VISUALISASI TRAFIK SERANGAN DENGAN GEO IP UNTUK PEMANTAUAN DI *NETWORK MONITORING CENTER*

TUGAS AKHIR
Program Studi Sistem Komputer
Jenjang S1

Oleh

Muhammad Ajran Saputra
09011381520072

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2019

VISUALISASI TRAFIK SERANGAN DENGAN GEO IP UNTUK PEMANTAUAN DI *NETWORK MONITORING CENTER*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Strata 1

Oleh

Muhammad Ajran Saputra
09011381520072

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019

HALAMAN PENGESAHAN

VISUALISASI TRAFIK SERANGAN DENGAN GEO IP UNTUK PEMANTAUAN DI *NETWORK MONITORING CENTER*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Strata 1

Oleh

Muhammad Ajran Saputra
09011381520072

Palembang, November 2019

Mengetahui,

Ketua Jurusan Sistem Komputer

Rossi Passarella, S.T., M.Eng.
NIP. 197806112010121004

Pembimbing Tugas Akhir

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Senin

Tanggal : 21 Oktober 2019

Tim Penguji :

1. **Ketua : Kemahyanto Exaudi, S.Kom., M.T.**
2. **Anggota 1 : Ahmad Fali Oklilas, S.T., M.T.**
3. **Anggota 2 : Huda Ubaya, S.T., M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

Rossi Passarella,S.T., M.Eng.

NIP. 197806112010121004

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : **Muhammad Ajran Saputra**

NIM : **09011381520072**

Judul : **Visualisasi Trafik Serangan Dengan Geo IP Untuk Pemantauan di *Network Monitoring Center***

Hasil Pengecekan Software iThenticate/Turnitin : 3 %

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, 15 November 2019

Muhammad Ajran Saputra

NIM 09011381520072

VISUALIZATION OF ATTACK TRAFFIC WITH GEO IP FOR MONITORING IN NETWORK MONITORING CENTER

Muhammad Ajran Saputra (09011381520072)

Dept. Of Computer Engineering, Faculty of Computer Science, Sriwijaya University

Email : akhiajran@engineer.com

Abstract

Due to the frequent slowing of the SINTA RISTEKDIKTI web portal when accessed by users, a study was made based on visualization of attack traffic that would display attack files based on log files on the SINTA (Science and Technology Index) server of the Ministry of Research, Technology and Higher Education of the Republic of Indonesia using the method IPAddress or Geo IP Geolocation. The data to be generated is both normal and anomalous traffic data, from the generated data visualization graphs will be displayed to the web server created to obtain status information from attacks using IPAddress by extracting IPAddress data information and visualizing anomalous attack data using Geo IP based on the location of the country and the origin of the attack. From the IP Geo data, it concluded that the attack that led to the SINTA RISTEKDIKTI portal had a large number of sources of attack based on the sinta2.ritekdikti.go.id.log log file.

Keywords : visualization, Cyber Security, Monitoring, Log Analysis, Geo IP

Palembang, November 2019

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, S.T., M.Eng.
NIP. 197806112010121004

Pembimbing Tugas Akhir

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

VISUALISASI TRAFIK SERANGAN DENGAN GEO IP UNTUK PEMANTAUAN DI *NETWORK MONITORING CENTER*

Muhammad Ajran Saputra (09011381520072)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : akhiajran@engineer.com

Abstrak

Dikarenakan sering melambatnya web portal SINTA RISTEKDIKTI ketika diakses oleh para user, maka dibuatkan penelitian berdasarkan visualisasi trafik serangan yang akan menampilkan file serangan berdasarkan log file pada server SINTA (Science and Technology Index) KEMENRISTEKDIKTI Republik Indonesia dengan Geo IP . Data yang akan dihasilkan merupakan data trafik baik itu normal maupun anomali, dari data yang dihasilkan tersebut akan ditampilkan graph visualisasi ke web server yang dibuat untuk mendapatkan status informasi dari serangan menggunakan IPAddress dengan mengekstraksi informasi data IPAddress dan melakukan visualisasi data serangan anomali dengan menggunakan Geo IP berdasarkan letak negara dan asal serangan. Dari data Geo IP tersebut menghasilkan kesimpulan bahwa serangan yang menuju pada portal SINTA RISTEKDIKTI memiliki sumber serangan yang sangat banyak berdasarkan file log sinta2.ritekdikti.go.id.log.

Kata Kunci : Visualisasi, Cyber Security, Monitoring, Log Analysis, Geo IP

Palembang, November 2019

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, S.T., M.Eng.
NIP. 197806112010121004

Pembimbing Tugas Akhir

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

HALAMAN PERSEMBAHAN

Kupersembahkan Skripsi ini untuk yang selalu bertanya :

“kapan skripsimu selesai?”

Terlambat lulus atau lulus tidak tepat waktu bukan sebuah kejahatan, bukan sebuah aib. Alangkah kerdilnya jika mengukur kepintaran seseorang hanya dari siapa yang paling cepat lulus. Bukankah sebaik-baiknya skripsi adalah skripsi yang selesai? Baik itu selesai tepat waktu maupun tidak tepat waktu.

KATA PENGANTAR

Alhamdulilahirabbil'alamin. Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan Tugas Akhir ini dengan judul "Visualisasi trafik serangan dengan Geo IP untuk pemantauan di *network monitoring center* ".

Dalam laporan ini penulis menjelaskan mengenai teknik deteksi serangan dan visualisasi dari serangan tersebut berbasis geografis penyerang. Penulis berharap tulisan ini dapat bermanfaat bagi orang banyak, dan menjadi tambahan bahan bacaan bagi yang tertarik meneliti di keamanan jaringan komputer.

Pada penyusunan laporan ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allat SWT dan terimakasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga tugas akhir penulisan ini dapat berjalan dengan lancar.
2. Kedua orang tua beserta keluarga yang selalu mendoakan serta memberikan motivasi dan semangat.
3. Bapak Jaidan Jauhari, S.Pd. M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
4. Bapak Rossi Passarella, S.T.,M.Eng selaku Ketua Jurusan Sistem Kompuer Fakutas Ilmu Komputer Universitas Sriwijaya
5. Bapak Deris Stiawan, Ph. D selaku Pembimbing Tugas Akhir Penulis yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan tugas akhir ini.
6. Bapak Sutarno, MT selaku Pembimbing Akademik Jurusan Sistem Komputer

7. Seluruh teman-teman Jurusan Sistem Komputer khususnya kelas unggulan angkatan 2015 yang tidak dapat saya sebutkan satu persatu
8. Dan semua pihak yang telah membantu

Penulis menyadari bahwa tugas akhir ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dikemudian hari.

Akhir kata dengan segala keterbatasan, penulis berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran.

Palembang, November 2019

Penulis

VISUALIZATION OF ATTACK TRAFFIC WITH GEO IP FOR MONITORING IN NETWORK MONITORING CENTER

Muhammad Ajran Saputra (09011381520072)

Dept. Of Computer Engineering, Faculty of Computer Science, Sriwijaya University

Email : akhiajran@engineer.com

Abstract

Due to the frequent slowing of the SINTA RISTEKDIKTI web portal when accessed by users, a study was made based on visualization of attack traffic that would display attack files based on log files on the SINTA (Science and Technology Index) server of the Ministry of Research, Technology and Higher Education of the Republic of Indonesia using the method IPAddress or Geo IP Geolocation. The data to be generated is both normal and anomalous traffic data, from the generated data visualization graphs will be displayed to the web server created to obtain status information from attacks using IPAddress by extracting IPAddress data information and visualizing anomalous attack data using Geo IP based on the location of the country and the origin of the attack. From the IP Geo data, it concluded that the attack that led to the SINTA RISTEKDIKTI portal had a large number of sources of attack based on the sinta2.ritekdikti.go.id.log log file.

Keywords : visualization, Cyber Security, Monitoring, Log Analysis, Geo IP

Palembang, November 2019

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, S.T., M.Eng.
NIP. 197806112010121004

Pembimbing Tugas Akhir

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

VISUALISASI TRAFIK SERANGAN DENGAN GEO IP UNTUK PEMANTAUAN DI *NETWORK MONITORING CENTER*

Muhammad Ajran Saputra (09011381520072)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : akhiajran@engineer.com

Abstrak

Dikarenakan sering melambatnya web portal SINTA RISTEKDIKTI ketika diakses oleh para user, maka dibuatkan penelitian berdasarkan visualisasi trafik serangan yang akan menampilkan file serangan berdasarkan log file pada server SINTA (Science and Technology Index) KEMENRISTEKDIKTI Republik Indonesia dengan Geo IP . Data yang akan dihasilkan merupakan data trafik baik itu normal maupun anomali, dari data yang dihasilkan tersebut akan ditampilkan graph visualisasi ke web server yang dibuat untuk mendapatkan status informasi dari serangan menggunakan IPAddress dengan mengekstraksi informasi data IPAddress dan melakukan visualisasi data serangan anomali dengan menggunakan Geo IP berdasarkan letak negara dan asal serangan. Dari data Geo IP tersebut menghasilkan kesimpulan bahwa serangan yang menuju pada portal SINTA RISTEKDIKTI memiliki sumber serangan yang sangat banyak berdasarkan file log sinta2.ritekdikti.go.id.log.

Kata Kunci : Visualisasi, Cyber Security, Monitoring, Log Analysis, Geo IP

Palembang, November 2019

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, S.T., M.Eng.
NIP. 197806112010121004

Pembimbing Tugas Akhir

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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Pada tahun 2018, [1] 10 insiden keamanan informasi terbanyak meliputi jaringan trojan, percobaan hak user, percobaan dos, percobaan penyadapan informasi, percobaan hak akses administrator, serangan privasi, deteksi serangan dos, trafik yang rusak berdasarkan laporan dari Indonesia Security Incident Response Team on Internet Infrastructure.

Disisi lain dalam penelitian [2] pada triwulan pertama 2019, tercatat jumlah serangan siber Indonesia menempati peringkat ke-8 dengan 360 juta permintaan laman berbahaya terhadap pengguna, yang mana hal ini mengalami peningkatan dari tahun sebelumnya dimana Indonesia menempati peringkat ke-17. Hal ini dikarenakan populasi internet yang tinggi. Berdasarkan riset [3] jumlah penetrasi pengguna internet Indonesia berjumlah 144 juta pengguna berbanding dengan total populasi masyarakat Indonesia yang berjumlah 262 juta orang.

Jaringan sangat rentan terhadap berbagai keadaan tidak terduga yang dapat mengganggu jalannya operasi yang sedang berjalan. Kejadian tidak terduga ini disebut anomali. Secara umum, anomali diklasifikasikan menjadi 2 macam : *malicious* dan *unusual behavior* [4].

Geo IP lebih mengacu kepada metode pencarian lokasi geografis terhadap suatu perangkat komputer yang terhubung ke internet dengan mengidentifikasi alamat IP komputer tersebut [5]. Meskipun Geo IP dapat menentukan lokasi pengguna komputer berada, tetapi harus membutuhkan databases lokasi seluruh dunia dan pemahaman tentang API untuk bisa diimplementasikan ke program tertentu sehingga penentuan lokasi lebih akurat dan benar [6].

Pada penelitian [7], memvisualkan deteksi serangan dengan menggunakan histogram dimana ini memiliki problem yaitu permasalahan di rentang IPAddress

yang terbatas serta port yang terbuka akan lebih mudah dideteksi ketika proses plotting visual dilakukan sesuai dengan range IPAddress yang ada.

Penelitian lainnya [8], memberikan sebuah masalah dalam evaluasi visualisasi, dimana visualisasi sekarang menggunakan log yang semakin besar dan bagaimana memecahkan masalah untuk memvisualisasikan deteksi serangan yang ditampilkan melalui web application secara *realtime* serta mampu memberikan penjelasan singkat yang mudah dibaca.

Sebelumnya pada penelitian [9], memberikan saran bahwa untuk menjaga ketersediaan layanan pada sebuah *web server*, maka diperlukan suatu pengembangan teknik yang memungkinkan GeoDNS dapat melakukan pengecekan otomatis secara periodik terhadap kondisi *web server*, sehingga apabila ada salah satu *web server* mengalami gangguan atau kerusakan, GeoDNS segera dapat mengarahkan request user ke server lain yang kondisinya baik.

Dari beberapa ulasan diatas, penulis akan melakukan visualisasi dari trafik serangan dengan Geo IP, Geo IP ini digunakan berdasarkan IPAddress penyerang berdasarkan log dari apache web service dengan mengekstraksi informasi dari IPAddress tersebut dan mengkategorikannya menjadi letak geografis sehingga mampu memvisualkan dan mengkategorikannya berdasarkan lokasi asal dari IPAddress tersebut.

1.2 TUJUAN

Adapun tujuan yang akan dicapai dalam penelitian ini adalah :

1. Menganalisa log yang terdapat pada server
2. Mengkategorikan trafik yang masuk berdasarkan lokasi IPAddress berasal
3. Mengekstraksi informasi dari sekumpulan IPAddress
4. Memvisualkan asal serangan berdasarkan letak geografisnya

1.3 MANFAAT

Adapun manfaat dari tugas akhir ini dilakukan adalah :

1. Mampu mengekstraksi informasi secara lengkap asal serangan hanya berdasarkan IPAddress yang tercatat pada log web service apache

2. Mendeteksi anomali yang melewati trafik yang masuk ke log apache web service
3. Ekstraksi informasi mampu memberikan lokasi koordinat direct ke google maps API
4. Dapat memberi suatu acuan atau membuat system monitoring jaringan terbaru bagi administrator dalam penerapan monitoring jaringan

1.4 RUMUSAN MASALAH

1. Bagaimana menganalisa trafik pengunjung yang tercatat pada log server ?
2. Bagaimana mendapatkan informasi detail hanya berdasarkan sumber IPAddress?
3. Bagaimana memvisualkan secara geografis berdasarkan informasi yang didapat melalui proses ekstraksi ?
4. Bagaimana merancang dan membangun sebuah sistem jaringan yang bisa untuk memvisualisasikan berdasarkan log yang sudah didapatkan berdasarkan lokasi asal.

1.5 BATASAN MASALAH

1. File log server berbasis apache service
2. Sumber file log berdasarkan portal sinta2.ristekdikti.go.id
3. Tidak membahas bagaimana pencegahan serangan yang telah terjadi
4. Hanya bisa divisualkan ketika serangan sudah dideteksi.
5. Mekanisme visualisasi menggunakan informasi negara asal
6. Tidak diujikan ketika penyerang melakukan serangan melalui jalur enkripsi

1.6 METODOLOGI PENELITIAN

Metode yang akan digunakan pada penelitian ini yaitu sebagai berikut :

1. Tahap Pertama (Studi Pustaka/Literatur)

   Pada tahap pertama ini diawali dengan mencari masalah yang sesuai dan berkaitan untuk diangkat sebagai observasi. Setelah itu, mencari beberapa sumber seperti pada artikel,jurnal,buku, internet dan beberapa sumber lainnya yang berhubungan langsung dengan tugas akhir.
2. Tahap Kedua (Perancangan Sistem)

Pada tahap kedua ini merupakan tahap yang membahas masalah proses bagaimana untuk menyusun metode atau pendekatan tertentu, perangkat lunak maupun perangkat keras apa saja yang dapat digunakan dan konfigurasi sistem beserta implementasi metode.

3. Tahap Ketiga (Pengujian)

   Pada tahap ketiga ini merupakan tahap tambahan dari perancangan sistem dimana pada tahap ketiga ini dilakukan pengujian berdasarkan metodologi observasi dan observasi sebelumnya sehingga didapatkan hasil percobaan yang sesuai dan tepat secara konsep ataupun praktis.

4. Tahap Keempat (Analisa)

   Pada tahap keempat ini dilakukan dengan pengolahan serta analisis data yang didapatkan dari hasil pengujian berdasarkan pendekatan tertentu untuk memperoleh data yang objektif.

5. Tahap Kelima (Kesimpulan dan saran)

   Pada tahapan ini, akan dirumuskan sebagai suatu kesimpulan yang didapatkan dari tahapan-tahapan sebelumnya. Selain itu, dapat ditambahkan beberapa saran yang dapat dijadikan sebagai landasan untuk observasi selanjutnya.

1.7 SISTEMATIKA PENULISAN

Untuk mempermudah dalam proses penyusunan tugas akhir dan memperjelas isi dari setiap bab maka dibuat secara sistematika penulisan sebagai berikut:

BAB I. PENDAHULUAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik observasi yang meliputi latar belakang,tujuan,manfaat,rumusan masalah dan batasan masalah kemudian metodologi penelitian serta sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada bab ini berisi dasar teori dari *Cyber Attack, Geo IP, log parser, apache web server, ssh attack system* dan teori lainnya yang berkaitan dengan observasi.

BAB III. METODOLOGI PENELITIAN

Bab ini menafsirkan secara sistematis, bagaimana proses observasi dilakukan. Penjelasan pada bab ini mencakup tahapan perancangan sistem “ System Design“ dan penerapan metode observasi.

BAB IV. HASIL DAN ANALISA

Bab ini menafsirkan secara sistematis, bagaimana proses observasi dilakukan. Penjelasan pada bab ini mencakup tahapan perancangan sistem “ “ dan penerapan metode observasi.

BAB V. KESIMPULAN

Pada bab ini yang berisi kesimpulan tentang observasi yang telah dilakukan, serta menjawab tujuan yang akan dicapai pada BAB I (Pendahuluan). Serta berisi saran-saran untuk observasi selanjutnya yang akan dilakukan.

DAFTAR PUSTAKA

[1] ID-SIRTII, “Indonesia Cyber Security Monitoring Report 2018.” p. 52, 2019.

[2] S. Keats, S. Ragan, and M. McKeay, “Security Credential Stuffing : Attacks and Economies Introduction,” 2019.

[3] Asosiasi Penyelenggara Jasa Internet Iindonesia, “Penetrasi & Perilaku Pengguna Internet Indonesia 2017,” *Penetrasi dan Perilaku Pengguna Internet Indones.*, pp. 1–39, 2017.

[4] A. A. Amaral, L. de S. Mendes, B. B. Zarpelão, and M. L. P. Junior, “Deep IP flow inspection to detect beyond network anomalies,” *Comput. Commun.*, vol. 98, pp. 80–96, 2017.

[5] MaxMind, “What is GeoIP?,” vol. 2012, no. 05/01/2012, p. 24, 2012.

[6] M. Syamkumar, R. Durairajan, and P. Barford, “Bigfoot: A geo-based visualization methodology for detecting BGP threats,” *2016 IEEE Symp. Vis. Cyber Secur. VizSec 2016*, 2016.

[7] K. Abdullah, C. Lee, G. Conti, and J. A. Copeland, “Visualizing network data for intrusion detection,” *Proc. from 6th Annu. IEEE Syst. Man Cybern. Inf. Assur. Work. SMC 2005*, vol. 2005, no. June, pp. 100–108, 2005.

[8] Ibrahim Elhenawy, A. El Din Riad, Ahmed Hassan, and Nancy Awadallah, “Visualization Techniques For Intrusion Detection - A Survey,” *Int. J. Comput. Sci. Eng. Surv.*, vol. 2, no. 3, pp. 107–119, 2011.

[9] M. J. Rajabi, “Analisa pemanfaatan DNS server dan GEOIP sebagai solusi untuk GSLB (Global server load balancing),” Universitas Indonesia. Fakultas Ilmu Komputer, 2008.

[10] I. Alsmadi, “The NICE Cyber Security Framework,” *NICE Cyber Secur. Framew.*, pp. 53–73, 2019.

[11] O. W. Purbo and T. Wiharjito, “Keamanan Jaringan Internet,” *PT Elex Media Koputindo, Jakarta*.

[12] A. Jamdagni, “Payload-based Anomaly Detection in HTTP Traffic,” no. November, 2012.

[13] C. M. Colombini, A. Colella, M. Mattiucci, and A. Castiglione, “Cyber threats monitoring: Experimental analysis of malware behavior in cyberspace,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8128 LNCS, pp. 236–252, 2013.

[14] J. Uramova, P. Segec, M. Moravcik, J. Papan, M. Kontsek, and J. Hrabovsky, “(11 Criteria for reliable dataset) Infrastructure for Generating New IDS Dataset,” *2018 16th Int. Conf. Emerg. eLearning Technol. Appl.*, pp. 603–610, 2018.

[15] V. Tavares *et al.*, “A Survey on Information Visualization for Network and Service Management,” 2015.

[16] L. Zeltser, *Analyzing malicious software. In CyberForensics (pp. 59-83).* 2010.

[17] N. Evans and W. Horsthemke, “Analysis of Cyber Dependencies,” *Cyber Resil. Syst. Networks*, pp. 93–106, 2018.

[18] S. Hafeef, “Deep Packet Inspection using Snort Supervisory Committee Deep Packet Inspection using Snort,” 2016.

[19] F. Mansmann, F. Fischer, D. A. Keim, and S. C. North, “Visual support for analyzing network traffic and intrusion detection events using TreeMap and graph representations,” pp. 19–28, 2009.

[20] N. Muraleedharan, A. Parmar, and M. Kumar, “A flow based anomaly detection system using chi-square technique,” *2010 IEEE 2nd Int. Adv. Comput. Conf. IACC 2010*, pp. 285–289, 2010.

[21] D. Systems, N. Services, and B. Weiland, “Intrusion Detection with Heterogenous Sensors,” 2007.

[22] D. Moon, H. Im, I. Kim, and J. H. Park, “DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks,” *J. Supercomput.*, vol. 73, no. 7, pp. 2881–2895, 2017.

[23] M. Akiyama, T. Yagi, T. Yada, T. Mori, and Y. Kadobayashi, “Analyzing the ecosystem of malicious URL redirection through longitudinal observation from honeypots,” *Comput. Secur.*, vol. 69, pp. 155–173, 2017.

[24] J. I. Maanari, R. Sengkey, H. Wowor, and Y. D. Y. Rindengan, “Perancangan Basis Data Perusahaan Distribusi dengan Menggunakan Oracle,” *J. Tek. Elektro dan Komput.*, vol. 2, no. 2, 2013.