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

TUGAS AKHIR

Oleh :

HARI ACHMAD AULIA
09011181621120

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

PENCEGAHAN 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 :

HARI ACHMAD AULIA
09011181621120

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN

PENCEGAHAN 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 :

HARI ACHMAD AULIA
09011181621120

Indralaya, Mei 2021

Mengetahui,

Pembimbing I Tugas Akhir

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

Pembimbing II Tugas Akhir

Ahmad Heryanto, S.Kom., M.T.
NIP.198701222015041002

Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at

Tanggal : 30 April 2021

Tim Penguji :

Ketua : Ahmad Zarkasi, M.T.

Sekretaris I : Deris Stiawan, M.T., Ph.D., IPU.

Sekretaris II : Ahmad Heryanto, S.Kom., M.T.

Anggota I : Sarmayanta Sembiring, M.T.

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Hari Achmad Aulia

NIM : 09011181621120

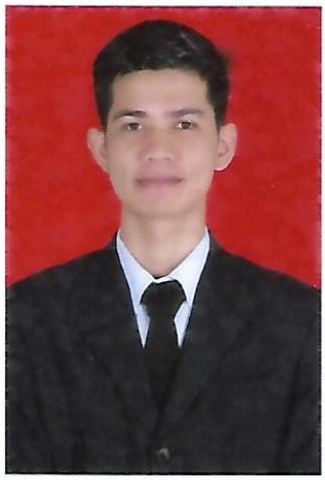
Program Studi : Sistem Komputer

Judul : Pencegahan Serangan Denial of Service Menggunakan Rule Based Signature Analysis Pada Jaringan Internet Of Things

Hasil Pengecekan *Software iThenticate / Turnitin* : 6%

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

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



Indralaya, Mei 2021

Hari Achmad Aulia
NIM. 09011181621120

HALAMAN PERSEMBAHAN

Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya. Dia mendapat (pahala) dari (kebajikan) yang dikerjakannya dan dia mendapat (siksa) dari (kejahatan) yang diperbuatnya. (Mereka berdoa), "Ya Tuhan kami, janganlah Engkau hukum kami jika kami lupa atau kami melakukan kesalahan. Ya Tuhan kami, janganlah Engkau bebani kami dengan beban yang berat sebagaimana Engkau bebankan kepada orang-orang sebelum kami. Ya Tuhan kami, janganlah Engkau pikulkan kepada kami apa yang tidak sanggup kami memikulnya. Maafkanlah kami, ampunilah kami, dan rahmatilah kami. Engkaulah pelindung kami, maka tolonglah kami menghadapi orang-orang kafir".

(QS. Al-Baqarah : 286)

Alhamdulillah, dengan izin Allah S.W.T beserta kesungguhan hati, akhirnya penelitian ini mampu diselesaikan, tugas akhir ini penulis persembahkan untuk :

1. Ibu (Ria Adel Gusti) dan Ayah (Hamdan) tercinta yang berjuang membesarkan, mendidik, dan selalu mengajarkan yang baik dari kecil hingga sekarang serta selalu memberikan do'a setiap saat sehingga penulis mampu menyelesaikan tugas akhir ini.
2. Almarhumah Enek (Anasiah), almarhumah Umi (Mardiah), Angah (Mardanis) dan Etek (Desy Adriyani) yang selalu memberikan motivasi dan dukungan apapun kepada penulis untuk melanjutkan dan meyelesaikan pendidikan.
3. Adik-adik tercinta (Rizki, Fajar Maulana, Farah Ayu Fatimah) yang selalu menjadi salah satu alasan penulis untuk menyelesaikan tugas akhir dan pendidikan sebagai motivasi untuk mereka.
4. Seluruh keluarga besar yang sudah memberikan bantuan dalam bentuk apapun kepada penulis hingga dapat menyelesaikan tugas akhir ini.

5. Dosen pembimbing I, Bapak Deris Stiawan, M.T., Ph.D. dan dosen pembimbing II, Bapak Ahmad Heryanto, S.Kom, M.T. yang telah membimbing dan mengarahkan penulis dalam menyelesaikan tugas akhir ini.
6. Dosen pembimbing akademik, Ibu Sri Desy Siswanti, S.T., M.T. yang selalu memberikan arahan dan motivasi setiap semester untuk menjalankan perkuliahan.
7. Seluruh teman-teman seperjuangan terkhusus kepada teman-teman kelas SK16A yang telah membantu penulis dari awal perkuliahan hingga dapat menyelesaikan tugas akhir ini.
8. Kakak-kakak, teman-teman dan adik-adik grup riset *Communication Network and Information Security* (COMNETS) yang telah membantu penulis menyelesaikan tugas akhir ini.
9. Kakak-kakak, teman-teman dan adik-adik keluarga besar Himpunan Mahasiswa Sistem Komputer (HIMASISKO) yang telah membantu penulis dari hingga dapat menyelesaikan tugas akhir ini.
10. Kakak-kakak, teman-teman dan adik-adik organisasi kedaerahan Persatuan Mahasiswa Tuah Sakato (PERMATO) yang sudah menjadi keluarga tempat berkeluh-kesah saat menjalani perkuliahan.
11. Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji dan syukur penulis selalu panjatkan atas kehadirat Allah Subhanahu Wata'ala yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul **"Pencegahan Serangan *Denial of Service* Menggunakan *Rule Based Signature Analysis* Pada Jaringan *Internet of Things*"**. Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad S.A.W beserta keluarga, sahabat dan para pengikutnya yang InshaAllah istiqomah hingga akhir zaman.

Selesainya penyusunan laporan Tugas Akhir ini tidak terlepas dari peran serta semua pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam menyusun Proposal Tugas Akhir ini.
2. Orangtua tercinta, yaitu Ibu Ria Adel Gusti dan Ayah Hamdan, serta saudara penulis, yaitu Rizki, Fajar Maulana dan Farah Ayu Fatimah, serta keluarga besar penulis yang tersayang.
3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Ibu Sri Desy Siswanti, S.T., M.T., selaku Pembimbing Akademik.
6. Bapak Deris Stiawan, M.T., Ph.D., IPU., selaku Dosen Pembimbing I Tugas Akhir.
7. Bapak Ahmad Heryanto, S.Kom., M.T., selaku Dosen Pembimbing II Tugas Akhir.
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.

9. Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Penulis menyadari dalam penyusunan laporan Tugas Akhir ini masih terdapat banyak kekurangan, karenanya penulis mengharapkan kritik dan saran untuk perbaikan. Semoga laporan Tugas Akhir ini dapat bermanfaat bagi siapa saja yang membacanya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Indralaya, Mei 2021

Penulis

Hari Achmad Aulia
NIM. 09011181621120

PENCEGAHAN SERANGAN *DENIAL OF SERVICE* MENGGUNAKAN *RULE BASED SIGNATURE ANALYSIS* PADA JARINGAN *INTENET OF THINGS*

Hari Achmad Aulia (0901181621120)

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

Email : achmadaulia27@gmail.com

ABSTRACT

Internet of Things (IoT) is a system that connects physical objects to one another via an internet connection, communicates by sending data without human assistance. No system is safe when connected to the internet. Denial of Service (DoS) attacks are one of the threats to IoT systems. Intrusion Detection Prevention System (IDPS) is an effort to protect IoT systems from DoS attacks. This research was conducted to prevent DoS attacks in the FIN Flood category. The first step before taking prevention is to detect packets that have the same signature as the attack rule. The attacks detected were DoS attacks in the FIN Flood category and Zbassocflood/Association Flood contained in the previous research dataset. Attack detection is carried out using Rule Based Signature Analysis. The detection results of the FIN Flood attack and Zbassocflood/Association Flood using Rule Based Signature Analysis and the results of the FIN Flood attack prevention have a very good level of accuracy, reaching 100%.

Keywords: *Internet of Things (IoT), Denial of Service (DoS), Intrusion Detection Prevention System (IDPS), FIN Flood, Zbassocflood/Association Flood.*

Mengetahui

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

Ketua Jurusan Sistem Komputer

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

PENCEGAHAN SERANGAN *DENIAL OF SERVICE* MENGGUNAKAN *RULE BASED SIGNATURE ANALYSIS* PADA JARINGAN *INTENET OF THINGS*

Hari Achmad Aulia (0901181621120)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : achmadaulia27@gmail.com

ABSTRAK

Internet of Things (IoT) merupakan sistem yang menghubungkan *physical object* satu sama lain melalui koneksi internet, melakukan komunikasi dengan mengirimkan data tanpa bantuan manusia. Tidak ada sistem yang aman ketika terhubung ke internet. Serangan *Denial of Service (DoS)* merupakan salah satu ancaman bagi sistem *IoT*. *Intrusion Detection Prevention System (IDPS)* merupakan salah satu upaya untuk melindungi sistem *IoT* dari serangan *DoS*. Penelitian ini dilakukan untuk mencegah serangan *DoS* kategori *FIN Flood*. Langkah awal sebelum melakukan pencegahan adalah melakukan deteksi terhadap paket yang memiliki *signature* yang sama dengan *rule* serangan. Serangan yang dideteksi adalah serangan *DoS* kategori *FIN Flood* dan *Zbassocflood/Association Flood* yang terdapat pada dataset penelitian sebelumnya. Deteksi serangan dilakukan menggunakan *Rule Based Signature Analysis*. Hasil deteksi serangan *FIN Flood* dan *Zbassocflood/Association Flood* menggunakan *Rule Based Signature Analysis* dan hasil pecegahan serangan *FIN Flood* yang dilakukan memiliki tingkat akurasi yang sangat baik, yaitu mencapai 100%.

Kata kunci: *Internet of Things (IoT), Denial of Service (DoS), Intrusion Detection Prevention System (IDPS), FIN Flood, Zbassocflood/Association Flood.*

Mengetahui

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

Ketua Jurusan Sistem Komputer

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

DAFTAR ISI

Halaman

BAB II TINJAUAN PUSTAKA

BAB III METODOLOGI PENELITIAN

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dengan kemajuan teknologi yang terus-menerus sebagai inovasi potensial, *Internet of Things (IoT)* kini semakin berkembang sebagai jaringan komputasi global di mana semua orang dan semua hal akan terhubung ke Internet [1]. Paradigma *Internet of Things (IoT)* diperkenalkan oleh Kevin Ashton pada tahun 1998. Kevin Ashton menyatakan bahwa *IoT* adalah komputer yang tahu segalanya tentang berbagai hal dan menggunakan data yang mereka kumpulkan tanpa bantuan manusia kemudian saling berhubungan dengan internet [2]. *Internet of things (IoT)* adalah *internetworking* dari *physical objects* yang tertanam dalam elektronik, perangkat lunak, sensor, aktuator, dan konektivitas jaringan yang memungkinkan perangkat-perangkat ini untuk mengumpulkan dan bertukar data [3]. Masalah keamanan, seperti privasi, otorisasi, verifikasi, kontrol akses, konfigurasi sistem, penyimpanan informasi, dan manajemen, adalah tantangan utama dalam lingkungan *IoT* [4].

Serangan *Denial of Service (DoS)* adalah salah satu ancaman keamanan pada jaringan *IoT*. *DoS* didefinisikan sebagai salah satu metode serangan oleh penyerang untuk menghabiskan sumber daya, seperti *bandwidth* dan meningkatkan konsumsi energi yang menghasilkan sumber energi pada perangkat akan cepat habis [5]. Serangan *DoS* diwujudkan dengan membanjiri target dengan lalu lintas, atau mengirimkannya informasi untuk memicu masalah. Ini adalah salah satu metode serangan *cyber* paling populer dalam keamanan jaringan [6]. Untuk melindungi jaringan dari serangan *DoS*, skema penyerangan diselidiki dengan hati-hati terlebih dahulu, kemudian skema perlindungan untuk mencegah serangan perlu dikembangkan untuk mengamankan sistem *IoT* [7].

Salah satu konsep yang paling baik dalam keamanan informasi adalah pendekatan *defense-in-depth* yang memanfaatkan desain struktural *multilayer*, di

mana *firewall*, alat penilaian kerentanan (anti-virus), dan *IDPS (Intrusion Detection and Prevention Systems)* digunakan untuk mencegah segala upaya penyerangan pada sistem jaringan dan *server* [8]. *IDPS* terdiri dari serangkaian mekanisme perlindungan yang bertujuan untuk mendeteksi, mencatat, dan mencegah potensi ancaman secara *real-time* [9].

Rule Based Signature Analysis adalah mekanisme ini mengidentifikasi pola unik serangan *DoS* yang diketahui dan membedakannya dari pola normal, pola serangan tersebut didefinisikan sebagai *rule* serangan. Berdasarkan diferensiasi ini, *database rule* serangan yang diketahui dibangun dan selanjutnya digunakan untuk mengidentifikasi keberadaan aktivitas berbahaya di jaringan [10]. Pendekatan ini memberikan tingkat akurasi yang tinggi [9].

Pada penelitian [11], membahas tentang pengenalan pola serangan *TCP FIN Flood dan Zbassocflood/Association Flood* pada jaringan *Internet of Things (IoT)* menggunakan metode *Rule Based Signature Analysis*. Penelitian tersebut dilakukan pada komunikasi *WiFi* dan *IEEE 802.15.4*. Pengujian dilakukan dengan menggunakan dua parameter *Intrusion Detection System (IDS)*, pengujian pertama menggunakan *Snort* dan pengujian kedua mengunakan metode *Rule Based Signature Analysis*. Pengujian menggunakan *Snort* bertujuan sebagai pembanding dari pengujian menggunakan metode *Rule Based Signature Analysis*. Hasil dari pengujian tersebut menunjukkan bahwa pengujian menggunakan metode *Rule Based Signature Analysis* lebih baik, dengan tingkat persentase rata-rata akurasi 99,9199%, sedangkan *Snort* hanya memiliki tingkat persentase rata-rata akurasi 26,3268%.

Merujuk dari latar belakang dan penelitian sebelumnya, penelitian ini merupakan lanjutan dari penelitian [11] dengan menggunakan metode yang sama. Penelitian ini akan membahas tentang pencegahan serangan *Denial of Service (DoS)* pada jaringan *Internet of Things (IoT)* yang diberi judul **"Pencegahan Serangan *Denial of Service* Menggunakan *Rule Based Signature Analysis* Pada Jaringan *Internet of Things*"**.

1.2 Tujuan

Tujuan dari penulisan proposal tugas akhir ini adalah sebagai berikut :

1. Mengimplementasikan *rules* serangan yang telah ditemukan pada penelitian sebelumnya ke dalam *Intrusion Detection Sistem (IDS)* untuk mendeteksi serangan di jaringan *Internet of Things*.
2. Mencegah serangan yang terdeteksi oleh *Intrusion Detection Sistem (IDS)* dengan menerapkan *Intrusion Prevention Sistem (IPS)* di jaringan *Internet of Things*.
3. Mengukur efektifitas dan akurasi dari penerapan *Intrusion Prevention Sistem (IPS)*.

1.3 Manfaat

Manfaat dari penulisan proposal tugas akhir ini adalah sebagai berikut :

1. Dapat mencegah serangan yang telah terdeteksi menggunakan *Rule Based Signature Analysis* pada jaringan *Internet of Things*.
2. Dapat menjadi salah satu proteksi untuk serangan *Denial of Service* di jaringan *Internet of Things*.

1.4 Rumusan Masalah

Berdasarkan latar belakang dan penelitian sebelumnya, masalah yang akan di bahas pada penelitian ini adalah :

1. Bagaimana mengimplementasikan *rule*s yang telah ditemukan sebelumnya pada *Intrusion Detection System* untuk mendeteksi serangan.
2. Bagaimana mencegah serangan yang telah terdeteksi oleh *Intrusion Detection System (IDS)* dengan menerapkan *Intrusion Prevention System (IPS)*.

3. Bagaimana mengukur efektifitas dan akurasi dari penerapan *Intrusion Prevention System (IPS).*

1.5 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut :

1. Data yang digunakan pada penelitian ini diperoleh dari penelitian sebelumnya.
2. Penelitian ini fokus pada serangan *Denial of Service (DoS)* kategori *TCP FIN Flood* dan *Zbassocflood/Association Flood*.
3. Metode yang digunakan untuk mencegah serangan *Denial of Service (DoS)* pada jaringan *Internet of Things (IoT)* adalah *Rule Based Signature Analysis*.
4. *Rules* yang digunakan untuk mendeteksi serangan *Denial of Service (DoS)* diperoleh dari hasil pengenalan pola serangan pada penelitian sebelumnya.
5. Penelitian ini hanya akan mencegah salah satu dari serangan yang dideteksi, yaitu serangan *Denial of Service (DoS)* kategori *TCP FIN Flood.*

1.6 Metodologi Penelitian

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

1. Metode Literatur

Dalam tahap ini penulis mencari informasi yang diperlukan melalui media pembelajaran seperti jurnal ilmiah, buku, internet, serta artikel-artikel terkait yang mendukung penulisan laporan Tugas Akhir ini.

2. **Metode Konsultasi**

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

3. **Metode Pengumpulan Data**

Dalam tahap ini, pengumpulan data dilakukan dengan meminta data penelitian sebelumnya yang berjudul "Deteksi Serangan *Denial of Service* Menggunakan *Rule Based Signature Analysis* pada *Jaringan Internet of Things*".

4. **Metode Observasi**

Metode ini dilakukan dengan cara mengamati, mencatat, dan menganalisa terhadap data yang diperoleh.

5. **Metode Perancangan *Software***

Pada tahap ini akan dilakukan perancangan serta pembuatan sistem *(software) IDPS* untuk mendeteksi serangan *Denial of Service (DoS)* kategori *TCP FIN Flood* dan *Zbassocflood/Association Flood* dan memilih tindakan antara *allow* atau *denied* ketika ada paket *FIN Flood.*

6. **Metode Analisa dan Kesimpulan**

Hasil dari pengujian pada metode pengujian kemudian dianalisa dengan tujuan untuk mengetahui kekurangan pada hasil perancangan dan faktor penyebabnya, sehingga dapat digunakan untuk pengembangan pada penelitian selanjutnya dan dibuat kesimpulan dari hasil penelitian.

1.7 SISTEMATIKA PENULISAN

Adapun sistematika penulisan dalam laporan Tugas Akhir ini adalah sebagai berikut :

1. **Bab I. Pendahuluan**

   Pada Bab I akan berisikan latar belakang masalah, tujuan dan manfaat serta metodologi penelitian dan sistemaika penulisan.

2. **Bab II. Tinjauan Pustaka**

   Pada Bab II akan berisi dasar teori dari pendeteksian, pencegahan, metode-metode yang di gunakan serta *software* yang di gunakan dalam menjalankan penelitian tugas akhir ini.

3. **Bab III. Metodologi Penelitian**

   Pada Bab III akan membahas tentang metodologi penelitian sistem pencegahan serangan *Denial of Service (DoS)* menggunakan *Rule Based Signature Analysis* pada jaringan *Internet of Things*.

4. **Bab IV. Hasil dan Analisa**

   Pada Bab IV membahas hasil dan analisa dari proses implementasi perangkat lunak *(IDPS)* yang telah dirancang untuk melakukan deteksi dan pencegahan terhadap serangan *Denial of Service (DoS)* pada jaringan *Internet of Things*.

5. **Bab V. Kesimpulan dan Saran**

   Pada Bab V berisi kesimpulan dari bab-bab yang sudah dicantumkan mengenai hasil dari pengimplementasian *Rule Based Signature Analysis* dalam membangun *IPS* untuk mencegah serangan *Denial of Service* pada jaringan *Internet of Things*. Pada bab ini juga akan berisi saran yang diharapkan dapat digunakan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] M. U.Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A Review on Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 113, no. 1, pp. 1–7, 2015, doi: 10.5120/19787-1571.

[2] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," *2016 3rd Int. Conf. Electron. Des. ICED 2016*, pp. 321–326, 2017, doi: 10.1109/ICED.2016.7804660.

[3] M. Sain, Y. J. Kang, and H. J. Lee, "A Survey on Privacy and Security in Internet of Things," *Int. J. Innov. Eng. Technol.*, vol. 8, no. 1, pp. 699–704, 2017, doi: 10.21172/ijiet.81.017.

[4] 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, doi: 10.1016/j.jnca.2017.04.002.

[5] 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, doi: 10.3991/ijoe.v15i07.9848.

[6] 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, doi: 10.1007/978-3-319-64701-2_48.

[7] . V. K. B., S. L. Joshi, and S. H. Barshikar, "A Survey on Internet of Things," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 12, pp. 492–496, 2018, doi: 10.26438/ijcse/v6i12.492496.

[8] W. Bul'ajoul, A. James, and S. Shaikh, "A New Architecture for Network Intrusion Detection and Prevention," *IEEE Access*, vol. 7, pp. 18558–18573,

2019, doi: 10.1109/ACCESS.2019.2895898.

[9] P. I. Radoglou Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the Internet of Things: Challenges, threats and solutions," *Internet of Things*, vol. 5, pp. 41–70, 2019, doi: 10.1016/j.iot.2018.11.003.

[10] K. Zeb, O. Baig, and M. K. Asif, "DDoS attacks and countermeasures in cyberspace," *2015 2nd World Symp. Web Appl. Networking, WSWAN 2015*, 2015, doi: 10.1109/WSWAN.2015.7210322.

[11] D. Wahyudi, "Deteksi serangan denial of service menggunakan rule based signature analysis pada jaringan internet of things," 2018.

[12] C. Le Zhong, Z. Zhu, and R. G. Huang, "Study on the IOT architecture and gateway technology," *Proc. - 14th Int. Symp. Distrib. Comput. Appl. Business, Eng. Sci. DCABES 2015*, pp. 196–199, 2016, doi: 10.1109/DCABES.2015.56.

[13] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, "IoT architecture challenges and issues: Lack of standardization," *FTC 2016 - Proc. Futur. Technol. Conf.*, no. December, pp. 731–738, 2017, doi: 10.1109/FTC.2016.7821686.

[14] W. Goralski, *The Illustrated Network*. Elsevier, 2017.

[15] G. Shi and K. Li, *Signal Interference in WiFi and ZigBee Networks*. 2017.

[16] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 816–829, 2016, doi: 10.1109/JIOT.2016.2516102.

[17] T. Savić and M. Radonjic, "WSN architecture for smart irrigation system," *2018 23rd Int. Sci. Conf. Inf. Technol. IT 2018*, vol. 2018-Janua, pp. 1–4, 2018, doi: 10.1109/SPIT.2018.8350859.

[18] B. Fan, "Analysis on the Security Architecture of ZigBee Based on IEEE

802.15.4," *Proc. - 2017 IEEE 13th Int. Symp. Auton. Decentralized Syst. ISADS 2017*, pp. 241–246, 2017, doi: 10.1109/ISADS.2017.23.

[19] K. Lüke, J. Walther, and D. Wäldchen, *Innovations for Community Services*, vol. 863. Springer International Publishing, 2018.

[20] K. N. Mallikarjunan, K. Muthupriya, and S. M. Shalinie, "A survey of distributed denial of service attack," *Proc. 10th Int. Conf. Intell. Syst. Control. ISCO 2016*, 2016, doi: 10.1109/ISCO.2016.7727096.

[21] Allot Communications, "DDoS Attack Handbook," p. 20, 2017.

[22] T. Zitta, M. Neruda, and L. Vojtech, "The security of RFID readers with IDS/IPS solution using Raspberry Pi," *2017 18th Int. Carpathian Control Conf. ICCC 2017*, pp. 316–320, 2017, doi: 10.1109/CarpathianCC.2017.7970418.

[23] C. V. der V. and R. A. Nureni Ayofe Azeez, Taiwo Mayowa Bada, Sanjay Misra, Adewole Adewumi, "Intrusion Detection and Prevention Systems: An Updated Review," in *Data Management, Analytics and Innovation*, 2020, pp. 685–696.

[24] C. Turner, R. Jeremiah, D. Richards, and A. Joseph, "A Rule Status Monitoring Algorithm for Rule-Based Intrusion Detection and Prevention Systems," *Procedia Comput. Sci.*, vol. 95, pp. 361–368, 2016, doi: 10.1016/j.procs.2016.09.346.

[25] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of Service Defence for Resource Availability in Wireless Sensor Networks," *IEEE Access*, vol. 6, no. c, pp. 6975–7004, 2018, doi: 10.1109/ACCESS.2018.2793841.

[26] W. A. Jabbar *et al.*, "Design and Fabrication of Smart Home with Internet of Things Enabled Automation System," *IEEE Access*, vol. 7, pp. 144059–144074, 2019, doi: 10.1109/ACCESS.2019.2942846.

[27] H. Ouldzira, A. Mouhsen, H. Lagraini, M. Chhiba, A. Tabyaoui, and S.

Amrane, “Remote monitoring of an object using a wireless sensor network based on NODEMCU ESP8266,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 16, no. 3, pp. 1154–1162, 2019, doi: 10.11591/ijeecs.v16.i3.pp1154-1162.

[28] M. Hatti and H. Ed, *Lecture Notes in Networks and Systems 35 Artificial Intelligence in Renewable Energetic Systems*, no. January. 2018.

[29] X. Bajrami and I. Murturi, “An efficient approach to monitoring environmental conditions using a wireless sensor network and NodeMCU,” *Elektrotechnik und Informationstechnik*, vol. 135, no. 3, pp. 294–301, 2018, doi: 10.1007/s00502-018-0612-9.

[30] D. Aziz, “Webserver Based Smart Monitoring System Using ESP8266 Node MCU Module,” *Int. J. Sci. Eng. Res.*, vol. 9, no. 6, p. 801, 2018.

[31] A. Gautam, G. Verma, S. Qamar, and S. Shekhar, “Vehicle Pollution Monitoring, Control and Challan System Using MQ2 Sensor Based on Internet of Things,” *Wirel. Pers. Commun.*, vol. 116, no. 2, pp. 1071–1085, 2021, doi: 10.1007/s11277-019-06936-4.

[32] A. H. B, M. M. Gaber, and E. Elyan, “Engineering Applications of Neural Networks: 17th International Conference, EANN 2016, Aberdeen, UK, September 2-5, 2016, Proceedings,” *17th Int. Conf. EANN 2016, Aberdeen, UK, Sept. 2-5, 2016, Proc.*, vol. 629, pp. 3–17, 2016, doi: 10.1007/978-3-319-44188-7.

[33] I. Ghafir, V. Prenosil, J. Svoboda, and M. Hammoudeh, “A survey on network security monitoring systems,” *Proc. - 2016 4th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2016*, pp. 77–82, 2016, doi: 10.1109/W-FiCloud.2016.30.

[34] W. Park and S. Ahn, “Performance Comparison and Detection Analysis in Snort and Suricata Environment,” *Wirel. Pers. Commun.*, vol. 94, no. 2, pp. 241–252, 2017, doi: 10.1007/s11277-016-3209-9.

[35] O. K. Mondher Essid, Farah Jemili, “Distributed Architecture of Snort IDS

in Cloud Environment," in *Intelligent Systems Design and Applications*, 2019, pp. 100–111.

[36] R. Mehmood and A. Selwal, *Fingerprint biometric template security schemes: Attacks and countermeasures*, vol. 597. 2020.

[37] K. Wong, C. Dillabaugh, N. Seddigh, and B. Nandy, "Enhancing Suricata intrusion detection system for cyber security in SCADA networks," *Can. Conf. Electr. Comput. Eng.*, pp. 1–5, 2017, doi: 10.1109/CCECE.2017.7946818.

[38] D. A. Bhosale and V. M. Mane, "Comparative study and analysis of network intrusion detection tools," *Proc. 2015 Int. Conf. Appl. Theor. Comput. Commun. Technol. iCATccT 2015*, pp. 312–315, 2016, doi: 10.1109/ICATCCT.2015.7456901.

[39] F. Desprez, "Preface," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10104 LNCS, no. September, pp. VII–VIII, 2017, doi: 10.1007/978-3-319-58943-5.

[40] S. I. Hakak, A. Kamsin, P. Shivakumara, G. A. Gilkar, W. Z. Khan, and M. Imran, "Exact String Matching Algorithms: Survey, Issues, and Future Research Directions," *IEEE Access*, vol. 7, pp. 69614–69637, 2019, doi: 10.1109/ACCESS.2019.2914071.

[41] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *IEEE Access*, vol. 7, pp. 51691–51713, 2019, doi: 10.1109/ACCESS.2019.2908998.

[42] G. Wang, J. Chen, and L. T. Yang, *and Anonymity in Computation, Communication, and Storage*, vol. 1. Springer International Publishing, 2018.