DETEKSI SERANGAN *DENIAL OF SERVICE* MENGGUNAKAN *RULE BASED SIGNATURE ANALYSIS* PADA JARINGAN *INTERNET OF THINGS*

OLEH :

DIMAS WAHYUDI
09011281320004

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2018

DETEKSI SERANGAN *DENIAL OF SERVICE* MENGGUNAKAN *RULE BASED SIGNATURE ANALYSIS* PADA JARINGAN *INTERNET OF THINGS*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

DIMAS WAHYUDI
09011281320004

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018

HALAMAN PENGESAHAN

DETEKSI SERANGAN *DENIAL OF SERVICE* MENGGUNAKAN *RULE BASED SIGNATURE ANALYSIS* PADA JARINGAN *INTERNET OF THINGS*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

DIMAS WAHYUDI
09011281320004

Indralaya, Desember 2018

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng.
NIP. 197806112010121004

Pembimbing

Deris Stiawan, Ph.D.
NIP. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Sabtu
Tanggal : 24 November 2018

Tim Penguji :

1. **Ketua : Ahmad Fali Oklilas, M.T.**
2. **Anggota I : Dr. Reza Firsandaya Malik, M.T.**
3. **Anggota II : Huda Ubaya, M.T.**

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng.
NIP. 197806112010121004

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	:	Dimas Wahyudi
NIM	:	09011281320004
Program Studi	:	Sistem Komputer
Judul	:	Deteksi Serangan *Denial of Service* Menggunakan *Rule Based Signature Analysis* Pada Jaringan *Internet of Things*

Hasil Pengecekan *Software iThenticate/Turnitin* : 12%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya 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.

Indralaya, Desember 2018

Dimas Wahyudi
NIM. 09011281320004

HALAMAN PERSEMBAHAN

"Menunggu adalah memulai atau tertinggal."

"Balas dendam terbaik adalah menjadikan dirimu lebih baik."
(Ali Bin Abi Thalib Radhiyallahu'anhu)

"Failure only happens when we give up."
(B.J. Habibie)

"Hai orang-orang yang beriman, jadikanlah sabar dan shalat sebagai penolongmu, sesungguhnya Allah beserta orang-orang yang sabar."
(QS. Al-Baqarah [2]: 153).

Dengan mengucap syukur Alhamdulillah atas rahmat Allah Subhanahu wa Ta'ala, kupersembahkan karya kecil ini untuk . . .

Terkhusus untuk ibuku tercinta
(Mely Mardiah)

Kedua orang tua tercinta
(Ayah Rusli Abu Bakar dan Ibu Mely Mardiah)

Ketiga kakakku
(Rely Esa Kusuma, Muhammad Jaka Priadi, Agung Noprianto)

Saudaraku
(Ratih Komala Sari & Emilia Nurhuda)

Teman-teman seperjuangan
(Sistem Komputer angkatan 2013)

Teman-teman organisasi
(Lab COMNETS, HIMASISKO, NAC dan LDF WIFI)

Almamaterku
(Universitas Sriwijaya)

14 Desember 2018

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah Subhanahu wa Ta'ala yang telah memberikan rahmat, hidayah serta izin-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul **"Deteksi Serangan *Denial of Service* Menggunakan *Rule Based Signature Analysis* Pada Jaringan *Internet of Things*"**. Laporan ini disusun setelah melaksanakan penelitian yang diajukan untuk memperoleh gelar Sarjana (S1) pada Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya.

Sholawat dan salam semoga senantiasa tercurah kepada Rasulullah Muhammad Shallallahu 'alaihi wa sallam, keluarga dan para sahabat yang menjadi panutan dan teladan bagi umat manusia sehingga kehidupan umat manusia lebih baik terutama dalam bidang ilmu pengetahuan.

Penulis menyampaikan ucapan terima kasih kepada semua pihak untuk setiap bimbingan, semangat dan doa yang telah diberikan kepada penulis sehingga terselesaikannya tugas akhir ini. Ucapan terima kasih, penulis sampaikan kepada:

1. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer, Universitas Sriwijaya.
2. Bapak Rossi Passarella, M.Eng. selaku Ketua Jurusan Sistem Komputer, Fakultas Ilmu, Komputer Universitas Sriwijaya.
3. Bapak Rossi Passarella, M.Eng. selaku Pembimbing Akademik, yang telah membimbing penulis selama menempuh kuliah di Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya.
4. Bapak Deris Stiawan, Ph. D. selaku Dosen Pembimbing tugas akhir, yang telah memberikan bimbingan, semangat, serta memfasilitasi sarana dan prasarana proses penelitian pengerjaan tugas akhir ini.
5. Bapak Dr. Reza Firsandaya Malik, M.T, Bapak Ahmad Fali Oklilas, M.T, Bapak Huda Ubaya, M.T selaku dosen tim penguji sidang tugas akhir yang telah memberikan kritik dan saran serta ilmu yang bermanfaat sehingga laporan tugas akhir ini menjadi lebih baik.

6. Seluruh Dosen Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Univeristas Sriwijaya.
7. Staff di Fakultas Ilmu Komputer, bagian akademik, kemahasiswaan, tata usaha, perlengkapan, dan keuangan, yang telah membantu penyelesaian proses administrasi.
8. Staff di jurusan Sistem Komputer, khususnya Kak Ahmad Reza yang telah membantu penyelesaian proses administrasi.
9. Keluarga tercinta, terkhusus untuk Ibuku tercinta Mely Mardiah, Ayah Rusli Abu Bakar, Kakakku Rely Esa Kusuma, Muhammad Jaka Priadi dan Agung Noprianto, Keponakan Muhammad Alif Irsyad, Saudaraku Ratih Komala Sari dan Emilia Nurhuda yang selalu ada dan tidak pernah lelah dalam mendidik dan memberikan dukungan baik secara moril maupun materil kepada penulis sehingga dapat menyelesaikan laporan tugas akhir ini.
10. Teman-teman satu tema dalam penelitian bidang keamanan jaringan *Internet of Things (IoT)* – IoTA Team, Riki Andika S.Kom, Meilinda Eka Suryani S.Kom, serta kak Kgs Rahmat Shaleh, S.Kom (c).
11. Teman-teman seperjuangan Laboratorium COMNETS Johan Wahyudi, S.Kom (c), Rendika Adha Tanjung, S.Kom (c), Riki Andika S.Kom, Sri Suryani, S.Kom, Fepiliana, S.Kom, Meilinda Eka Suryani, S.Kom dan Leny Novita Sari, S.Kom.
12. Kakak-kakak panutan yang telah memberikan pengetahuan, wawasan, bantuan teknis, motivasi dan masukan-masukannya, Kak Eko Arif Winanto, S.Kom, Kak Candra Adi Winanto, S.Kom dan Kak Ahmad Zaki, S.Kom.
13. Teman penghuni baru Laboratorium COMNETS yang telah membantu dalam proses penelitian, Meila Kusuma Perdana, S.Kom (c).
14. Teman-teman satu angkatan, Sistem Komputer kelas B.
15. Serta Organisasi di Fakultas Ilmu Komputer, Universitas Sriwijaya, LDF WIFI (Lembaga Dakwah Fakultas Wahana Islamiyah dan Forum Ilmu), HIMASISKO (Himpunan Mahasiswa Sistem Komputer) dan NAC (Network Administrator Club),
16. Serta semua pihak yang telah membatu dalam penyelesaian tugas ahir ini.

Semoga dengan terselesainya tugas ahir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan untuk penelitian selanjutnya dalam penelitian terkait Deteksi Serangan *Denial of Service* Menggunakan *Rule Based Signature Analysis* Pada *Jaringan Internet of Things*.

Dalam penulisan laporan ini, penulis menyadari bahwa masih banyak terdapat kekurangan dan ketidak sempurnaan, oleh karena itu penulis mohon saran dan kritik yang membangun untuk perbaikan laporan Tugas Akhir ini, agar menjadi lebih baik dimasa yang akan datang.

Indralaya, Desember 2018

Penulis

Denial of Service Attack Detection using Rule based Signature Analysis on Internet of Things (IoT) Network

Dimas Wahyudi (09011281320004)
Department of Computer Engineering, Faculty of Computer Science, Sriwijaya University
email : mail.dimaswahyudi@gmail.com

Abstract

This research focus on pattern recognition of TCP FIN flood and zbassocflood/association flooding attacks on Internet of Things (IoT) network using rule based signature analysis method. The research was conducted on WiFi and IEEE 802.15.4 communication with normal traffic, attack traffic and combined normal – attack traffic, fifteen different datasets were generated from these schemes, consisting of normal datasets, attack datasets and normal-attack datasets. The testing was performanced on two stages, there are : (i) testing with Snort Rules as Intrusion Detection System (IDS), and (ii) testing with rule based signature analysis method using Intrusion Detection Engine (IDE) naive string matching. In this research, the measurement of detection result using confusion matrix detection rate method bases on Snort IDS and Intrusion Detection Engine (IDE) naive string matching are presented. The Snort IDS shows that has average 17,7845% of TPR, 0,0266% FPR, 79,9734% TNR, 62,2155% for FNR and the detection accuracy is 26,3268%. While the Intrusion Detection Engine (IDE) using naive string matching that has average percentage 99,9131% of TPR, 0% FPR, 100% TNR, 0,0869% FNR and the detection accuracy is 99,9199%.

Keywords : TCP FIN flood, zbassocflood / association flooding, Internet of Things (IoT), Snort Intrusion Detection System (IDS), Intrusion Detection Engine (IDE), Naive String Matching

Deteksi Serangan *Denial of Service* Menggunakan *Rule Based Signature Analysis* Pada Jaringan *Internet of Things*

Dimas Wahyudi (09011281320004)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
email : mail.dimaswahyudi@gmail.com

Abstrak

Fokus penelitian ini adalah pengenalan pola serangan *TCP FIN flood* dan *zbassocflood/association flooding* pada jaringan *Internet of Things (IoT)* menggunakan metode *rule based signature analysis*. Penelitian dilakukan pada komunikasi *WiFi* dan *IEEE 802.15.4* dengan trafik normal, trafik serangan dan gabungan trafik normal-serangan, dari skenario ini dihasilkan lima belas *dataset* berbeda, yang terdiri dari *dataset* normal, *dataset* serangan dan *dataset* normal-serangan. Pengujian dilakukan dengan dua tahapan : (i) pengujian dengan *Snort* sebagai *Intrusion Detection System (IDS)*, dan (ii) pengujian menggunakan metode *rule based signature analysis* dengan *Intrusion Detection Engine (IDE) naive string matching*. Evaluasi hasil deteksi dengan menggunakan metode *confusion matrix detection rate* pada *Snort IDS* dan *Intrusion Detection Engine (IDE) naive string matching*. Menunjukkan *Snort IDS* memiliki persentase rata-rata dengan tingkat *TPR* sebesar 17,7845%, *FPR* sebesar 0,0266%, *TNR* sebesar 79,9734%, *FNR* sebesar 62,2155% dan tingkat akurasi deteksi *(accuracy)* sebesar 26,3268%. Sedangkan *Intrusion Detection Engine (IDE)* menggunakan *naive string matching* memiliki persentase rata-rata dengan tingkat *TPR* sebesar 99,9131%, *FPR* sebesar 0%, *TNR* sebesar 100%, *FNR* sebesar 0,0869% dan tingkat akurasi *(accuracy)* sebesar 99,9199%.

Kata Kunci : *TCP FIN flood, zbassocflood / association flooding, Internet of Things (IoT),* S*nort Intrusion Detection System (IDS), Intrusion Detection Engine (IDE), Naive String Matching*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I. PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) merupakan suatu jaringan yang mengintegrasikan berbagai teknologi perangkat identifikasi, penginderaan dan komunikasi, seperti *Radio Frequency Identification (RFID)*, *tags*, sensor, aktuator, ponsel, dan berbagai perangakat kabel/nirkabel lainnya melalui skema pengalamatan yang unik berdasarkan protokol komunikasi standar [1]. Setiap objek dalam jaringan *IoT* mampu berinteraksi, bekerja sama, memproses, mengolah dan menyampaikan informasi secara otonom untuk menghasilkan layanan, seperti informasi statistik, *monitoring* dan sistem kontrol [2]. Hal ini memungkinkan setiap orang untuk dapat saling terhubung, dan menggunakan layanan apapun, kapanpun dan dimanapun. *IoT* dapat diklasifikasikan menjadi tiga *layer*, yaitu *application layer, perception layer* dan *network layer* [3],[4].

Tantangan utama dalam pengimplementasian *Internet of Things (IoT)* adalah masalah keamanan, seperti privasi, otorisasi, verifikasi, kontrol akses, konfigurasi sistem, penyimpanan dan manajemen informasi. *IoT* rentan terhadap banyaknya serangan yang ditujukan untuk mengganggu komunikasi jaringan. Serangan keamanan dapat terjadi pada semua *layer IoT*, seperti serangan melalui komunikasi *WiFi*, *RFID, IEEE 802.15.4*/*ZigBee* dan *bluetooth*, serta *node* (sensor atau kontroler) pada *perception layer* yang berperan sebagai pengoleksi informasi [5].

Serangan *Denial of Service (DoS)* merupakan salah satu ancaman keamanan pada jaringan *IoT* [6]. *DoS* didefinisikan sebagai salah satu metode penyerangan yang dilakukan oleh *attacker* untuk menghabiskan sumber daya, seperti *bandwidth* dan meningkatkan konsumsi energi yang mengakibatkan sumber energi pada perangkat akan cepat habis [7].

Dalam penelitian [8], dijelaskan serangan *DoS* dapat dikelompokan menjadi dua kategori utama, yaitu (i) *Flooding Attack* didefinisikan sebagai serangan dengan teknik mengirimkan banyak paket kepada target dengan tujuan

agar fungsi *CPU*, memori dan *resource* pada jaringan berfungsi secara maksimal. (ii) *Logic Attack* didefinisikan sebagai serangan dengan mengambil keuntungan dari kelemahan yang telah ada pada sistem, sehingga menyebabkan sistem mengalami *malfunction*.

Pada penelitian[5] dan [9], membahas masalah keamanan pada n*ode* (sensor atau kontroler) menggunakan komunikasi *Radio Frequency (RF)* seperti *WiFi*, *RFID*, *IEEE 802.15.4*/*ZigBee* dan *bluetooth* yang umumnya menerapkan mekanisme *broadcast* untuk berkomunikasi satu sama lain. Mekanisme ini sulit untuk melindungi dari terjadinya serangan. *Node* pada *IoT* rentan terhadap berbagai jenis ancaman dan serangan, termasuk *capturing*, *eavesdropping* dan *tampering*. *Resource* yang terbatas pada *node*, dimanfaatkan dengan melakukan serangan *DoS*, seperti *flooding* yang berakibat kinerja sensor dan *bandwidth* berada pada kemampuan maksimalnya.

Pada penelitian lain [10], membahas tiga tipe serangan *DoS* pada *IoT*, yaitu *ICMP flood*, *SYN flood* dan *TCP flood*. Pada penelitian ini, serangan ditujukan pada *node IoT*. Hasil dari penelitian ini membandingkan hasil serangan berdasarkan parameter *CPU utility*, *memory utility, time* dan *packet loss rate*. Penelitian [11] membahas peracangan *Intrusion Detection System (IDS)* berbasis pengetahuan *(knowledge base)* pada *interface* berbeda menggunakan protokol *IEEE 802.15.4*, *WiFi*, *bluetooth*, dan *interface* lainnya. Serangan *DoS* dikategorikan berdasarkan sumber dan target serangan. Pada penelitian ini dilakukan perbandingan evaluasi hasil deteksi rancangan sistem terhadap sistem *IDS* lainnya.

Selanjutnya penelitian [6] dan [12], membahas bagaimana menerapkan mekanisme deteksi serangan menggunakan *Intrusion Detection System (IDS)* pada jaringan *IoT* menggunakan rule based, seperti *petri nets*, *state machine* dan *signature analysis*. Dalam penelitian ini *IDS* didistribusikan untuk menghindari masalah yang berkaitan dengan resource yang terbatas pada perangkat *IoT*. Dengan merujuk pada masing-masing penelitian sebelumnya, *rule based signature analysis* dapat dimanfaatkan untuk mendeteksi serangan *Denial of Service (DoS)* pada jaringan *Internet of Thing (IoT)*, selain itu *IDS* perlu didistribusikan untuk menghindari masalah yang berkaitan *resource* yang terbatas.

1.2 Tujuan

Adapun tujuan yang hendak dicapai dalam penelitian tugas akhir adalah sebagai berikut :

1. Mengenali pola paket serangan *Denial of Service (DoS)* pada jaringan *Internet of Things (IoT)*.
2. Mengimplementasikan *Intrusion Detection System (IDS)* pada jaringan *Internet of Things (IoT)* menggunakan *rule based signature analysis*.
3. Mengukur akurasi dan efektivitas deteksi serangan *Denial of Service (DoS)* terhadap *Intrusion Detection System (IDS)* dengan menerapkan *rule based signature analysis.*

1.3 Manfaat

Adapun manfaat yang dapat diambil dari penelitian tugas akhir adalah :

1. Dapat mengenali dan mendeteksi pola serangan *Denial of Service (DoS)* dengan menerapkan *rule based signature analysis* pada jaringan *Internet of Things (IoT)*.
2. Dapat digunakan sebagai alternatif metode keamanan pada jaringan *Internet of Things (IoT)* pada komunikasi *IEEE 802.15.4/ZigBee* dan *WiFi*.

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan sebelumnya, permasalahan utama yang akan dibahas pada penelitian ini yaitu :

1. Bagaimana mengenali dan mengidentifikasi pola serangan *Denial of Service (DoS)* pada jaringan *Internet of Things (IoT)* menggunakan *rule based signature analysis* pada komunikasi *IEEE 802.15.4/ZigBee* dan *WiFi*.
2. Bagaimana merancang dan cara kerja sistem pengamanan *Intrusion Detection System (IDS)* untuk mendeteksi serangan *Denial of Service (DoS*) menggunakan *rule based signature analysis* pada jaringan *Internet of Things (IoT).*

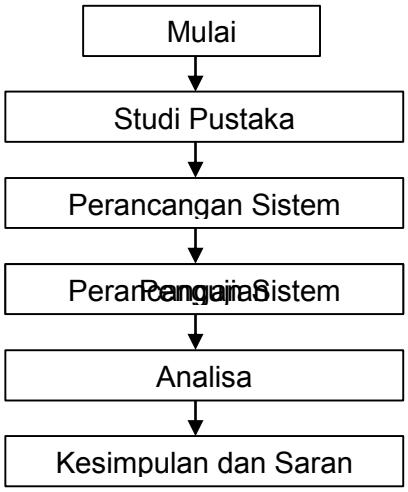
1.5 Batasan Masalah

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

1. Pengujian dilakukan pada komunikasi *IEEE 802.15.4/ZigBee* dan *WiFi*.
2. Pengujian dilakukan dengan serangan *Denial of Service (DoS)* kategori *TCP FIN flood* dan *zbassocflood/association flood*.
3. Pengujian dilakukan secara *offline*, menggunakan *dataset* yang sudah terekam (ter*capture*) berupa *network log connection* untuk lalu lintas data normal dan data serangan *Denial of Service (DoS)*.
4. Tidak membahas mengenai pencegahan terhadap serangan yang ada pada jaringan.
5. Metode yang digunakan untuk mengenali dan mendeteksi serangan adalah *rule based signature analysis*.
6. Sistem yang dibangun terdiri dari enam *end node*, dua *middleware* dan satu *server monitoring*.
7. Sensor yang digunakan pada *end node* terdiri dari *DHT-22, DHT-11, MQ-2, Soil moisture (FC28)* dan *water level (K-0135).*
8. Pada setiap *end node* terdiri dari satu sensor.

1.6 Metodologi Penelitian

Agar tujuan penelitian ini dapat tercapai berikut merupakan tapahan penelitian yang digunakan dalam penelitian tugas akhir :



1. Tahap Pertama (Studi Pustaka / *Literature*)

Tahap ini dilakukan dengan cara mengkaji dan mempelajari *literature* dan referensi berupa naskah ilmiah, buku, *internet* dan lain-lain yang dapat menunjang metodologi dan pendekatan yang akan diterapkan pada penelitian tugas akhir.

2. Tahap Kedua (Perancangan Sistem)

Tahap ini membahas mengenai proses bagaimana membangun sistem dengan menggunakan metode atau pendekatan tertetu. Menentukan perangkat keras, seperti tipe sensor, kontroler, perangkat lunak pendukung, jenis topologi untuk membangun jaringan *Internet of Things (IoT)*, kemudian bagaimana proses installasi dan konfigurasi sistem, serta implementasi *Intrusion Detection System (IDS)* menggunakan *rule based signature analysis*.

3. Tahap Ketiga (Pengujian)

Tahap ini merupakan tahap lanjutan dari proses perancangan yang telah dilakukan. Dengan melakukan pengujian berdasarkan metodologi penelitian dan penelitian sebelumnya sehingga didapatkan data hasil pengujian yang sesuai dengan batasan masalah dan parameter pengujian yang telah ditentukan untuk medapatkan hasil yang optimal.

4. Tahap Keempat (Analisa)

Hasil dari pengujian pada tahap sebelumnya, selanjutnya akan dianalisa dengan tujuan untuk mengetahui kekurangan pada hasil perancangan dan faktor penyebabnya sehingga dapat dilakukan pengembangan pada penelitian selanjutnya.

5. Tahap Kelima (Kesimpulan dan Saran)

Pada tahap ini akan dilakukan penarikan kesimpulan berdasarkan studi pustaka/*literature*, metodologi penelitian dan analisis hasil pengujian sistem. Kemudian beberapa saran dari penulis yang dapat dijadikan landasan untuk penelitian selanjutnya.

1.7 Sistematika Penelitian

Untuk memudahkan dalam proses penyusunan tugas akhir dan memperjelas konten dari setiap bab, maka dibuat suatu sistematika penulisan sebagai berikut :

BAB I. PENDAHULUAN

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

BAB II. TINJAUAN PUSTAKA

Bab ini berisi dasar teori dari penelitian tugas akhir terkait *Internet of Things (IoT)*, *Denial of Service (DoS)*, *Intrusion Detection System (IDS)*, *Rule Based Signature Analysis*, *Snort* serta teori lainnya yang berkaitan 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 ANALISIS

Bab ini menjelaskan hasil pengujian yang dilakukan serta analisis dari tiap data yang diperoleh dari hasil pengujian berdasarkan parameter yang telah ditentukan sebelumnya.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan tentang hasil penelitian yang dilakukan, serta menjawab setiap tujuan yang hendak dicapai seperti yang tercantum pada BAB 1 (Pendahuluan), serta saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things : A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision , architectural elements , and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[4] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context Aware Computing for The Internet of Things," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[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, pp. 10–28, 2017.

[6] 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.

[7] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer (Long. Beach. Calif).*, vol. 35, no. 10, pp. 54–62, 2012.

[8] D. Wang, L. He, Y. Xue, and Y. Dong, "Exploiting Artificial Immune systems to detect unknown DoS attacks in real-time," *Proc. - 2012 IEEE 2nd Int. Conf. Cloud Comput. Intell. Syst. IEEE CCIS 2012*, vol. 2, pp. 646–650, 2013.

[9] S. Ghildiyal, A. K. Mishra, A. Gupta, and N. Garg, "Analysis of Denial of Service (Dos) Attacks in Wireless Sensor Networks," *Int. J. Res. Eng. Technol.*, vol. 03, no. 22, pp. 140–143, 2014.

[10] L. Liang, K. Zheng, Q. Sheng, W. Wang, R. Fu, and X. Huang, “A denial of service attack method for iot system in photovoltaic energy system,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10394 LNCS, pp. 613–622, 2017.

[11] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, “Kalis - A System for Knowledge-Driven Adaptable Intrusion Detection for the Internet of Things,” *Proc. - Int. Conf. Distrib. Comput. Syst.*, pp. 656–666, 2017.

[12] D.J.A.Chandulal, D. K. N. Rao, and S. Akbar, “Intrusion Detection System Methodologies Based on Data Analysis,” *Found. Comput. Sci.*, vol. 5, no. 2, pp. 10–20, 2010.

[13] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future internet: The internet of things architecture, possible applications and key challenges,” in *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012*, 2012, pp. 257–260.

[14] A. Movaghar, “Intrusion Detection : A Survey Chapter 2 Intrusion Detection : A Survey,” no. January 2008, 2014.

[15] M. Gou, “Algorithms for String matching,” pp. 1–8, 2014.

[16] S. Jakka, “String Matching,” *English*, pp. 1–5, 2014.

[17] D. Wang, L. He, Y. Xue, and Y. Dong, “Exploiting Artificial Immune Systems to Detect Unknown DoS Attacks in Real-Time,” pp. 1–5, 1857.

[18] C.A.Winanto, “Deteksi Serangan Denial of Service Menggunakan Artificial Immune System,” Universitas Sriwijaya, 2017.

[19] Allot Communications, “DDoS Attack Handbook,” p. 20, 2017.

[20] B. Stelte and G. D. Rodosek, “Thwarting attacks on ZigBee-Removal of the KillerBee stinger,” *2013 9th Int. Conf. Netw. Serv. Manag.*, pp. 219 – 226, 2013.

[21] C. Azzi, “Vulnerability analysis and security framework for ZigBee communication in IoT,” 2016.

[22] Behrouz A. Forouzan, *TCP/IP Protocol Suite*. 2008.

[23] Ahmad Zaki, “Implementasi Jaringan Sensor Nirkabel Jarak Jauh Untuk Mengukur Kualitas Udara,” 2017.

[24] NXP Laboratories, “IEEE 802.15.4 Stack User Guide,” 2014.

[25] J. Cache, J. Wright, and V. Liu, *Hacking Wireless Exposed*. 2010.

[26] R. U. Rehman, *Introduction to Intrusion Detection and Snort*. 2003.

[27] Muhammad Reyhan Zalbina, *Implementasi Routing Pegasis pada Arduino dan XBee*. Palembang, 2015.

[28] B. N. Alhasnawi, “Wirelessly Controlled Smart home System,” vol. 13, no. 1, 2017.

[29] D. R. Keyes, “Water Sensor Module User’s Manual,” pp. 1–3, 2013.

[30] X. Fan, F. Susan, W. Long, and S. Li, “Security Analysis of Zigbee,” pp. 1–18, 2017.

[31] H. T. Elshoush and I. M. Osman, “Alert correlation in collaborative intelligent intrusion detection systems - A survey,” *Appl. Soft Comput. J.*, vol. 11, no. 7, pp. 4349–4365, 2011.