KLASIFIKASI SERANGAN UDP FLOOD PADA JARINGAN INTERNET OF THINGS (IOT) MENGGUNAKAN METODE SUPPORT VECTOR MACHINE (SVM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

BUDIMAN ALFIAN

09011381823094

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

HALAMAN PENGESAHAN

KLASIFIKASI SERANGAN UDP FLOOD PADA JARINGAN INTERNET OF THINGS (IOT) MENGGUNAKAN METODE SUPPORT VECTOR MACHINE (SVM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

BUDIMAN ALFIAN
09011381823094

Palembang, 13 Januari 2023

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 20 Desember 2022

Tim Penguji :

1. **Ketua** : **Sarmayanta Sembiring, M.T.**
2. **Sekretaris** : **Iman Saladin B. Azhar, S.Kom., M.MSI**
3. **Penguji** : **Huda Ubaya, M.T**
4. **Pembimbing** : **Deris Stiawan, M.T., Ph.D.**

Mengetahui, 13/1/23

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Budiman Alfian

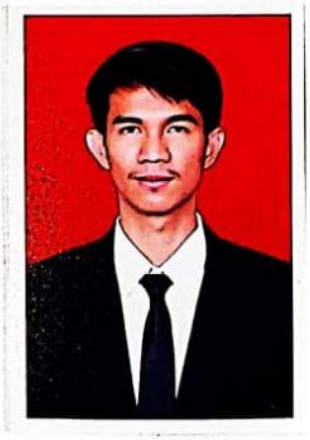
NIM : 09011381823094

Judul : Klasifikasi Serangan *UDP Flood* pada Jaringan *Internet of Things* (*IoT*) menggunakan Metode *Support Vector Machine* (*SVM*)

Hasil Pengecekan Software iThenticate/Turnitin : 17%

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

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



Palembang, Januari 2023

Budiman Alfian

NIM. 09011381823094

HALAMAN PERSEMBAHAN

“Definisi dari kata kuat itu bukan berarti tidak pernah dan tidak boleh menangis. Tetapi, orang yang kuat itu adalah orang yang terus beristikamah di jalan Allah ketika menghadapi segala ujian dan godaan.”

(Penulis, Budiman Alfian)

Skripsi ini kupersembahkan untuk :

Kedua Orang Tuaku.
(Jakfar dan Nikmawati)

Keluarga Besarku.
(ABU GETA dan RAHMAN YAVA)

Teman – temanku.
(Sistem Komputer 2018)

Dan Almamaterku.
(Universitas Sriwijaya)

“Jangan biarkan rintangan kecil menghalangi jalan menuju kemenangan. Ingatlah bahwa Anda lebih kuat dari tantangan yang dihadapi”
(Cristiano Ronaldo)

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur atas kehadirat Allah SWT yang telah memberikan rahmat dan karunianya sehingga penulis dapat menyelesaikan proposal Tugas Akhir yang berjudul "**Klasifikasi Serangan *UDP FLOOD* pada Jaringan *Internet of Things* (IoT) menggunakan Metode *Support Vector Machine* (SVM)"**

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

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

1. Allah SWT yang telah memberikan rahmat serta karunia-Nya sehingga penulis dapat menyelesaikan Proposal Tugas Akhir ini dengan baik.
2. Kepada Orang tua, Saudara, dan Keluarga Besar yang selalu mendoakan dan memberikan motivasi serta dukungan kepada penulis.
3. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Firdaus, M.Kom. selaku Dosen Pembimbing Akademik.
5. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran serta motivasi untuk penulis dalam penyusunan Tugas Akhir ini.

6. Mba Sari dan Mba Renny selaku Admin Jurusan Sistem Komputer yang telah membantu dalam melancarkan proses administrasi.
7. Garinnang Baiduri Salasa selaku teman saya dari awal kuliah sampai sekarang.
8. M. Rifqi Abiyyu Ariq dan Christoper Marlo selaku teman seperjuangan dalam penelitian serta membantu dalam masa sulit selama pengerjaan Tugas Akhir.
9. Febi Rusmiati selaku kating yang selalu membantu saya dari awal perkuliahan hingga bisa mendapatkan gelar S.Kom.
10. Aqila Luqman Hakim, M. Hafiz, Muhammad Chendy Maulana dan Adinda Nur Ramadiyah selaku teman saya yang selalu mesupport saya.
11. A Josman Pratama, Ronnie Radhitya Raffi, Ageng Raharjo, dan Muhammad Arief Saifullah selaku asisten di Center Of Excellence (CoE) dan Tri Shena Orivia Pasin dan Tarissa Fitriani selaku teman grup riset di Lab Communication Network and Information Security (COMNETS) Universitas Sriwijaya serta teman dekat dalam masa pengerjaan Tugas Akhir.
12. Teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2018.

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

Palembang, Januari 2023
Penulis,

Budiman Alfian
NIM. 09011381823094

KLASIFIKASI SERANGAN UDP FLOOD PADA JARINGAN INTERNET OF THINGS (IOT) MENGGUNAKAN METODE SUPPORT VECTOR MACHINE (SVM)

BUDIMAN ALFIAN (09011381823094)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : budimanalfian@gmail.com

ABSTRAK

Internet of things (IoT) adalah jaringan perangkat yang dapat terhubung ke internet. Serangan *Denial of Service (DoS)* pada *IoT* adalah serangan yang menggunakan permintaan layanan yang wajar untuk mendapatkan komputasi dan sumber daya jaringan yang berlebihan dan mengakibatkan pengguna yang sah tidak bisa mengaksesnya. Salah satu serangan *Denial of Service* adalah *User Datagram Protocol (UDP)* yang merupakan bentuk umum serangan *Denial of Service (DoS),* di mana cara kerjanya adalah *node* jahat memalsukan sejumlah besar identitas palsu, yaitu *spoofing Internet Protocol (IP)*. Pada penelitian ini akan di lakukan klasifikasi serangan UDP Flood. Didapatkan hasil klasifikasi Support Vector Machine *kernel sigmoid* menggunakan data *split training* 80% dan *testing* 20% menunjukan hasil akurasi sebesar 99.7%, presisi sebesar 5.7%, recall sebesar 100% dan F1 – score sebesar 10.8%. Untuk data *Split training* 70% dan *Testing* 30% menghasilkan akurasi sebesar 99.7%, presisi sebesar 6.2%, recall 100%, dan F1 – score sebesar 11.8 %. Dan untuk data *Split training* 60% dan *Testing* 40% memperlihatkan hasil akurasi sebesar 99.7%, presisi sebesar 6.2%, recall sebesar 100% dan F1 – Score sebesar 11.8%.

Kata Kunci : Klasifikasi, *Denial of Service, UDP Flood, Support Vector Machine*

Palembang, 12 Januari 2023

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

CLASSIFICATION OF UDP FLOOD ATTACKS ON THE INTERNET OF THINGS (IOT) NETWORK USING SUPPORT VECTOR MACHINE (SVM) METHOD

BUDIMAN ALFIAN (09011381823094)

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

Email : budimanalfian@gmail.com

ABSTRACT

The Internet of things (IoT) is a network that can connect any device to the internet. Denial of Service (DoS) attacks on IoT use reasonable service requests to gain excessive processing and network resources and prevent legitimate users from accessing them. One of the Denial of Service attacks is the User Datagram Protocol (UDP) which is a common form of Denial of Service (DoS) attack, where it works by impersonating large number of fake identities with malicious node, i.e. Internet Protocol (IP) spoofing. In this research, the classification of UDP Flood attacks will be carried out. The results of the Sigmoid Kernel Support Vector Machine classification using 80% split training data and 20% testing show an accuracy of 99.7%, a precision of 5.7%, a recall of 100%, and an F1 – score of 10.8%. For Split training data 70% and Testing 30% produce an accuracy of 99.7%, precision of 6.2%, recall of 100%, and F1 – a score of 11.8%. And for Split training data 60% and Testing 40% show results of accuracy of 99.7%, precision of 6.2%, recall of 100%, and F1 – Score of 11.8%.

Keywords : *Classification, Denial of Service, UDP Flood, Support Vector Machine*

Palembang, 13 Januari 2023

Acknowledged,

Head of Computer System Department	**Supervisor**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era revolusi industri saat ini (4*IR* atau Industri 4.0), dunia digital memiliki kekayaan data, seperti Data *Internet of Things (IoT)*, data keamanan siber, data seluler, data bisnis, data media sosial, data kesehatan,dan lainnya[1]. *Internet Of Things* (IoT) sendiri adalah konsep di mana suatu objek digunakan pada teknologi – teknologi contohnya seperti sensor dan software tujuannya adalah untuk berkomunikasi, mengendalikan, menguhubungkan, dan mengubah data menggunakan perangkat lain selama terhubung pada jaringan internet. *Internet of Things* juga memiliki kaitan yang sangat erat dengan nama *machine-to-machine* atau M2M. Akan tetapi, keamanan pada IoT mendapat berbagai resiko akibat serangan *cyber* yang dapat menyerang perangkat IoT target dengan menggunakan berbagai serangan *Denial of Service*[2]. Berbagai bentuk serangan yang bisa menyebabkan efek yang signifikan pada router adalah UDP *(User Datagram Protocol*). UDP *Flood* adalah jenis serangan menggunakan protocol UDP dengan menurunkan sambungan (*connectionless)* untuk menyerang target[3]. Serangan UDP *Flood* pada *DoS* adalah metode serangan yang menyebabkan penolakan layanan berbasis host. Itu terjadi karena ketika penyerang mengirim paket *UDP* ke port acak pada sistem korban, menyebabkan tanggapan dikirim ke alamat IP palsu[4].

Algoritma *Machine learning* telah dipergunakan secara luas di berbagai aplikasi dan area. Untuk menyesuaikan model pembelajaran mesin ke dalam masalah yang berbeda, parameter hipernya harus disetel. Dan memilih konfigurasi hyper-parameter terbaik untuk model *machine learning* memiliki dampak langsung pada performa model. Ini sering membutuhkan pengetahuan mendalam tentang algoritme pembelajaran mesin dan teknik optimasi hyper-parameter yang tepat.

Meskipun beberapa teknik optimasi otomatis ada, mereka memiliki keunggulan dan kelemahan yang berbeda ketika diterapkan pada berbagai jenis masalah[5]. *Machine Learning* digunakan untuk mendeteksi dan klasifikasi pada penelitian sebelumnya[6]. Salah satunya adalah penggunaan algoritma Support Vector Machine (SVM). Algoritma Support Vector Machine adalah teknik supervised learning yang menentukan hyperplanes terbaik agar dapat memisahkan kelas yang telah diberikan.

Pada penilitan[7] menggunakan Algoritma Support Vector Machine untuk melakukan deteksi dan klasifikasi pada DDoS atau DoS. Dimana pada penelitian ini, metode SVM, KNN, dan RF untuk mengetahui hasil performa terbaik dari gabungan algoritma dan metode yang digunakan. Dan dari pengujian didapatkan hasil bahwa algoritma SVM menghasilkan tingkat akurasi paling baik yaitu 99.08% dibandingkan dengan gabungan kedua metode lainnya.

Penelitian berikut [8], menjelaskan tentang dataset *UDP Flood Attack Pattern on Internet of Things Network* yang dibuat oleh *Communication Network and Information Security* (COMNETS) Universitas Sriwijaya, terdapat pola serangan *UDP Flooding* yang terjadi pada dataset tersebut..

Berdasarkan penjelasan diatas, penulis akan membahas mengenai klasifikasi Serangan UDP Flood pada jaringan Internet of Thinf (Iot) menggunakan algoritma Support Vector Machine (SVM).

1.2 Perumusan Masalah

Perumusan masalah dalam penelitian ini, yaitu :

1. Bagaimana cara klasifikasi terhadap data serangan *UDP Flood* dan data normal pada *Internet of Things* ?

2. Berapa hasil performa tingkat akurasi, presisi, recall, dan f1-score pada algoritma SVM menggunakan kernel sigmoid ?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini, yaitu :

1. Dataset yang dipakai pada penelitan ini berasal yang bersumber dari *GitHub Communciation Network and Information Security Research Group* (COMNETS)
2. Data yang di uji pada peneltian ini antara lain data serangan *UDP Flood* dan data normal

3. Algoritma yang digunakan untuk mengklasifikasikan serangan *UDP Flood* dan data normal ialah algoritma *Support Vector Machine* (SVM)

4. Pada riset ini tidak membahas sistem pencegahan serangan *UDP Flood* pada (IoT) *Internet of Things*

1.4 Tujuan

Tujuan dari penelitian ini, ialah:

1. Menerapkan Algoritma *Support Vector Machine* untuk mengklasifikasi data serangan *UDP Flood* dan data normal pada jaringan *Internet of Things*

2. Mengukur tingkat performa akurasi, presisi, recall dan f1 – score terhadap kinerja pengklasifikasian algoritma *Support Vector Machine* menggunkan kernel *Sigmoid* dan Menguji pengukuran hasil akurasi dari metode yang digunakan dengan *test train split dataset 40% test, 60% train, 30% test, 70% train,* dan *20% test, 80% train.*

1.5 Manfaat

Manfaat dari penelitian ini, yaitu:

1. Dapat mengklasifikasi data normal dan data serangan *UDP Flood* pada jaringan *Internet of Things* dengan menggunakan algoritma *Support Vector Machine*

2. Dapat menvalidasi kernel sigmoid dalam mengingkatkan performa akurasi, presisi, recall, dan f1-score

1.6 Metodologi Penelitian

Metodologi dalam penelitian ini melalui beberapa tahapan yaitu:

1. Tahapan Pertama (Study Pustaka / Literatur)

   Tahapan ini dilakukan dengan mencari dan mengumpulkan refernsi berupa literature dari beberapa sumber ilmiah seperti *journal*, *paper*, buku dan internet mengenai topik penelitian yang di lakukan.

2. Tahapan Kedua (Pengolahan Data)

   Tahapan ini membahas tentang proses ekstraksi data atau merubah format data yang diperoleh yaitu format *.pcap* menjadi file dengan format *.csv* agar dapat dibaca oleh mesin.

3. Tahapan Ketiga (Klasfikasi

   Tahapan ini akan dilakukan dengan proses pengklasifikasian data normal dan data serangan *UDP Flood* dengan menggunakan algoritma *Support Vector Machine*.

4. Tahapan Keempat (Analisa)

   Tahapan ini akan menganlisi hasil dari penelitian yang telah dilakukan dengan tujuan untuk mendapatkan tingkas performa dari penelitian yang telah dilangsungkan.

1.7 Sistematika Penulisian

Sistematika penulisan selama penyusunan tugas akhir ini, ialah:

BAB I. PENDAHULUAN

Bab ini berisi tentang tujuan dasar terkait subjek riset baik itu dari latar belakang, perumusan masalah, Batasan masalah, tujuan dan manfaat dari penlitian yang di lakukan.

BAB II. TINJUAN PUSTAKA

Bab ini berisi tentang beberapa *literature review* dari penelitian terkait topik klasifikasi serangan UDP flood menggunakan SVM.

BAB III. METODOLGI PENELITIAN

Bab ini membuat metode penelitian yang dilakukan. Penjelasannya meliputi mulai dari tahapan mempersiapkan data, penerapan algoritma SVM.

BAB IV. ANALISA DAN PEMBAHASAN

Bab ini memuat hasil dari eksperimen yang telah dilakukan serta analisis dari tiap data yang didapatkan dari hasil penelitian.

BAB V. KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan yang didapatkan dari hasil riset yang dilakukan serta saran yang bisa digunakan untuk penlitian selanjutnya.

DAFTAR PUSTAKA

[1] I. H. Sarker, «Machine Learning: Algorithms, Real-World Applications and Research Directions», *SN Comput. Sci.*, vol. 2, núm. 3, p. 1-21, 2021, doi: 10.1007/s42979-021-00592-x.

[2] F. Antony i R. Gustriansyah, «Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata», *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, núm. 1, p. 43-52, 2021, doi: 10.30812/matrik.v21i1.1078.

[3] D. Aprilianto, T. Fadila, i M. A. Muslim, «Sistem Pencegahan UDP DNS Flood Dengan Filter Firewall Pada Router Mikrotik», *Techno.Com*, vol. 16, núm. 2, p. 114-119, 2017, doi: 10.33633/tc.v16i2.1291.

[4] A. Singh i D. Juneja, «Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks», *Int. J. Eng. Sci. Technol.*, vol. 2, núm. 8, p. 3405-3411, 2010.

[5] L. Yang i A. Shami, «On hyperparameter optimization of machine learning algorithms: Theory and practice», *Neurocomputing*, vol. 415, p. 295-316, 2020, doi: 10.1016/j.neucom.2020.07.061.

[6] A. O. Sangodoyin, M. O. Akinsolu, P. Pillai, i V. Grout, «Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning», *IEEE Access*, vol. 9, p. 122495-122508, 2021, doi: 10.1109/ACCESS.2021.3109490.

[7] U. Islam *et al.*, «Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models», 2022.

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

[9] M. V. Kotpalliwar i R. Wajgi, «Classification of attacks using support vector

machine (SVM) on KDDCUP'99 IDS database», *Proc. - 2015 5th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2015*, p. 987-990, 2015, doi: 10.1109/CSNT.2015.185.

[10] A. Maslan, K. M. Bin Mohamad, i F. B. Mohd Foozy, «Feature selection for DDoS detection using classification machine learning techniques», *IAES Int. J. Artif. Intell.*, vol. 9, p. 137-145, 2020, doi: 10.11591/ijai.v9.i1.pp137-145.

[11] S. Wankhede i D. Kshirsagar, «DoS Attack Detection Using Machine Learning and Neural Network», *Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018*, 2018, doi: 10.1109/ICCUBEA.2018.8697702.

[12] A. Mubarakali, K. Srinivasan, R. Mukhalid, S. C. B. Jaganathan, i N. Marina, «Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems», *Comput. Intell.*, vol. 36, núm. 4, p. 1580-1592, 2020, doi: 10.1111/coin.12293.

[13] A. Ramamoorthi, T. Subbulakshmi, i S. M. Shalinie, «Real time detection and classification of DDoS attacks using enhanced SVM with string kernels», *Int. Conf. Recent Trends Inf. Technol. ICRTIT 2011*, p. 91-96, 2011, doi: 10.1109/ICRTIT.2011.5972281.

[14] M. Arshi, M. D. Nasreen, i K. Madhavi, «A Survey of DDOS Attacks Using Machine Learning Techniques», *E3S Web Conf.*, vol. 184, p. 1-6, 2020, doi: 10.1051/e3sconf/202018401052.

[15] C. M. Bao, «Intrusion detection based on one-class SVM and SNMP MIB data», *5th Int. Conf. Inf. Assur. Secur. IAS 2009*, vol. 2, p. 346-349, 2009, doi: 10.1109/IAS.2009.124.

[16] J. Yu, H. Lee, M.-S. Kim, i D. Park, «Traffic flooding attack detection with SNMP MIB using SVM», *Comput. Commun.*, vol. 31, p. 4212-4219, 2008, doi: 10.1016/j.comcom.2008.09.018.

[17] T. M. Tatarnikova i P. Y. Bogdanov, «Intrusion detection in internet of things networks based on machine learning methods», *Informatsionno-*

Upravliaiushchie Sist., p. 42-52, 2021, doi: 10.31799/1684-8853-2021-6-42-52.

[18] I. Ibrahim, Z. Ibrahim, H. Ahmad, i Z. M. Yusof, «Trends in Applied Knowledge-Based Systems and Data Science», *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9799, 61272374, p. 841-852, 2016, doi: 10.1007/978-3-319-42007-3.

[19] I. S. Al-Mejibli, J. K. Alwan, i D. H. Abd, «The effect of gamma value on support vector machine performance with different kernels», *Int. J. Electr. Comput. Eng.*, vol. 10, p. 5497-5506, 2020, doi: 10.11591/IJECE.V10I5.PP5497-5506.

[20] K. Kato i V. Klyuev, «An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine», *Int. J. Intell. Comput. Res.*, vol. 5, p. 464-471, 2014, doi: 10.20533/ijicr.2042.4655.2014.0060.

[21] A. Aris, S. F. Oktug, i S. B. O. Yalcin, «Internet-of-Things security: Denial of service attacks», *2015 23rd Signal Process. Commun. Appl. Conf. SIU 2015 - Proc.*, p. 903-906, 2015, doi: 10.1109/SIU.2015.7129976.

[22] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, i R. Budiarto, «Investigating Brute Force Attack Patterns in IoT Network», *J. Electr. Comput. Eng.*, vol. 2019, 2019, doi: 10.1155/2019/4568368.

[23] S. Niksefat, P. Kaghazgaran, i B. Sadeghiyan, «Privacy issues in intrusion detection systems: A taxonomy, survey and future directions», *Comput. Sci. Rev.*, vol. 25, p. 69-78, 2017, doi: 10.1016/j.cosrev.2017.07.001.

[24] P. M. Kumar i U. Devi Gandhi, «A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases», *Comput. Electr. Eng.*, vol. 65, p. 222-235, 2018, doi: 10.1016/j.compeleceng.2017.09.001.

[25] S. Y. Ji, B. K. Jeong, S. Choi, i D. H. Jeong, «A multi-level intrusion detection method for abnormal network behaviors», *J. Netw. Comput. Appl.*, vol. 62, p. 9-17, 2016, doi: 10.1016/j.jnca.2015.12.004.

[26] K. Verma, H. Hasbullah, i A. Kumar, «An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET», *Proc. 2013 3rd IEEE Int. Adv. Comput. Conf. IACC 2013*, p. 550-555, 2013, doi: 10.1109/IAdCC.2013.6514286.

[27] A. Yasin i S. Suleman, «Pengujian Serangan UDP Flood di Jaringan Software-Defined pada GNS3», *J. Teknol. Inf. Indones.*, vol. 3,p. 15, 2018, doi: 10.30869/jtii.v3i1.182.

[28] Y. X. Chu, X. G. Liu, i C. H. Gao, «Multiscale models on time series of silicon content in blast furnace hot metal based on Hilbert-Huang transform», *Proc. 2011 Chinese Control Decis. Conf. CCDC 2011*, p. 842-847, 2011, doi: 10.1109/CCDC.2011.5968300.

[29] S. Amarappa i S. V Sathyanarayana, «Data classification using Support vector Machine (SVM), a simplified approach», *Int. J. Electron. Comput. Sci. Eng.* , vol. 3, p. 435-445, 2011, [En línia]. Disponible a: www.ijecse.org.

[30] V. Hernandez i L. Jodar, «Boundary Problems and Periodic Riccati Equations», *IEEE Trans. Automat. Contr.*, vol. 30, p. 1131-1133, 1985, doi: 10.1109/TAC.1985.1103831.