VISUALISASI DATA SERANGAN PING FLOOD DENGAN METODE NAIVE BAYES DI JARINGAN *INTERNET OF THINGS* (IoT)

TUGAS AKHIR

Diajukan untuk melengkapi salah satu syarat
Memperoleh gelar sarjana komputer

Oleh :

Sri Mardhiati
09011281621125

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN

VISUALISASI DATA SERANGAN PING FLOOD DENGAN METODE NAIVE BAYES DI JARINGAN INTERNET OF THINGS (IoT)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

Sri Mardhiati
(09011281621125)

Indralaya, Juli 2020

Mengetahui,
Ketua Jurusan Sistem Komputer

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

Pembimbing Tugas Akhir

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

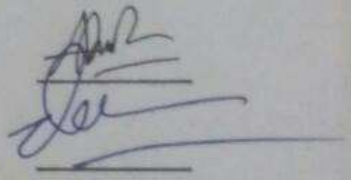
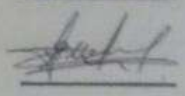
HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis

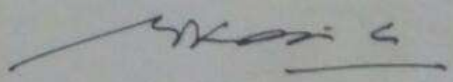
Tanggal : 09 Juli 2020

Tim Penguji :

1. Ketua	**: Aditya Putra Perdana P, M.T**	
2. Sekretaris	**: Deris Stiawan,Ph.D.**	
3. Anggota I	**: Ahmad Heryanto, M.T.**	
4. Anggota II	**: Sarmayanta Sembiring, M.T.**	

Mengetahui,

Ketua Jurusan Sistem Komputer



Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Sri Mardhiati

Nim : 09011281621125

Program Studi : Sistem Komputer

Judul Skripsi : Visualisasi Data Serangan *Ping Flood* dengan Metode *Naïve Bayes* di Jaringan *Internet of Things* (IoT)

Hasil Pengecekan Software iThenticate/Turnitin : 15 %

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 sanki akademik yang diberikan oleh jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Demikian pernyataan ini saya buat dengan sebenar-benarnya.

Indralaya, Juli 2020

Yang Menyatakan,

Sri Mardhiati

NIM. 09011281621125

HALAMAN PERSEMBAHAN

"Barangsiapa bertakwa pada Allah, maka Allah memberikan jalan keluar kepadanya dan memberi rezeki dari arah yang tidak disangka-sangka.. Barangsiapa yang bertaqwa pada Allah, maka Allah jadikan urusannya menjadi mudah.. barangsiapa yang bertaqwa pada Allah akan dihapuskan dosa2nya dan mendapatkan pahala yang agung" (QS. Ath-Thalaq: 2, 3, 4)

"Janganlah kamu bersikap lemah dan janganlah pula kamu bersedih hati, padahal kamulah orang orang yang paling tinggi derajatnya jika kamu beriman" (***QS Al Imran : 139***)

Dengan mengucapkan syukur Alhamdulillah atas rahmat dari ALLAH SWT , kupersembahkan karya kecil ini untuk ...

Kedua orang tua ku yang tercinta

Umi Dra.Tisah

Buya Nasrul TM

Saudara Dan Saudari Ku Yang Ku Sayangi

Habibatur Rahmi, S.Si

Raudatul Hasanah

Rima Rahmawati

Khairul Anwar

Hasnah Nurul Huda

KATA PENGANTAR

Bismillahirrahmanirrahim.

Assalamu'alaikum Warahmatullahi Wabarakatuh. Puji dan syukur penulis panjatkan kehadirat Allah SWT, karena berkat karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini dengan judul "Visualisai data serangan ping flood dengan metode naïve bayes di jaringan internet of things (IoT)*".*

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

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga penulisan proposal tugas akhir ini dapat berjalan dengan lancar.
2. Umi Dra.Tisah, Buya Nasrul,T.M , Uni ku Habibarur Rahmi.S.Si, Kakak ku Raudatul Hasanah, Adik perempuan ku Rima Rahmawati, Adik laki-laki ku Khairul Anwar dan Adik Bungsu ku Hasnah Nurul Huda yang selalu memberikan semangat dan do'a.
3. Bapak Jaidan Jauhari, S.Pd. M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
4. Bapak Ir. Sukemi selaku Ketua Jurusan Sistem Kompuer Fakutas Ilmu Komputer Universitas Sriwijaya
5. Bapak Deris Stiawan, M.T ., Ph.D. selaku Pembimbing Tugas Akhir Penulis.
6. Ibu Sri Desy Siswanti, M.T. selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer.
7. Kak Nurul Afifah yang telah membantu memberikan arahan dan bimbingan dalam mengerjakan tugas akhir.
8. Ahmad Firdaus S.SI yang banyak membantu dan menemani dari awal hingga selesainya tugas akhir ini.
9. Teman-teman Jurusan Sistem Komputer Reguler kelas A dan B angkatan 2016 yang tidak dapat saya sebutkan satu persatu.

Penulis juga berterima kasih kepada semua pihak yang terlibat, baik secara langsung ataupun tidak langsung dalam penyelesaian tugas akhir ini.

Tentunya dalam pembuatan tugas akhir ini, masih terdapat beberapa kekurangan dan kesalahan yang mungkin terjadi. 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 kita terhadap pengolahan citra digital dan dapat menjadi bahan referensi terhadap mahasiswa yang memerlukan.

Indralaya, Juli 2020

Penulis

Ping Flood Attack Data Visualization Using Naive Bayes Method On Internet Of Things (IoT)

Sri Mardhiati (09011281621125)
Department of Computer Engineer, Faculty of Computer Science
Universitas Sriwijaya
Email : srimardhiati.5@gmail.com

Abstract

This research focused on ping flood attack visualization using naive Bayes method. This research using Internet of Thing (IoT) network which are have three kinds of cluster, normal, attack and combined. Dataset testing was performed using snort to prove ping flood attack on that dataset.(The classification is performed to cluster the data into normal attack and combined Based on confussion matrix result, the accuracy value obtained is 0.972. The final step is visualized dataset which are already identified and classified based on each class, using naive Bayes method. In the training data, attack class probability value obtained is 0,034 and for normal class value obtained is 0,004. For testing data, value obtained is 0,12

Keyword : *Internet of Things* (IoT), *Visualization, Classification Naive Bayes, Ping Flood*

Visualisasi Data Serangan Ping Flood dengan Metode Naïve Bayes di Jaringan Internet of Things (IoT)

Sri Mardhiati (09011281621125)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email : srimardhiati.5@gmail.com

Abstrak

Penelitian ini difokuskan pada visualisasi serangan *ping flood* menggunakan metode *Naive Bayes.* Penelitian ini menggunakan jaringan *Internet of Thing* (IoT) yang memiliki tiga jenis *claster* yaitu, normal, serangan dan gabungan. Pengujian dataset dilakukan menggunakan *snort* untuk membuktikan serangan *ping flood* pada dataset tersebut. (Klasifikasi ini dilakukan untuk mengelompokkan data menjadi serangan normal dan gabungan). Berdasarkan hasil *confussion matrix*, nilai akurasi yang diperoleh adalah 0,972. Langkah terakhir adalah memvisualisasikan dataset yang sudah di identifikasi dan di klasifikasikan berdasarkan masing-masing kelas, menggunakan metode naive Bayes. Dalam data *Training* nilai probabilitas kelas serangan yang diperoleh adalah 0,034 dan untuk nilai kelas normal yang diperoleh adalah 0,004.Untuk hasil data *testing*, nilai yang diperoleh adalah 0,12.

Kata Kunci : *Internet of Things* (IoT), *Visualization, Classification Naive Bayes, Ping Flood*

DAFTAR ISI

Halaman

BAB III METODOLOGI PENELITIAN

BAB IV HASIL DAN ANALISA

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Internet of Things (IoT) adalah sebuah kemampuan untuk menghubungkan objek-obek cerdas dan memungkinkannya untuk berinteraksi dengan objek lain, lingkungan maupun dengan peralatan komputasi cerdas lainnya melalui jaringan internet [1]. IoT sesungguhnya sangat perlu suatu sistem keamanan yang cukup ketat. Karena IoT juga diancam oleh serangan dan ancaman yang spesifik bagi IoT [3]. Ancaman-ancaman yang dapat mempengaruhi entitas IoT sangat beragam, tergantung dari target serangan tersebut. Macam-macam ancaman terhadap IoT adalah *Denial of Service* (DoS), *Eavesdropping, Node capture, Controlling*, dan merusak secara fisik pada objek IoT [2].

Serangan pada *internet of things* (IoT) salah satu nya adalah *Denial of Service* (DoS), yaitu serangan yang menyebabkan pihak yang sah tidak dapat mengkses layanan [2]. Ada berbagai macam sasaran penyerangan DoS, seperti membanjiri jaringan dengan lalu lintas yang tidak berguna, kekuatan kelelahan sumber daya, serangan DoS ke sumber data, dan jamming sinyal [3]. Salah satu jenis serangan DoS adalah *ping flooding*. *Ping Flooding* adalah *brute force denial of service* sederhana. Jika serangan dilakukan oleh penyerang dengan *bandwidth* yang lebih baik dari korban, maka mesin korban tidak dapat mengirimkan paket data ke dalam jaringan (*network*). Hal ini terjadi karena mesin korban di banjiri (*flood*) oleh peket-paket ICMP [2].

Visualisasi menjadi salah satu solusi dalam menampilkan serangan di *network* [5]. Dengan visulisasi data, akan lebih mudah dalam mengenali dan menyimpulkan pola dari gambar visual yang komplek. Visualisasi data yang baik

dapat membantu *data scientist* untuk menjelaskan temuan-temuan dalam data menjadi informasi yang mudah dipahami[4].

Pada penelitian sebelumnya [5] menyajikan visualisasi dalam bidang two dimensional (2D) untuk mengkategorikan paket ISCX dan DARPA dataset. Paket data akan dibedakan dalam dua kategori yaitu paket data *attack* dan paket data normal berdasarkan pattern serangan *brute force*. Serangan *brute force* melakukan penyerangan pada beberapa layanan protokol seperti *secure shell* (SSH) dan *telecommunication network* (Telnet). Pada ISCX dataset serangan *brute force* terjadi pada layanan SSH, sedangkan DARPA dataset terjadi pada layanan TELNET. Metode *K-Means* dan metode *Naïve Bayes* di implementasikan pada penelitian ini untuk memberikan gambaran visual serta mendapatkan hasil pengkategorian yang efektif.

Berdasarkan rujukan pada masing-masing penelitian diatas, maka dalam penelitian ini akan dilakukan klasifikasi terhadap serangan *Denial of Service* (DoS) khususnya *Ping Flood* menggunakan metode naïve bayes pada jaringan *internet of things* (IoT). Penggunaan algoritma ini bertujuan untuk dapat mengelompokan jenis data serangan, data normal, dan data gabungan (normal dan serangan). Kemudian memvisualisasikannya menjadi data yang lebih mudah untuk di pahami.

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang diatas, maka rumusan masalah yang akan dibahas pada penelitian ini adalah :

1. Bagaimana cara melakukan pengujian adanya serangan pada dataset serangan *ping flood* ?
2. Bagaimana cara melakukan klasifikasi terhadap *traffic* serangan yang telah didapatkan ?
3. Bagaimana cara memvisualisasikan *traffic* serangan *ping flood* ke dalam bentuk grafik menggunakan metode *Naïve bayes* ?

1.3 BATASAN MASALAH

Selain perumusan masalah diatas, juga terdapat batasan masalah pada penelitian ini, antara lain :

1. Data serangan *ping flood* diambil dari dataset pada penelitian sebelumnya
2. Data serangan diuji terlebih dahulu menggunakan *snort*, untuk memastikan adanya serangan pada dataset tersebut.
3. Data serangan *ping flood* diklarifikasikan atau dikelompokan berdasarkan jenis nya
4. Data serangan *ping flood* divisualisasikan.
5. Metode yang digunakan adalah *Naïve Bayes*.
6. Bahasa pemprograman yang dipakai adalah Python

1.4 TUJUAN

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Melakukan pengujian adanya serangan pada dataset serangan *ping flood*
2. Melakukan klasifikasi terhadap *traffic* serangan *ping flood*
3. Memvisualisasikan *traffic* serangan *ping flood* ke dalam bentuk grafik menggunakan metode *Naïve bayes*.

1.5 MANFAAT

Adapun manfaat yang dapat diambil dari penelitian ini adalah sebagai berikut :

1. Dapat melakukan pengujian ada nya serangan pada dataset serangan *ping flood*
2. Dapat meng-klasifikasi kan *traffic* serangan *ping flood*
3. Dapat Memvisualisasikan *traffic* serangn *ping flood* ke dalam bentuk grafik menggunakan metode *Naïve bayes*.

1.6 METODOLOGI PENELITIAN

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

1. Metode study pustaka/Literatur.

Dalam tahap ini akan dilakukan segmentasi menggunakan Algoritma *Naïve Bayes* yang didapat melalui jurnal ilmiah, buku, majalah maupun internet untuk menyelesaikan tugas akhir ini.

2. Metode Konsultasi

   Pada metode ini, peneliti melakukan konsultasi kepada orang-orang yang dianggap memiliki pengetahuan dan wawasan terhadap permasalahan yang ditemui saat pembuatan Tugas Akhir.

3. Metode pengumpulan data

   Dalam tahap ini, dilakukan dengan berbagai cara. Yakni dengan menggunakan serangan *ping flood* database yang sudah tersedia yang saya ambil dalam database *STARE*. Data yang akan diteliti sebanyak satu serangan.

4. Metode Observasi

   Metode ini dilakukan dengan pengamatan dan pencatatan terhadap data yang diperoleh.

5. Metode perancangan dan pembuatan sistem

   Pada tahap ini akan dilakukan perancangan serta pembuatan sistem yang dapat dilakukan untuk visualisasi data serangan *ping flood* menggunakan metode *Naïve Bayes*. Sehingga sistem tersebut dapat melakukan visualisasi terhadap data serangan *ping flood*.

1.7 SITEMATIKA PENULISAN

Dalam memudahkan proses penyusunan tugas akhir ini, dan memperjelas konten dari setiap bab, maka dibuat adanya suatu sistematika penulisan yakni sebagai berikut ;

1. BAB I. PENDAHULUAN

   Pada bab ini berisikan penjelasan secara sistematis mengenai landasan topik penelitian, Yang meliputi latar belakang, tujuan, manfaat, rumusan masalah, batasan masalah, metodologi penelitian dan sistematika penulisan.

2. BAB II. TINJAUAN PUSTAKA

Bab ini berisikan landasan teori dari penelitian tugas akhir yang terkait mengenai *Internet Of Things (Iot), Serangan Ping Flood, Clustering Algorithm*, *Naïve Bayes*, serta teori lain yang berkaitan dengan penelitian ini.

3. BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian tugas akhir ini dilakukan. Penjelasan yang terkait pada bab ini meliputi tahapan perancangan system serta penerapan metode penelitian.

4. BAB IV HASIL DAN ANALISA

Bab ini menjelaskan mengenai hasil pengujian yang telah dilakukan, serta analisis dari hasil pemgujian tersebut berdasarkan parameter yang telah ditentukan sebelumnya.

5. BAB V. KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan terhadap hasil penelitian yang telah dilakukan, yang merupakan jawaban dari setiap tujuan yang hendak dicapai pada penelitian ini yang sudah tercantum pada Bab I. selanjutnya bab ini juga bersisikan mengenai saran terhadap penelitian ini yang berguna untuk pengembangan dipenelitian selanjutnya.

DAFTAR PUSTAKA

[1] E. D. Meutia, "Internet of Things – Keamanan dan Privasi," *Semin. Nas. dan Expo Tek. Elektro 2015*, pp. 85–89, 2015.

[2] 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.

[3] 348–354.psiah NaNapsiah, Stiawan, D., & Heryanto, A. (2016). Visualisasi Serangan Denial Of Service Dengan Clustering Menggunakan K-Means Algorithm. Annual Research Seminar, 2(1), D. Stiawan, and A. Heryanto, "Visualisasi Serangan Denial Of Service Dengan Clustering Menggunakan K-Means Algorithm," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 348–354, 2016.

[4] S. Sandra, D. Stiawan, and A. Heryanto, "Visualisasi Serangan Brute Force Menggunakan Metode K-Means dan Naïve Bayes," *Proceeding - Annu. Res. Semin. Proceeding*, vol. 2, no. 1, pp. 315–320, 2016.

[5] 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.

[6] C. De Souza, "Brasil Journal of Pembangunan Brasil Journal of Pembangunan," no. November, 2019.

[7] H. Choi, H. Lee, and H. Kim, "Fast detection and visualization of network attacks on parallel coordinates," *Comput. Secur.*, vol. 28, no. 5, pp. 276–288, 2009.

[8] W. Wilianto and A. Kurniawan, "Sejarah, Cara Kerja Dan Manfaat Internet of Things," *Matrix J. Manaj. Teknol. dan Inform.*, vol. 8, no. 2, p. 36, 2018.

[9] A. K. Jain and V. Tokekar, “Classification of denial of service attacks in mobile ad hoc networks,” *Proc. - 2011 Int. Conf. Comput. Intell. Commun. Syst. CICN 2011*, pp. 256–261, 2011.

[10] M. Mustafa, “Intelligent Systems dan Aplikasi Teknik Analisis kinerja JST dan Naif Bayes Klasifikasi Algoritma Klasifikasi data,” vol. 7, pp. 88–91, 2019.

[11] “Analisis Bayes , Neural Network dan Pohon Klasi fi er dari Klasifikasi Teknik dalam Data Mining Analisis Bayes , Neural Network dan Pohon Classifier Klasifikasi Teknik dalam Data,” 2016.

[12] J. Aviles and R. Esquivel, “Mining Social Media Data of Philippine Higher Education Institutions Using Naive Bayes Classifier Algorithm,” *SSRN Electron. J.*, 2019.

[13] A. Wood, V. Shpilrain, K. Najarian, and D. Kahrobaei, “Private naive bayes classification of personal biomedical data: Application in cancer data analysis,” *Comput. Biol. Med.*, vol. 105, pp. 144–150, 2019.

[14] N. Komang, S. Julyantari, and I. K. D. Suryawan, “Data Mining Prestasi Akademik Dengan Naive Bayes Berdasarkan Attribut Importance (AI),” *J. Sist. Dan Inform.*, pp. 75–85, 2013.

[15] A. Saleh, “Implementasi Metode Klasifikasi Naïve Bayes Dalam Memprediksi Besarnya Penggunaan Listrik Rumah Tangga,” *Creat. Inf. Technol. J.*, vol. 2, no. 3, pp. 207–217, 2015.

[16] V. Kumar, “Signature Based Intrusion Detection System Using SNORT,” *Int. J. Comput. Appl. Inf. Technol. - IJCAIT*, vol. I, no. Iii, pp. 35–41, 2012.

[17] A. Chahal and R. Nagpal, “Performance of Snort on DARPA Dataset and different False Alert Reduction techniques,” *3rd Int. Conf. Electr. Electron. Eng. Trends, Commun. Optim. Sci.*, pp. 350–355, 2016.

[18] T. M., A. A., and H. M., “A Hybrid Snort-Negative Selection Network Intrusion

Detection Technique," *Int. J. Comput. Appl.*, vol. 146, no. 5, pp. 24–31, 2016.

[19] A. Garg and P. Maheshwari, "Performance analysis of Snort-based Intrusion Detection System," *ICACCS 2016 - 3rd Int. Conf. Adv. Comput. Commun. Syst. Bringing to Table, Futur. Technol. from Arround Globe*, pp. 0–4, 2016.

[20] Y. C. Zhang and L. Sakhanenko, "The naive Bayes classifier for functional data," *Stat. Probab. Lett.*, vol. 152, pp. 137–146, 2019.

[21] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing Adversarial Attacks Against Deep Learning for Intrusion Detection in IoT Networks."

[22] V. H. Bezerra, V. G. Turrisi, R. A. Martins, S. B. Junior, R. S. Miani, and B. B. Zarpel, "Providing IoT host-based datasets for intrusion detection."

[23] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics : Bot-IoT dataset," *Futur. Gener. Comput. Syst.*, vol. 100, pp. 779–796, 2019.

[24] I. P. D. A. N. Port, S. D. A. N. Wireshark, D. N. Apriliani, M. A. Sasmita, and T. Windari, "Kata Kunci :," vol. 1, pp. 6–16, 2017.

[25] R. Hermawan, "ANALISIS KONSEP DAN CARA KERJA SERANGAN KOMPUTER DISTRIBUTED DENIAL OF SERVICE (DDOS)," vol. 5, no. 1, pp. 1–14, 1979.

[26] Q. Gu and P. Liu, "Denial of Service Attacks," *Handb. Comput. Networks*, vol. 3, no. 9, pp. 454–468, 2012.