VISUALISASI SERANGAN DDOS *FIN FLOOD* DENGAN METODE *ARTIFICIAL IMMUNE SYSTEM* PADA JARINGAN *INTERNET OF THINGS* (IoT)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh:

AGUNG SETIAWAN

09011281722039

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

VISUALISASI SERANGAN DDOS *FIN FLOOD* DENGAN METODE *ARTIFICIAL IMMUNE SYSTEM* PADA JARINGAN *INTERNET OF THINGS* (IoT)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

AGUNG SETIAWAN

09011281722039

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

VISUALISASI SERANGAN DDOS *FIN FLOOD* DENGAN METODE *ARTIFICIAL IMMUNE SYSTEM* PADA JARINGAN *INTERNET OF THINGS* (IoT)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

AGUNG SETIAWAN
09011281722039

Indralaya, Juli 2021

Pembimbing I	Pembimbing II
Deris Stiawan, M.T., Ph.D., IPU	**Ahmat Heryanto, S.Kom., M.T.**
NIP. 197806172006041002	**NIP. 198701222015041002**

Ketua Jurusan Sistem Komputer

16/8/21

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 15 Juli 2021

Tim Penguji :

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

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Jr. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Agung Setiawan

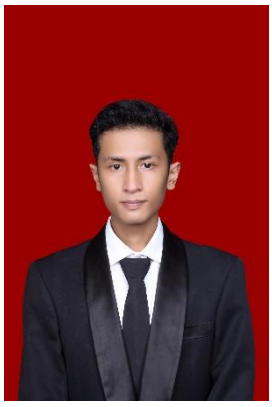
NIM : 09011281722039

Judul : Visualisasi Serangan DDoS *FIN Flood* Dengan Metode *Artificial Immune System* Pada Jaringan *Internet of Things* (IoT)

Hasil Penyecekan *Software iThenticate/Turnitin* : 3%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan 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 paksaan dari siapapun.



Indralaya, Juli 2021

Agung Setiawan
NIM. 09011281722039

HALAMAN PERSEMBAHAN

"Tidak ada penyesalan. Jika seseorang dapat bangga dengan hidupnya, maka seharusnya tidak mengharapkan kesempatan lain."

"If you cannot do great things, do small things but in a great way."

"Tugas Akhir ini saya persembahkan untuk kedua orang tua saya yang tercinta, dengan doa serta dukungan penuh dari mereka yang tanpa lelah selalu memberikan saya semangat sehingga semua yang saya kerjakan dapat berjalan dengan apa yang di harapkan. Pencapaian ini adalah persembahan istimewa untuk papa dan mama."

"Terkadang saya merasa seperti tidak berada ditempat yang seharusnya. Tetapi kemudian saya ingat bahwa saya memiliki kalian, kawan. Sejujurnya saya tidak tahu apa yang saya lakukan tanpa kalian temanku. Terimakasih telah menjadi teman terbaik di dunia."

KATA PENGANTAR

Puji syukur Alhamdulillah penulis panjatkan atas kehadirat Allah SWT yang telah memberikan karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini yang berjudul **"Visualisasi serangan DDoS *FIN Flood* dengan metode *Artificial Immune System* pada jaringan *Internet of Things* (IoT)"**.

Dalam laporan ini penulis menjelaskan mengenai pemodelan untuk identifikasi dan klasifikasi author terhadap suatu publikasi dengan disertai data-data yang diperoleh penulis saat melakukan penelitian dan pengujian data. Penulis berharap agar tulisan ini dapat bermanfaat bagi orang banyak.

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan Proposal Tugas Akhir ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur kepada Allah SWT dan terimakasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan baik dan lancar.

2. Orang tua saya tercinta yang telah membesarkan saya dengan penuh kasih sayang dan selalu mengajarkan saya dalam berbuat hal yang baik. Terimakasih untuk segala do'a, motivasi dan dukungannya baik moril, materil maupun spritual selama ini.

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 Fakultas Ilmu Komputer Universitas Sriwijaya.

5. Bapak Deris Stiawan, M.Kom., PH.D., selaku Dosen Pembimbing Tugas Akhir I yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.

6. Bapak Ahmat Heryanto, M.T., selaku Dosen Pembimbing Tugas Akhir II Tugas Akhir yang telah meluangkan waktunya guna membantu membimbing dan memberi saran terbaik untuk menyeleseikan Tugas Akhir ini.

7. Bapak Rossi Passarella, S.T., M.Eng., selaku Pembimbing Akademik Jurusan Sistem Komputer.

8. Mbak Nurul Afifah, S.Kom, M.Kom. yang telah membantu membimbing dalam menyeleseikan tugas akhir.

9. Mbak Renny selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.

10. Ahmad Afidin, Amartya Bimantara, M. Khoir Septiawan, Meutia Zamieyus, Tia Hermita, Febi Rusmiati, dan teman-teman seperjuangan Tim Grup Riset Comnets yang lainnya yang telah banyak membantu.

11. Dan semua pihak yang telah membantu.

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis. Akhir kata penulis berharap, semoga proposal tugas akhir ini bermanfaat dan berguna bagi khalayak.

Indralaya, Juli 2021

Penulis,

VISUALIZATION OF DDOS FIN FLOOD ATTACKS USING ARTIFICIAL IMMUNE SYSTEM ON THE INTERNET OF THINGS NETWORK

Agung Setiawan (09011281722039)
Dept. of Computer Engineering, Faculty of Computer Science, Sriwijaya University
Email : agungchaniago07@gmail.com

ABSTRACT

Distributed Denial of Service (DDoS) is an attack that can disrupt network traffic by exploiting zombie device controlled by an attacker to flood request. FIN Flood attack is a type of attack that uses TCP FIN packets to measure resources on the server for the purpose of bandwidth duration. In this research, using the TCP FIN flood and zbassocflood dataset from COMNETS labs, Sriwijaya University. Using the Dendritic Cell Algorithm (DCA) which is part of the Artificial Immune System (AIS) to detect DDoS FIN Flood attacks. The result of attack detection in this study in the form of attack alerts which will be grouped according to the MCAV result and visualization the these results will be carried out.

***Keywords*:**

***DDoS, FIN Flood, Visualization, Intenet of Things* (IoT), *Dendritic Cell Algorithm* (DCA), *Artificial Immune System* (AIS)**

VISUALISASI SERANGAN DDOS *FIN FLOOD* DENGAN METODE *ARTIFICIAL IMMUNE SYSTEM* PADA JARINGAN *INTERNET OF THINGS* (IOT)

Agung Setiawan (09011281722039)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : agungchaniago07@gmail.com

ABSTRAK

Distribute Denial of Service (DDoS) merupakan serangan yang bertujuan untuk mengganggu lalu lintas sebuah jaringan dengan memanfaatkan perangkat zombie yang dikendalikan oleh penyerang untuk membanjiri request. Serangan *FIN Flood* jenis serangan yang memakai paket TCP FIN untuk menghabiskan *resource* pada server dengan tujuan menghabiskan *bandwidth*. Pada penelitian ini menggunakan dataset TCP FIN flood dan zbassocflood yang berasal dari *COMNETS* labs Universitas Sriwijaya. Digunakan algoritma *Dendritic Cell Algorithm* (DCA) yang merupakan bagian dari *Artificial Immune System* (AIS) untuk melakukan deteksi serangan *DDoS FIN Flood*. Hasil deteksi serangan pada penelitian ini adalah berupa alert serangan yang akan dikelompokkan sesuai hasil MCAV dan akan dilakukan visualisasi dari hasil tersebut.

Kata Kunci :

DDoS, FIN Flood, Visualization, Intenet of Things (IoT), Dendritic Cell Algorithm (DCA), Artificial Immune System (AIS)

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) adalah sebuah kemampuan untuk menghubungkan beberapa perangkat atau objek-objek yang mempunyai identitas pengenal beserta alamat IP, dengan begitu objek tersebut bisa saling berkomunikasi dan kemudian bertukar informasi melalui jaringan internet [4]. Ancaman yang ada pada IoT bermacam dan beragam, adapun beberapa ancaman yang mempengaruhi IoT adalah seperti *Denial of Service* (DoS), *Distribute Denial Of Service* (DDoS), *Eavesdropping, Node capture, Controlling,* and *Tampering* dapat menurunkan efisiensi jaringan dan mempengaruhi objek IoT [5].

Serangan DDoS telah menjadi ancaman untuk jaringan IoT karena dapat menyebabkan penurunan kecepatan dalam mengakses layanan sehingga layanan tidak dapat melayani akses [6]. Salah satu serangan DDoS yaitu FIN *Flood* yang memakai paket serangan TCP untuk membanjiri server dengan paket FIN untuk menghabiskan *resource* server berupa (RAM, *Processor*, dll) dengan mengakibatkan server tidak dapat menerima *request* lebih lanjut [7]. *Distributed Denial of Service* (DDoS) adalah bentuk lain dari serangan *Denial of Service* (DoS) yang dimana serangan adalah jenis serangan yang menggunakan banyak mesin untuk menyerang targetnya dan mesin-mesin ini bekerja sebagai *zombie* dimana mesin melakukan serangan tanpa persetujuan dari pemiliknya [8].

Pada penelitian [1] membahas bagaimana mendeteksi serangan DDoS *SYN Flood* dengan menerapkan algoritma *Dendritic Cell Algorithm (DCA)*. Tetapi pada pembahasannya tidak terlihat perhitungan *treshold* yang dilakukan dan nilai *MCAV*. Dalam penelitian ini [9] juga ikut dibahas bagaimana menerapkan algoritma *Dendritic Cell Algorithm (DCA)* yang digunakan untuk mendeteksi serangan *Denial of Service (DoS)* dan mendapatkan hasil akurasi 82.7% dan *Detection Rate* sekitar 90.2%. Memanfaatkan metode *Artificial Immune System* dalam mendeteksi serangan DDoS FIN *Flood* dan memvisualkan serangan kedalam bentuk grafik.

Visualisasi ini adalah salah satu solusi dalam menampilkan serangan pada *Network* [10]. Data visualisasi serangan ini akan digunakan untuk mengenali dan menyimpulkan pola serangan dari gambar visual yang komplek. Dengan visualisasi serangan yang baik maka dapat membantu untuk menjelaskan temuan-temuan dalam data menjadi informasi yang mudah ditemukan dan bisa menganalisa pola serangan tersebut [11].

Berdasarkan beberapa penjelasan diatas mengenai penelitian terkait dengan hasil dan penjelasan masing-masing, maka penelitian ini mengusulkan untuk melakukan visualisasi serangan DDoS FIN *Flood* pada jaringan *Internet of Things* (IoT) dengan menggunakan metode *Artificial Immune System*. Pada penelitian ini akan digunakan sebuah dataset dari *COMNETS* lab Universitas Sriwijaya yang berfokus pada serangan FIN *Flood.*

1.2 Rumusan Masalah

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

1. Bagaimana cara membedakan atribut paket serangan DDoS FIN *Flood* dengan paket data normal?
2. Bagaimana melakukan pengujian serangan DDoS FIN *Flood* menggunakan algoritma *Dendritic Cell Algorithm* (DCA)?
3. Bagaimana cara memvisualisasikan traffic serangan DDoS FIN *Flood* dalam bentuk grafik?

1.3 Batasan Masalah

Dari rumusan masalah dan latar belakang penelitian, maka berikut ini batasan masalah pada tugas akhir, anatara lain :

1. Pengamatan hanya difokuskan pada serangan *Distributed Denial of Service* DDoS FIN *Flood.*

2. Metode yang digunakan adalah *Artificial Immune System* dengan algoritma *Dendritic Cell Algorithm*.

3. Tidak membahas mengenai pencegahan terhadap serangan yang ada pada jaringan IoT.

1.4 Tujuan

Adapun tujuan dari penulisan tugas akhir ini, yaitu :

1. Mengenali atribut paket serangan DDoS FIN *Flood* pada sistem jaringan *Internet of Things* (IoT).

2. Mampu mendeteksi serangan DDoS FIN *Flood* dengan algoritma *Dendritic Cell Algorithm* (DCA).

3. Mampu memvisualisasikan traffic serangan DDoS FIN *Flood* ke dalam bentuk grafik.

1.5 Manfaat

Adapun manfaat dari penulisan tugas akhir ini, yaitu :

1. Dapat mempelajari atribut data serangan *Distributed Denial of Service* (DDoS)-FIN *Flood* pada jaringan IoT.

2. Dapat mendeteksi paket serangan DDoS FIN *Flood* menggunakan algoritma *Dendritic Cell Algorithm* (DCA).

3. Dapat Memvisualisasikan traffic serangan DDoS FIN *Flood* ke dalam bentuk grafik.

1.6 Metodelogi Penelitian

Pada tugas akhir ini menggunakan metodologi sebagai berikut :

1. Tahapan Pertama (Studi Pustaka/ Literatur)

Tahap ini dilakukan setelahmasalah 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. Tahapan Kedua (Pengolahan Data)

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

3. Tahap Ketiga (Visualisasi)

   Pada tahap ini dilakukan proses visualisasi serangan DDoS FIN *Flood* dan data normal menggunakan metode *Artificial Immune System*. Setelah proses visualisasi selesei, dilanjutkan pada proses validasi.

4. Tahap Keempat (Analisa)

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

5. Tahap Kelima (Kesimpulan dan Saran)

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

1.7 Sistematika Penulisan

Agar memperoleh gambaran jelas mengenai penelitian ini, maka dibuatlah suatu sistematika penulisan yang berisi gambaran dalam tiap bab penelitian ini, yaitu:

BAB I. PENDAHULUAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah dan Batasan Masalah kemudian Metodologi Penelitian, dan yang terakhir adalah mengenai Sistematika Penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini berisikan teori dari penelitan terkait dengan *Internet of Things* (IoT), *Intrusion Detection System*, *FIN Flood Distributed Denial of Service attack*, *Dendritic Cell Algorithm* (DCA), Visualisasi serangan, dan yang berkaitan secara langsung dengan penelitian.

BAB III. METODOLOGI PENELITIAN

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

BAB IV. PENGUJIAN DAN ANALISA

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

BAB V. KESIMPULAN

Bab ini berisi kesimpulan tentang hasil penelitian yang telah dilakukan, serta menjawab setiap tujuan yang hendak dicapai sesuai yang tercantum pada BAB I (Pendahuluan) .

DAFTAR PUSTAKA

[1] G. Ramadhan, Y. Kurniawan, and C. S. Kim, "Design of TCP SYN Flood DDoS attack detection using artificial immune systems," *Proc. 2016 6th Int. Conf. Syst. Eng. Technol. ICSET 2016*, pp. 72–76, 2017.

[2] L. Ding, F. Yu, and Z. Yang, "Survey of DCA for abnormal detection," *J. Softw.*, vol. 8, no. 8, pp. 2087–2094, 2013.

[3] D. Stiawan *et al.*, "TCP FIN flood attack pattern recognition on Internet of Things with rule based signature analysis," *Int. J. online Biomed. Eng.*, vol. 15, no. 7, pp. 124–139, 2019.

[4] Ernita Dewi Meutia, "Internet of things–Keamanan dan Privasi," p. (Vol. 1, No. 1, pp. 85-89)., 2015.

[5] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, no. March, pp. 10–28, 2017.

[6] 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.

[7] A. Sahi, D. Lai, Y. Li, and M. Diykh, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment," *IEEE Access*, vol. 5, no. c, pp. 6036–6048, 2017.

[8] S. Behal and K. Kumar, "Trends in Validation of DDoS Research," *Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 7–15, 2016.

[9] C. A. Winanto, "Deteksi serangan Denial of Service mengunakan Artificial Immune System," *Comput. Eng.*, vol. 2, no. Faculty of Computer Science, Sriwijaya University, pp. 1–57, 2017.

[10] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, 2017.

[11] 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.

[12] Sharipuddin *et al.*, “Features extraction on iot intrusion detection system using principal components analysis (Pca),” *Int. Conf. Electr. Eng. Comput. Sci. Informatics*, vol. 2020-Octob, pp. 114–118, 2020.

[13] S. Sheng, C. Wu, and X. Dong, “Research on Visualization Systems for DDoS Attack Detection,” *Proc. - 2018 IEEE Int. Conf. Syst. Man, Cybern. SMC 2018*, pp. 2986–2991, 2019.

[14] O. Igbe, O. Ajayi, and T. Saadawi, “Detecting Denial of Service Attacks Using a Combination of Dendritic Cell Algorithm and the Negative Selection Algorithm,” *Proc. - 2nd IEEE Int. Conf. Smart Cloud, SmartCloud 2017*, pp. 72–77, 2017.

[15] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, “Internet of things security: A top-down survey,” *Comput. Networks*, vol. 141, pp. 199–221, 2018.

[16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[17] R. Hermawan, “Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos),” *Anal. Konsep Dan Cara Kerja Serangan Komput. Distrib. Denial Serv.*, vol. 5, no. 1, pp. 1–14, 2013.

[18] 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. 2017-Janua, no. Cic, pp. 253–262, 2017.

[19] D. Dasgupta, S. Yu, and F. Nino, “Recent advances in artificial immune systems: Models and applications,” *Appl. Soft Comput. J.*, vol. 11, no. 2, pp. 1574–1587, 2011.

[20] Z. Chelly and Z. Elouedi, “A survey of the dendritic cell algorithm,” *Knowl. Inf. Syst.*, vol. 48, no. 3, pp. 505–535, 2016.

[21] J. Z. H. D. Yanping Zhang, Yang Xiao, Min Chen, “A survey of security visualization for computer network logs,” *Secur. Commun. NETWORKS*, vol. 9, no. 22, pp. 404–421, 2012.

[22] T. Zhang, X. Wang, Z. Li, F. Guo, Y. Ma, and W. Chen, “A survey of network anomaly visualization,” *Sci. China Inf. Sci.*, vol. 60, no. 12, pp. 1–17, 2017.

[23] W. Wilianto and A. Kurniawan, “Sejarah, Cara Kerja Dan Manfaat Internet of Things,” *Matrix J. Manaj. Teknol. dan Inform.*, vol. 8, no. 2, pp. 36–41, 2018.