PENGENALAN POLA SERANGAN *PING FLOOD* DENGAN ALGORITMA *K-MEANS* PADA JARINGAN *INTERNET of THINGS* (IoT)

TUGAS AKHIR

Diajukan untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

MEILINDA EKA SURYANI

09011181320033

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

LEMBAR PENGESAHAN

PENGENALAN POLA SERANGAN *PING FLOOD* DENGAN ALGORITMA *K-MEANS* PADA JARINGAN *INTERNET of THINGS* (IoT)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

MEILINDA EKA SURYANI
09011181320033

Palembang, Desember 2018

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng.
NIP. 197806112010121004

Pembimbing

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Sabtu
Tanggal : 24 November 2018

Tim Penguji :

1. **Ketua : Ahmad Zarkasi. S.T., M.T.**
2. **Anggota I : Dr. Reza Firsandaya Malik, M.T.**
3. **Anggota II : Rido Zulfahmi, M.T.**

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng.
NIP. 197806112010121004

HALAMAN PERNYATAAN

Yang bertandatangan dibawah ini :

Nama	: Meilinda Eka Suryani
NIM	: 09011181320033
Program Studi	: Sistem Komputer
Judul Skripsi	: Pengenalan Pola Serangan *Ping Flood* dengan Algoritma *K-Means* pada Jaringan *Internet of Things* (IoT)

Hasil Pengecekan *Software iThenticate/Turnitin* : 10%

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

Demikian Pernyataan ini saya buat dengan sebenar-benarnya.

Palembang, Desember 2018

Yang menyatakan,

Meilinda Eka Suryani
NIM. 09011181320033

HALAMAN PERSEMBAHAN

“ Sesungguhnya bersama kesusahan (kesulitan) ada kemudahan. Maka apabila kamu telah usai (dari suatu hal), tetaplah bersungguh-sungguh untuk (urusan) yang lainnya. Dan hanya pada Tuhanmu lah kamu berharap.“

(QS. Al Insyirah : 6-8)

“Barangsiapa yang menempuh suatu perjalanan dalam rangka untuk menuntut ilmu maka Allah akan mudahkan baginya jalan ke surga. Tidaklah berkumpul suatu kaum disalah satu masjid diantara masjid-masjid Allah, mereka membaca Kitabullah serta saling mempelajarinya kecuali akan turun kepada mereka ketenangan dan rahmat serta diliputi oleh para malaikat. Allah menyebut-nyebut mereka dihadapan para malaikat.”

(HR. Imam Muslim)

Dengan mengucap syukur Alhamdulillah atas rahamat dari Allah SWT, kupersembahakan karya kecil ini untuk...

Kedua orangtuaku yang tercinta

(Agus Putranto dan Endang Sutarti)

Adikku satu-satunya

(Endro Tegar Prakoso)

Teman-teman seperjuangan

(Sistem Komputer 2013)

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan rahmat, hidayah serta ijin-Nya sehingga penulis dapat menyelesaikan penulisan tugas akhir dengan judul **"Pengenalan Pola Serangan *Ping Flood* dengan Algoritma *K-Means* pada Jaringan *Internet of Things (IoT)*".** Penulisan tugas ahir ini dibuat dalam rangka memenuhi persyaratan untuk menyelesaikan pendidikan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya untuk memperoleh gelar strata 1.

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

1. Allah SWT, yang telah memberikan segalanya kepada penulis berupa kesehatan, orang tua, pembimbing, teman, dll sehingga dapat menyelesaikan laporan tugas akhir ini.
2. Orang-orang tercinta, Ayah, Ibu, Adik, Nenek, Om, Bibi, Pakde, Bude, Lelek, Bulek, Sepupu-sepupuku, Keponakanku yang baru lahir, serta seluruh keluarga besar yang tidak bisa disebutkan satu persatu.
3. Bapak Rossi Pasarella, M.Eng selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Deris Stiawan, Ph. D selaku Dosen Pembimbing tugas akhir, yang telah memberikan bimbingan dan semangat kepada penulis dalam menyelesaikan tugas akhir.
5. Bapak Dr. Reza Firsandaya Malik, M.T dan Bapak Rido Zulfahmi, M.T selaku dosen penguji sidang tugas akhir yang telah memberikan kritik dan saran serta ilmu yang bermanfaat sehingga tulisan ini menjadi lebih baik.
6. Bapak Huda Ubaya, M.T. selaku Pembimbing Akademik, yang telah membimbing penulis dari semester satu hingga terselesainnya tugas ahir ini dengan baik.
7. Seluruh Dosen Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Univeristas Sriwijaya.

8. Staff di jurusan Sistem Komputer, khususnya Kak Ahmad Reza yang telah membantu penyelesaian proses administrasi.
9. Staff di Fakultasi Ilmu Komputer, bagian akademik, kemahasiswaan, tata usaha, perlengkapan, dan keuangan, yang telah membantu penyelesaian proses administrasi.
10. Teman-teman satu tema dalam penelitian ini dikeamanan jaringan *internet of things (IoT)*, Dimas Wahyudi, Kak Kgs Rahmat Shaleh, dan Riki Andika.
11. Teman-teman Laboratorium COMNETS yang telah banyak berbagi cerita, pengalaman, dan kenangan, Dimas Wahyudi, S.Kom, Johan Wahyudi, S.Kom (segera), Fepiliana, S.Kom, Leny Novita Sari, S.Kom, Rendika Adha Tanjung, S.Kom (segera), Riki Andika, S.Kom, Sri Suryani, S.Kom.
12. Sahabat-sahabat TINEMY, Nova Dyati Pradista (TI), Leny Novita Sari (N), Lisa Mardaleta (M), Indah Sari (Y).
13. Kakak-kakak yang telah memberikan motivasi dan masukan-masukannya, Kak Eko Arif Winanto, S.Kom, Kak Candra Adi Winanto, S.Kom, Kak Deni Danuarta, S.Kom.
14. Teruntuk teman-teman satu angkatan, khususnya Sistem Komputer kelas A, Dede Triseptiawan, Rian Fitra Perdana, Ulan Purnama Sari, Eko Pratama, Nova Dyati Pradista, Yayang Prayoga, Sri Suryani, Nur Rahma Dela, Ahmad Kuswandi, Umi Yanti, Indah Sari, Erick Okvanty Haris, Elfa Purnama Sari, Rio Astani, Riki Andika, Kusuma Dwi Indriani, Yoppy Prayudha, Dwi Kurnia Putra, Faris Abdul Aziz, Fahrul Rozi, Fepiliana, Muhammad Fachrurroji Ilham Saputra, Tri Atmoko Malik Kurniawan, Leny Novita Sari, Imam Mustofa, Sandi Sarpani, Suci Anggraeni, Kholil Anggara, Lisa Mardaleta, Agus Juliansyah, Andhika Rizky Perdana, Saros Sakiyana.
15. Adik-adik angkatan 2014 yang kwiyowo, Resti Handayani, Kristiawati, Tya Rhesnia.
16. Serta semua pihak yang telah membatu baik moril maupun materil yang tidak dapat disebutkan satu persatu dalam penyelesaian tugas ahir ini. Terima kasih semuanya.

Semoga dengan terselesainya tugas ahir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua dalam mempelajari deteksi serangan *Pingflood* dengan algoritma *K-Means* pada jaringan *Internet of Thing*. Dalam Penulisan laporan ini penulis juga sangat 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 di masa yang akan datang.

Palembang, Desember 2018

Penulis

Pattern Recognition of Ping Flood Attack with K-Means Algorithm on Internet of Things (IoT)

Meilinda Eka Suryani (09011181320033)
Departement of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email: meilindaeka61@gmail.com

Abstract

This research is focused on pattern recognition of ping flood attack on Internet of Things (IoT). The research was conducted on WiFi communication with normal traffic, attack traffic, and the combination of normal and attack traffic. From the scenario, normal dataset, attack dataset, and a combination of normal and attack dataset are generated. The testing was performed by grouping the datasets into two clusters, namely: (i) normal cluster and (ii) attack cluster, using Weka and implementation of K-Means algorithm. The result of clustering with Weka and implementation of K-Means algorithm shows that has average 95.931 packages in attack cluster, and 4.068 packages in normal cluster. The accuracy of clustering result is then calculated using confusion matrix equation. Based on confusion matrix calculation, the accuracy of clustering using K-Means algorithm is very good, reaching 99,94% with 98,62% true negative rate, 100% true positive rate, 0% false negative rate, and 1,38% false positive rate.

Keywords: Interenet of Things (IoT), Pattern, Ping flood, K-Means, Clustering

Pengenalan Pola Serangan *Ping Flood* dengan Algoritma *K-Means* pada Jaringan *Internet of Things* (IoT)

Meilinda Eka Suryani (09011181320033)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: meilindaeka61@gmail.com

Abstrak

Penelitian ini berfokus pada pengenalan pola serangan *ping flood* pada jaringan *Internet of Things* (IoT). Penelitian dilakukan pada komunikasi *WiFi* dengan lalu lintas normal, lalu lintas serangan, dan lalu lintas gabungan normal-serangan. Dari skenario yang dilakukan, dihasilkan *dataset* normal, *dataset* serangan, dan dataset gabungan normal-serangan. Tahapan pengujian dilakukan dengan pengelompokan *dataset* kedalam dua buah *cluster*, yaitu : (i) *cluster* normal dan (ii) *cluster* serangan, menggunakan *tool* Weka dan implementasi algoritma *K-Means*. Hasil *clustering* menggunakan *tool* Weka dan implemetasi algoritma *K-Means* menunjukan jumlah rata-rata objek pada *cluster* serangan berjumlah 95.931 paket, dan rata-rata objek pada *cluster* normal berjumlah 4.068 paket. Tingkat akurasi dari hasil *clustering* ini kemudian dihitung menggunakan persamaan *confusion matrix.* Berdasarkan perhitungan *confusion matrix*, akurasi dari *clustering* menggunakan algoritma *K-Means* yang diterapkan pada penelitian ini sangat baik, yaitu 99,94% dengan *true negative rate* mencapai 98,62%, *true positive rate* 100%, *false negative rate* 0%, dan *false positive rate* yang mencapai 1,38%.

Kata Kunci : *Internet of Things* (IoT), Pengenalan Pola, *Ping flood*, *K-Means*, *Clustering*

DAFTAR ISI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) merupakan suatu konsep *computing* dimana setiap *physical object* terhubung ke internet dan mampu mengidentifikasi dirinya sendiri dan juga perangkat lain yang ada dalam jaringan. Dengan kata lain, IoT adalah suatu jaringan raksasa dari "*things"* yang saling berhubungan [1]. *Internet of Things* (IoT) telah menjadi topik penelitian utama hampir satu dekade ini, *Internet of Things* (IoT) berkembang pesat. Namun ada ketidakpastian tentang keamanan dan kerahasiaan yang dapat mempengaruhi pembangunan selanjutnya. Salah satu tujuan utama dari keamanan *Internet of Things* (IoT) adalah menyediakan data untuk penggunanya, kapanpun dibutuhkan. Ketersediaan data memastikan akses langsung dari pengguna ke sumber informasi, oleh karena itu perlu disediakan sistem keamanan untuk menangkal serangan terhadap *Internet of Things* (IoT) seperti serangan *Denial of service* (DoS) [2].

Serangan *Denial of service* (DoS) adalah upaya *malicious attacker* untuk mengkonsumsi sumber daya atau bandwidth pengguna. Umumnya serangan DoS melibatkan *flooding* dalam jumlah besar pada *traffic* untuk mengkonsumsi sumber daya jaringan, *bandwidth*, dan sebagainya. Salah satu serangan DoS yang paling umum adalah *ICMP flood* atau *Ping flood* [3].

Pada penelitian sebelumnya [4] membahas masalah deteksi pola abnormal dengan menggunkan *clustering* pada *Distributed Sensor Network*, dimana metode yang diusulkan dapat menerima alamat IP dan port *traffic data,* lalu memvisualisasikannya kedalam gambar dua dimensi, dan mengekstrak pola dengan *brightness value* dan *linear patterns* yang tinggi. Kemudian mengelompokkan port yang telah divisualisasi dan mengizinkan *Artificial Neural Network* untuk mempelajari *extracted features* untuk mendeteksi *traffic data* normal, serangan DDoS, DoS, atau *Internet Worms* secara otomatis.

Pada penelitian lain [5] membahas tentang analisis *thread* pada jaringan *Internet of Things.* Dimana dalam penelitian ini memanfaatkan *Intrusion Detection System* (IDS) *offline* untuk mengumpulkan dan menganalisis informasi dari

berbagai jaringan *Internet of Things* serta mengidentifikasi serangan *Denial of Services* (DoS) pada jaringan *Internet of Things*.

Penelitian selanjutnya [6] membahas mengenai pendeteksian serangan *wormhole* pada *Internet of Things.* Dalam penelitian ini, Shukla menerapkan IDS dengan tiga pendekatan yang berbeda, yaitu IDS menggunakan *K-means, decision tree,* serta *hybrid* antara *K-means* dan *decision tree.* Dari tiga pendekatan yang diterapkan, IDS dengan tingkat deteksi tertinggi adalah IDS yang menggunakan pendekatan *K-means,* tingkat deteksi pendekatan ini mencapai 70-93%. Sedangkan tingkat deteksi IDS dengan *decision tree* mencapai 71-80%, dan IDS dengan pendekatan *hybrid* mencapai 71-75%.

Berdasarkan rujukan pada masing-masing penelitian di atas, maka dalam penelitian tugas akhir ini akan dilakukan *clustering* terhadap serangan *Denial of Services* (DoS) khususnya *Ping Flood* menggunakan algoritma *K-means* pada jaringan *Internet of Things* (IoT). Penggunaan algoritma ini dimaksudkan untuk dapat mengenali pola serangan *Ping Flood* dan membedakannya dengan pola data normal.

1.2 Tujuan

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

1. Untuk mengenali pola serangan *Ping/ICMP flood* pada *Internet of Things* (IoT).
2. Mengimplementasikan *Intrusion Detection System* (IDS) pada jaringan *Internet of Things* (IoT) menggunakan algoritma *K-means.*

1.3 Manfaat

Adapun manfaat yang dapat diambil dari penelitian ini adalah :

1. Dapat mengelompokkan paket pada suatu *dataset* ke dalam kelompok data yang berupa pola data normal dan pola data serangan *Ping/ICMP flood* menggunakan metode *K-means.*
2. Dapat digunakan untuk mengenali pola serangan pada *Internet of Things* (IoT) khususnya serangan *Ping/ICMP flood*.

1.4 Rumusan Masalah

Rumusan masalah berdasarkan latar belakang di atas adalah:

1. Bagaimana mengidentifikasi pola serangan *Denial of Services* (DoS) khususnya *Ping/ICMP flood* pada jaringan *Internet of Things* (IoT).
2. Bagaimana cara melakukan *clustering* terhadap data yang telah diperoleh menggunakan algoritma *K-means.*

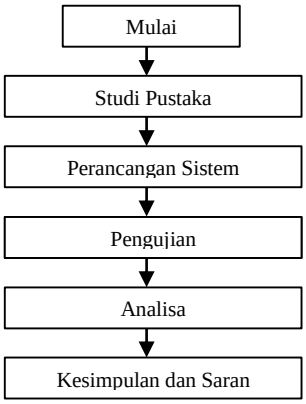
1.5 Batasan Masalah

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

1. Protokol komunikasi yang difokuskan dalam pengujian adalah *WiFi.*
2. Sistem yang dibangun terdiri dari enam *end node,* dimana empat diantaranya menggunakan protokol *WiFi* dan dua lainnya menggunakan protokol Zigbee. satu router dan satu coordinator.
3. Sensor yang digunakan pada *end node* terdiri dari DHT22, *Soil Moisture,* MQ2, sensor *water level,* dan DHT11.
4. Pada setiap end *node* terdiri dari satu sensor.
5. Membahas teknik pengenalan pola serangan *Ping/ICMP flood* pada IoT.
6. Pengujian sistem dilakukan secara *offline.*
7. Algoritma yang digunakan untuk mengenali pola serangan adalah algoritma *clustering K-means.*

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian akan melewati beberapa tahapan, yaitu :



Gambar 1.1 Metodelogi Penelitian

1. Tahap Pertama (Studi Pustaka)

Tahap ini dilakukan dengan cara mengkaji dan mempelajari *literature* dan referensi berupa naskah ilmiah, buku dan *mailing list* sehingga dapat menunjang metodologi dan pendekatan yang akan diterapkan pada penelitian.

2. Tahap Kedua (Perancangan Sistem)

Tahap ini merupakan tahap dimana menentukan perangkat keras maupun perangkat lunak yang *suitable* untuk merancang sistem dan kemudian menentukan topologi yang sesuai. Setelah itu langkah selanjutnya melakukan pengembangan yang telah dirumuskan sebelumnya.

3. Tahap Ketiga (Pengujian)

Setelah semua sistem selesai dibuat kemudian melakukan pengujian sesuai dengan batasan masalah dengan parameter-parameter yang telah ditentukan.

4. Tahap Keempat (Analisa)

Hasil dari pengujian pada tahap sebelumnya, selanjutnya akan dianalisa, dengan tujuan 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, hasil perancangan sistem dan hasil analisa sistem, dan kemudian dihadirkan pula beberapa poin saran dari penulis untuk penelitian selanjutnya.

1.7 Sistematika Penulisan

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, Metedologi 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), Clustering Algorithm,* 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] M. A. Razzaq, M. A. Qureshi, and S. Ullah, “Security Issues in the Internet of Things (IoT): A Comprehensive Study,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, pp. 383–388, 2017.

[2] M. U. Farooq and M. Waseem, “A Critical Analysis on the Security Concerns of Internet of Things (IoT),” *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, 2015.

[3] K. Sonar and H. Upadhyay, “A Survey : DDOS Attack on Internet of Things,” *Int. J. Eng. Res. Dev.*, vol. 10, no. 11, pp. 58–63, 2014.

[4] S. Jang, G. Kim, and S. Byun, “Clustering-Based Pattern Abnormality Detection in Distributed Sensor Networks,” *Hindawi Publ. Corp. Int. J. Distrib. Sens. Networks*, vol. 2014, pp. 1–9, 2014.

[5] E. Hodo *et al.*, “Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System,” *Int. Symp. Networks, Comput. Commun.*, pp. 4–9, 2016.

[6] P. Shukla, “ML-IDS : A Machine Learning Approach to Detect Wormhole Attacks in Internet of Things,” *Intell. Syst. Conf. 2017*, no. September, pp. 234–240, 2017.

[7] L. Wallgren, S. Raza, and T. Voigt, “Routing Attacks and Countermeasures in the RPL-Based Internet of Things,” *Hindawi Publ. Corp. Int. J. Distrib. Sens. Networks*, vol. 2013, pp. 1–12, 2013.

[8] S. Raza, L. Wallgren, and T. Voigt, “Ad Hoc Networks SVELTE : Real-time intrusion detection in the Internet of Things,” *AD HOC NETWORKS*, pp. 1–14, 2013.

[9] A. Al-fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things : A Survey on Enabling Technologies , Protocols and

Applications," *IEEE Commun. Surv. Tutorials*, no. c, pp. 1–33, 2015.

[10] Z. Yang *et al.*, "Study and Application on the Architecture and Key Technologies for IOT," *2011 Int. Conf. Multimed. Technol.*, pp. 747–751, 2011.

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

[12] Y. Zhang, "Technology Framework of the Internet of Things and Its Application," *2011 Int. Conf. Electr. Control Eng.*, pp. 4109–4112, 2011.

[13] R. K. ; S. U. K. ; R. Z. ; S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," *2012 10th Int. Conf. Front. Inf. Technol.*, pp. 257–260, 2012.

[14] L. Tan, "Future Internet: The Internet of Things," *Int. Conf. Adv. Comput. Theory Eng.*, pp. 376–380, 2010.

[15] S. Yan-rong, "Internet of Things key technologies and architectures research in information processing," *Int. Conf. Comput. Sci. Electron. Eng.*, no. Iccsee, pp. 2008–2011, 2013.

[16] N. Koshizuka and K. Sakamura, "Ubiquitous ID: Standards for Ubiquitous Computing and the Internet of Things," *IEEE Pervasive Comput.*, vol. 9, no. 4, pp. 98–101, 2010.

[17] R. Want, "Near Field Communication," *IEEE Pervasive Comput.*, vol. 10, no. 3, pp. 4–7, 2011.

[18] Z. Xu, Y. Yin, and J. Wang, "A Density-based Energy-efficient Clustering Algorithm for Wireless Sensor Networks," *Int. J. Futur. Gener. Commun. Netw.*, vol. 6, no. 1, pp. 75–86, 2013.

[19] A. Dunkels, "Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors," *29th Annu. IEEE Int. Conf. Local Comput. Networks*, pp. 1–8, 2013.

[20] M. Gigli and S. G. M. Koo, "Internet of Things : Services and Applications

Categorization," *Adv. Internet Things*, pp. 1–4, 2013.

[21] P. Barnaghi, W. E. I. Wang, C. Henson, and K. Taylor, "Semantics for the Internet of Things : early progress and back to the future," *Int. J. Semant. Web Inf. Syst.*, vol. 8, no. 1, pp. 1–22, 2015.

[22] D. Wang, L. He, Y. Xue, and Y. Dong, "Exploiting Artificial Immune systems to detect unknown DoS attacks in real-time," *2012 IEEE 2nd Int. Conf. Cloud Comput. Intell. Syst.*, pp. 1–5, 2012.

[23] A. Pradesh, "DoS Attacks Prevention Using IDS and Data Mining," *IEEE*, pp. 1–6, 2016.

[24] Harshita, "Detection and Prevention of ICMP Flood DDOS Attack," *Inetrnational J. New Technol. Res.*, vol. 3, no. 3, pp. 63–69, 2017.

[25] Subramani rao Sridhar, "Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis," *Inf. Secur. Read. Room*, pp. 1–47, 2011.

[26] S. Akbar, N. Rao, and Chandulal, "Intrusion Detection System Methodologies Based on Data Analysis," *Int. J. Comput. Appl.*, vol. 5, no. 2, pp. 10–20, 2010.

[27] H. T. Elshoush and I. M. Osman, "Alert correlation in collaborative intelligent intrusion detection systems — A survey," *Appl. Soft Comput.*, vol. 11, pp. 4349–4365, 2011.

[28] E. A. Winanto, "Visualisasi Serangan Remote to Local (R2l) dengan Clustering *K-means*," Universitas Sriwijaya, 2017.

[29] S. Sandra, "Analisis perbandingan metode *K-means* dan metode naïve bayes untuk visualisasi serangan brute force," Universitas Sriwijaya, 2016.

[30] G. Tzortzis and A. Likas, "The MinMax k -Means clustering algorithm," *Pattern Recognit.*, vol. 47, no. 7, pp. 2505–2516, 2014.

[31] J. A. Hartigan and M. A. Wong, "Algorithm AS 136 A *K-means* Clustering Algorithm," *R. Stat. Soc.*, vol. 28, no. 1, pp. 100–108, 2012.

[32] E. Nugroho and A. Sahroni, “ZigBee and Wifi Network Interface on Wireless Sensor Networks,” *Makassar Int. Conf. Electr. Eng. Infonnatics*, no. November, pp. 54–58, 2014.

[33] S. Rukhmode, G. Vyavhare, S. Banot, and A. Narad, “IOT Based Agriculture Monitoring System Using Wemos,” *Int. Comference Emanations Mod. Eng. Sci. Manag.*, vol. 5, no. March, pp. 14–19, 2017.

[34] N. Kumar, V. Khatri, S. Mangipudi, S. Srivastava, and C. Engineering, “AIR MONITORING AND DATA ACQUISITION SYSTEM,” *Int. J. Educ. Sci. Res. Rev.*, no. 2, pp. 223–227, 2016.

[35] I. Mobin, N. Islam, and R. Hasan, “An Intelligent Fire Detection and Mitigation System Safe from Fire (SFF),” *Int. J. Comput. Appl.*, vol. 133, no. 6, pp. 1–7, 2016.

[36] A. Gaddam and W. F. Esmael, “Designing a Wireless Sensors Network for Monitoring and Predicting Droughts,” *Annu. Conf.*, pp. 1–6, 2014.

[37] W. Sensor, “Water Sensor Module User â€™ s Manual,” pp. 1–3, 2013.