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, “REATO: REActing TO Denial of Service attacks in the Internet of Things,” *Comput. Networks*, vol. 137, pp. 37–48, 2018, doi: 10.1016/j.comnet.2018.03.020.

[4] A. A. Acharya, K. M. Arpitha, and B. J. Santhosh Kumar, “An intrusion detection system against UDP flood attack and ping of death attack (DDOS) in MANET,” *Int. J. Eng. Technol.*, vol. 8, no. 2, pp. 1112–1115, 2016.

[5] A. Singh and D. Juneja, “Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks,” *Int. J. Eng. Sci. Technol.*, vol. 2, no. 8, pp. 3405–3411, 2010.

[6] N. A. Putri, D. Stiawan, A. Heryanto, T. W. Septian, L. Siregar, and R. Budiarto, “Denial of service attack visualization with clustering using K-means algorithm,” *ICECOS 2017 - Proceeding 2017 Int. Conf. Electr. Eng. Comput. Sci. Sustain. Cult. Herit. Towar. Smart Environ. Better Futur.*, pp. 177–183, 2017, doi: 10.1109/ICECOS.2017.8167129.

[7] R. Andika, “Pengenalan pola serangan denial of service (udp flood) pada jaringan internet of things (iot) dengan algoritma decision tree c4.5,” 2018.

[8] D. Stiawan *et al.*, “UDP Flood Attack Pattern on Internet of Things Network Dataset,” Dec. 2018, doi: 10.5281/ZENODO.4436127.

[9] S. S. De, M. Mishra, and S. Dehuri, “MVClustViz,” *Int. J. Syst. Dyn. Appl.*, vol. 2, no. 4, pp. 19–32, 2013, doi: 10.4018/ijsda.2013100102.

[10] H. Choi and H. Lee, “PCAV: Internet attack visualization on parallel coordinates,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif.*

Intell. Lect. Notes Bioinformatics), vol. 3783 LNCS, pp. 454–466, 2005, doi: 10.1007/11602897_38.

[11] K. P. Sinaga and M. S. Yang, "Unsupervised K-means clustering algorithm," *IEEE Access*, vol. 8, pp. 80716–80727, 2020, doi: 10.1109/ACCESS.2020.2988796.

[12] M. I. W. Pramana, Y. Purwanto, and F. Y. Suratman, "DDoS detection using modified K-means clustering with chain initialization over landmark window," *ICCEREC 2015 - Int. Conf. Control. Electron. Renew. Energy Commun.*, pp. 7–11, 2015, doi: 10.1109/ICCEREC.2015.7337056.

[13] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," *Int. Conf. Wirel. Mob. Comput. Netw. Commun.*, pp. 600–607, 2013, doi: 10.1109/WiMOB.2013.6673419.

[14] E. Umargono, J. E. Suseno, and V. G. S. K., "K-Means Clustering Optimization using the Elbow Method and Early Centroid Determination Based-on Mean and Median," vol. 474, no. Isstec 2019, pp. 234–240, 2020, doi: 10.5220/0009908402340240.

[15] K. R. Shahapure and C. Nicholas, "Cluster quality analysis using silhouette score," *Proc. - 2020 IEEE 7th Int. Conf. Data Sci. Adv. Anal. DSAA 2020*, pp. 747–748, 2020, doi: 10.1109/DSAA49011.2020.00096.

[16] M. S. Yang and K. P. Sinaga, "A feature-reduction multi-view k-means clustering algorithm," *IEEE Access*, vol. 7, pp. 114472–114486, 2019, doi: 10.1109/ACCESS.2019.2934179.

[17] B. S. Kumar, T. C. S. P. Raju, M.Ratnakar, S. D. Baba, and N.Sudhakar, "Intrusion Detection System- Types and Prevention," *Int. J. Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 77–82, 2013.

[18] M. K. Pakhira, "A Modified k-means Algorithm to Avoid Empty Clusters," *Int. J. Recent Trends Eng.*, vol. 1, no. 1, p. 220, 2009.

[19] S. Haller, "The Things in the Internet of Things," pp. 97–129, 2010, [Online]. Available: http://www.iot-a.eu/public/news/resources/TheThingsintheInternetofThings_SH.pdf

[20] Y. Gu, K. Li, Z. Guo, and Y. Wang, "Semi-supervised k-means ddos

detection method using hybrid feature selection algorithm," *IEEE Access*, vol. 7, pp. 64351–64365, 2019, doi: 10.1109/ACCESS.2019.2917532.

[21] N. Abughazaleh, R. Bin, M. Btish, and H. M., "DoS Attacks in IoT Systems and Proposed Solutions," *Int. J. Comput. Appl.*, vol. 176, no. 33, pp. 16–19, 2020, doi: 10.5120/ijca2020920397.

[22] S. Axelsson, "Research in Intrusion-Detection Systems:," no. October 2002, 2015.

[23] H. Altwaijry and S. Algarny, "Bayesian based intrusion detection system," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 24, no. 1, pp. 1–6, 2012, doi: 10.1016/j.jksuci.2011.10.001.

[24] Y. Li and H. Wu, "A Clustering Method Based on K-Means Algorithm," *Phys. Procedia*, vol. 25, pp. 1104–1109, 2012, doi: 10.1016/j.phpro.2012.03.206.

[25] M. G. H. Omran, A. P. Engelbrecht, and A. Salman, "An overview of clustering methods," *Intell. Data Anal.*, vol. 11, no. 6, pp. 583–605, 2007, doi: 10.3233/ida-2007-11602.

[26] M. Shutaywi, "Silhouette Analysis for Performance Evaluation in Machine," pp. 1–17, 2021.

[27] G. Ogbuabor and U. Kingdom, "C LUSTERING A LGORITHM FOR A H EALTHCARE D ATASET U SING S ILHOUETTE," vol. 10, no. 2, pp. 27–37, 2018, doi: 10.5121/ijcsit.2018.10203.