DETEKSI SERANGAN *BRUTE FORCE* PADA *TANGLE NETWORK* NODE IOTA HORNET DENGAN METODE *SIGNATURE-BASED DETECTION*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

Sultan Zidan

09011382025119

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

DETEKSI SERANGAN *BRUTE FORCE* PADA *TANGLE NETWORK* NODE IOTA HORNET DENGAN METODE *SIGNATURE-BASED DETECTION*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

Sultan Zidan

09011382025119

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

HALAMAN PENGESAHAN

DETEKSI SERANGAN *BRUTE FORCE* PADA *TANGLE NETWORK* NODE IOTA HORNET DENGAN METODE *SIGNATURE-BASED DETECTION*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

Sultan Zidan

09011382025119

Palembang, 17 Juli 2024

Mengetahui

Pembimbing I TA	Pembimbing II TA
Huda Ubaya, M.T.	Adi Hermansyah, M.T.
NIP. 198106162012121003	NIP. 198904302024211001

Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 20 Juni 2024

Tim Penguji :

1. **Ketua : Kemahyanto Exaudi, M.T.**
2. **Sekretaris : Muhammad Ali Buchari, M.T.**
3. **Pembimbing I : Huda Ubaya, M.T.**
4. **Pembimbing II : Adi Hermansyah, M.T.**
5. **Penguji : Dr. Ahmad Zarkasi, M.T.**

Mengetahui, 15/7/24
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang Bertanda Tangan Di Bawah Ini :

Nama : Sultan Zidan

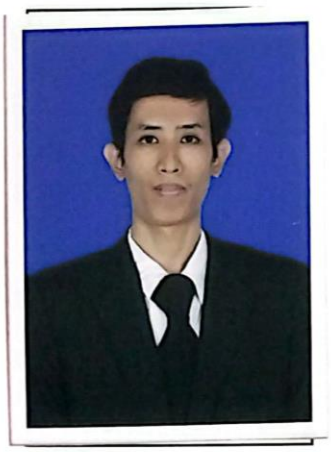
NIM : 09011382025119

Judul : DETEKSI SERANGAN *BRUTE FORCE* PADA *TANGLE NETWORK* NODE IOTA HORNET DENGAN METODE *SIGNATURE-BASED DETECTION*

Hasil Pengecekkam Software iThenticate/Turnitin : 3%

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

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



Palembang, Juli 2024

Penulis,

Sultan Zidan

NIM.09011382025119

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيْم

Assalamualaikum Warahmatullahi Wabarakatuh

Puji syukur Alhamdulillah penulis panjatkan atas kehadirat Allah SWT yang telah memberikan karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penulisan Tugas Akhir ini yang berjudul "**Deteksi Serangan *Brute force* Pada *Tangle Network* Node IOTA Hornet Dengan Metode *Signature-Based Detection***"

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan Proposal Tugas Akhir ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur kepada Allah SWT dan terima kasih kepada yang terhormat :

1. Allah SWT. yang telah memberikan kesehatan, kemudahan, serta keberkahan sehingga penulis dapat menyelesaikan penelitian tugas akhir beserta laporannya dengan baik.
2. Orang Tua yang telah memberikan banyak do'a dan dukungan serta semangat.
3. Bapak Prof. Dr. Erwin, S.SI, M.SI selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T. selaku Dosen Pembimbing Akademik serta Ketua Jurusan Sistem Komputer, Universitas Sriwijaya.
5. Bapak Huda Ubaya, M.T. selaku Dosen Pembimbing I Tugas Akhir yang berkenan meluangkan waktu dalam membimbing, memberikan saran dan motivasi untuk penulis dalam menyelesaikan tugas akhir ini.
6. Bapak Adi Hermansyah, M.T. selaku Dosen Pembimbing II Tugas Akhir yang berkenan meluangkan waktu dalam membimbing, memberikan saran dan motivasi untuk penulis dalam menyelesaikan tugas akhir ini.

7. Mbak Sari selaku Admin Jurusan Sistem Komputer Bukit yang telah membantu dalam mengelola seluruh berkas administrasi.
8. Teman-teman Sistem Komputer Unggulan 2020
9. Semua pihak yang terlibat yang telah turut ikut membantu, baik itu dalam memberikan masukan dan ide, kritik, maupun juga memberikan semangat kepada penulis yang mana tidak bisa disebutkan satu persatu..
10. Almamater

Penulis menyadari bahwa proposal 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 proposal ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung maupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran dan penelitian.

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang,……

Penulis,

Sultan Zidan
NIM. 09011382025119

DETEKSI SERANGAN *BRUTE FORCE* PADA *TANGLE NETWORK* NODE IOTA HORNET DENGAN METODE *SIGNATURE-BASED DETECTION*

Sultan Zidan (09011382025119)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : dorovskimontgomery@gmail.com

ABSTRAK

Brute force adalah salah satu metode umum yang paling sering digunakan oleh peretas dalam kejahatan siber. IOTA merupakan pendekakan *blockchain* sekuensial dengan *Directed Acyclic Graph* (DAG) berdasarkan *Distributed Ledger Technology* (DLT) open source yang dirancang khusus untuk industri IoT/IoE. IOTA Hornet node yang terpasang pada *cyber-physical system* seperti pada server yang merupakan *critical infrastructure* rentan terhadap serangan *brute force* karena node IOTA yang dapat diakses melalui website memiliki dashboard yang dapat melakukan login user dan password. Untuk menerapkan metode *signature-based detection* pada *Intrusion Detection System*(IDS) diperlukan analisis mengenai pola *signature* dari serangan *brute force*. Penelitian tugas akhir ini membahas mengenai deteksi serangan *brute force* pada node IOTA hornet dengan menggunakan IDS snort dan suricata yang sudah diterapkan *signature-based* didalamnya dan kemudian hasil deteksi akan dikalkulasikan untuk mendapatkan deteksi serangan dan akurasi dari IDS yang digunakan. Dari penelitian ini IDS snort memiliki tingkat deteksi serangan dan akurasi yang lebih baik dari suricata dengan tingkat deteksi serangan 99,35% dengan akurasi 99,02% sementara suricata dengan tingkat deteksi 73,95% dan akurasi 84,57% .

Kata Kunci : *Brute force*, IOTA, *Signature-based detection*, *Intrusion Detection System, Snort, Suricata*

BRUTE FORCE ATTACKS DETECTION ON THE IOTA HORNET TANGLE NETWORK NODE USING THE SIGNATURE-BASED DETECTION METHOD

Sultan Zidan (09011382025119)
Department of Computer System, Faculty of Computer Science,Sriwijaya University
Email : dorovskimontgomery@gmail.com

ABSTRACT

Brute force is one of the most common methods used by hackers in cybercrime. IOTA is a sequential blockchain approach with Directed Acyclic Graph (DAG) based on open source Distributed Ledger Technology (DLT) specifically designed for the IoT/IoE industry. IOTA Hornet nodes are installed on cyber-physical systems such as servers, which are critical infrastructure that are vulnerable to brute force attacks because IOTA nodes that can be accessed via the website have a dashboard that can provide user and password logins. To apply a signature-based detection method to an Intrusion Detection System (IDS), analysis of the signature patterns of brute force attacks is required. This final project research discusses the detection of brute force attacks on IOTA hornet nodes using IDS snort and suricata which have been implemented on a signature based and then the detection results will be calculated to obtain the detection of attacks and the accuracy of the IDS used. From this research, IDS Snort has the better attacks detection rate and accuracy than suricata with attacks detection rate 99,35% with 99,02% accuracy while suricata with attacks detection rate 73,95% with 84,57% accuracy.

Keywords : *Brute force, IOTA, Signature-based detection, Intrusion Detection System, Snort, Suricata*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi internet saat ini banyak sistem keamanan jaringan pada server yang tidak dapat menganalisis dan membuat keputusan ketika mengalami serangan. Keamanan jaringan sangat penting untuk menjaga dan memelihara informasi, terutama pada server yang sedang bekerja maupun menyimpan beberapa data dan informasi penting[1]. Ada banyak upaya yang dilakukan orang-orang yang tidak bertanggung jawab untuk meretas akun dan mendapatkan data sensitif orang lain maupun merusak sebuah infrastruktur yang sudah dibentuk untuk diakses melalui internet . Salah satunya adalah metode yang digunakan adalah *brute force attacks*. Serangan *brute* force menjadi sebuah serangan yang merupakan ancaman yang besar dalam keamanan jaringan, meskipun merupakan serangan yang memberikan beban komputasi bagi penyerang karena proses pemecahan password yang dilakukan akan memakan waktu dan kinerja perangkat yang besar[2]. Ada banyak teknik dan *tools* yang dapat digunakan untuk melakukan serangan *brute force* untuk berbagai tujuan, seperti Owasp Zap, Burp Suite, Hydra dan Hashcat. Serangan *brute force* dapat dilakukan baik pada sistem operasi seperti Windows dan Linux, menjadikannya sebagai sebuah metode serangan termudah untuk dilancarkan.

Merupakan serangan yang umum digunakan oleh penyerang dalam kasus kejahatan siber(*cyber crime)* karena merupakan sebuah metode serangan yang mudah untuk dilancarkan[3], Serangan *brute force* dilakukan melalui semua kemungkinan kombinasi karakter legal secara berurutan sehingga dapat menemukan input yang benar. Semakin panjang kata sandi, semakin banyak waktu yang dibutuhkan untuk menemukan masukan yang benar. Serangan *brute force* umumnya mencoba mendapatkan password dari target dengan menggunakan jutaan kata untuk digunakan dalam serangan.[4] Secara umum serangan brute force akan

meninggalkan data lalu lintas pada lalu lintas jaringan, dimana lalu lintas jaringan itu akan memiliki sebuah *pattern* atau *signature* dari data serangan dan data normal [5].

Blockchain merupakan sebuah *distributed ledger technology*(DLT) yang digunakan untuk memelihara atau menjaga secara berlanjut list data record yang terus berkembang atau bertambah serta menjaga record transaksi. Blockchain memiliki 3 kriteria; publik atau tidak resmi, private atau resmi, dan konsorsium[6]. IOTA foundation mengajukan sebuah protokol bernama IOTA dengan data struktur based DAG(*Directed Acyclic Graph*) dimana tidak ada rantai single(*single chain*) melainkan sebuah tangle yang berarti setiap transaksi terikat pada DLT secara langsung[7].

Jaringan *Internet of Things Application* (IOTA) Tangle telah menggantikan pendekatan blockchain sekuensial dengan *Directed Acyclic Graph* (DAG) berdasarkan *Distributed Ledger Technology* (DLT) open source yang dirancang khusus untuk industri IoT/IoE. Jaringan IOTA Tangle diperkenalkan terutama untuk mengatasi inefisiensi desain blockchain berurutan dan dapat dianggap sebagai cara baru untuk menangani sistem IoT peer-to-peer terdesentralisasi[8].

IOTA node yang terpasang pada *cyber-physical system* seperti pada server yang merupakan *critical infrastructure* rentan terhadap serangan *brute force* karena node IOTA yang dapat diakses melalui website memiliki dashboard yang dapat melakukan login user dan password, dan password yang kemungkinan besar dapat dieksploitasi oleh orang yang tidak bertanggung jawab dengan menggunakan serangan *brute force*[7].

Signature-based Detection diterapkan pada perangkat *intrusion detection system*(IDS) yang bertujuan untuk memonitor kemudian mendeteksi dengan membedakan peristiwa atau *event* yang terjadi pada sistem yang melanggar kebijakan sistem atau *system policy*. Skema *signature-based* mencari pola dan atau signature data yang dianalisis dari peristiwa yang terjadi pada traffic jaringan. Skema *signature-based* ini memberikan hasil deteksi yang cukup bagus untuk

serangan tertentu yang cukup dikenali, Namun tidak cukup bagus digunakan untuk mendeteksi ataupun menganalisis serangan yang baru terbentuk atau belum diketahui pola dan signaturenya,[9][10][11].

Proses pendeteksian dengan *signature-based* pada sistem IDS baik itu snort maupun suricata memiliki proses dalam melakukan identifikasi serangan, dimana ketika *signature* sudah didapatkan dan diaplikasikan pada IDS maka proses pengolahan data *traffic* baik itu berdasarkan *real-time* maupun berdasarkan dataset file pcap/pcapng yang akan dianalisis menggunakan IDS yang sudah diaplikasikan *signature-based* didalamnya. Proses kerja IDS yaitu mulai dari *packet capturing module, packer decoding module, preprocessing module, detection engine module, alerting module, dan output module* [12].

Dengan begitu penelitian ini akan mengusulkan penggunaan metode *Signature-based Detection* pada sistem IDS untuk mendeteksi serangan *Brute force* yang dilancarkan pada tangle network IOTA Hornet berdasarkan *signature* yang ditinggalkan pada data traffic.

1.2. Tujuan

1. Merangkai sebuah node IOTA hornet yang terhubung peer-to-peer
2. Melakukan serangan *Brute force* terhadap node IOTA hornet yang telah dirangkai dan bekerja.
3. Memberikan pengetahuan cara mengenali paket yang terindikasi sebagai bentuk serangan *brute force*.
4. Melakukan deteksi serangan *Brute force* dengan metode *Signature-based Detection* menggunakan snort dan suricata.
5. Mendapatkan akurasi persentase deteksi serangan.

1.3. Manfaat

1. Dapat merangkai sebuah node IOTA yang tersambung *peer-to-peer* terhadap node lain.

2. Dapat melakukan percobaan serangan *Brute force* ke node dashboard dari IOTA hornet yang telah dirangkai.
3. Dapat mengenali pola paket dan *signature* yang mengindikasikan sebuah serangan *brute force*.
4. Dapat mengimplementasikan pola serangan *Brute force* yang didapat ke dalam metode *Signature-based detection* menggunakan snort dan suricata.
5. Mengetahui efektivitas metode berdasarkan akurasi deteksi serangan dan perbandingan antara snort dan suricata

1.4.Perumusan Masalah

Berikut adalah rumusan masalah dalam penulisan Tugas Akhir ini :

1. Bagaimana bentuk pola dan signature dari serangan *Brute force* terhadap node IOTA hornet?.
2. Bagaimana hasil deteksi serangan *Brute force* yang menargetkan node IOTA hornet dengan menerapkan metode *Signature-based Detection* pada snort dan suricata?.
3. Apa saja dampak yang terjadi jika penyerang mendapatkan akses ke dalam node IOTA hornet setelah berhasil menjalankan serangan *Brute force*?.

1.5. Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu :

1. Tidak membahas mengenai cara penanganan ataupun pencegahan *Brute force* terhadap node IOTA hornet.
2. Serangan dilakukan secara real time dengan metode serangan *brute force* kemudian dilakukan *tapping* lalu lintas jaringan untuk dianalisis

3. Menganalisis serangan *Brute force* pada dashboard node IOTA hornet.
4. Membahas cara mengenali pola signature serangan *Brute force* sebelum diterapkan pada metode deteksi.

1.6. Metodologi Penelitian

Dalam tugas akhir ini akan menggunakan metodologi dan melewati beberapa tahapan dalam prosesnya yaitu :

1. Studi Pustaka/Literatur

   Tahapan ini dimulai setelah melakukan berbagai riset dan penelitian sebelumnya mengenai serangan pada IOTA yang mengacu pada banyak artikel, jurnal, paper, dan buku yang berhubungan dengan penelitian yang dilakukan yaitu "Deteksi Serangan *Brute force* Pada Node IOTA Hornet Dengan Metode *Signature-based Detection*".
2. Perancangan Sistem

   Pada tahap ini menentukan perangkat-perangkat yang dibutuhkan dan akan digunakan dalam penelitian baik itu perangkat keras maupun perangkat lunak.
3. Pengujian

   Melakukan pengujian yang sesuai dengan parameter serangan yang ditentukan oleh batasan masalah.
4. Analisa dan Hasil

   Mencakup hasil pengujian pada penelitian yang dilakukan kemudian hasil penelitian yang di analisa untuk mengetahui kelebihan dan kekurangan pada rancangan penelitian beserta faktor-faktor yang mempengaruhi
5. Kesimpulan dan Saran

   Tahapan terakhir meliputi kesimpulan dan saran dari hasil studi pustaka dan literatur perancangan sistem dan analisis pada

penelitian. Pada saran berisi poin-poin dari penulis untuk penelitian berikutnya.

1.7. Sistematika Penulisan

Adapun sistematika penulisan Tugas Akhir ini yaitu sebagai berikut :

BAB I - PENDAHULUAN

Bab pertama berisikan mengenai penjabaran secara sistematis yang berupa bahasan atau topik dari penelitian, bab pertama ini meliputi latar belakang masalah, tujuan dan manfaat, perumusan masalah, batasan masalah, metodologi yang digunakan untuk penelitian, serta mengenai sistematika penulisan.

BAB II - TINJAUAN PUSTAKA

Bab kedua ini berisi tentang dasar dan kerangka teori, serta kerangka pikir penelitian, dimana pada bab ini membahas mengenai IOTA, *Brute force*, DAG, DLT, Node, Signature-based Detection, NIDS dan lain sebagainya yang berkaitan langsung terhadap penelitian ini.

BAB III - METODOLOGI PENELITIAN

Bab ketiga membahas secara sistematis mengenai proses secara bertahap dan terperinci mengenai langkah-langkah yang dilakukan dalam penelitian, guna mencari, mengumpulkan, dan menganalisa data yang dihasilkan selama tahap simulasi terhadap skema IOTA hornet node dan proses serangan *Brute force*, serta akuisisi dataset.

BAB IV - ANALISA DAN HASIL

Bab keempat ini membahas hasil pengujian atau eksperimen dari proses yang telah dilakukan. Serta pada bab ini juga analisis akan dilakukan berdasarkan data yang telah diakuisisi sebelumnya dari hasil pengujian.

BAB V - KESIMPULAN DAN SARAN

Bab kelima atau terakhir ini berisi tentang kesimpulan dan saran berdasarkan hasil dan analisa dari penelitian yang telah dilaksanakan.

DAFTAR PUSTAKA

[1] M. Idhom, H. E. Wahanani, and A. Fauzi, "Network Security System on Multiple Servers Against Brute Force Attacks," *Proceeding - 6th Inf. Technol. Int. Semin. ITIS 2020,* pp. 258–262, 2020, doi: 10.1109/ITIS50118.2020.9321108.

[2] S. Salamatian, W. Huleihel, A. Beirami, A. Cohen, and M. Médard, "Why Botnets Work : Distributed Brute-Force Attacks Need No Synchronization," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 9, pp. 2288–2299, 2019, doi: 10.1109/TIFS.2019.2895955.

[3] S. Salamatian, W. Huleihel, A. Beirami, A. Cohen, and M. Médard, "Centralized vs Decentralized Targeted Brute-Force Attacks : Guessing With Side-Information," vol. 15, pp. 3749–3759, 2020, doi: 10.1109/TIFS.2020.2998949.

[4] S. K. Wanjau, G. M. Wambugu, and G. N. Kamau, "SSH-Brute Force Attack Detection Model based on Deep Learning," *Int. J. Comput. Appl. Technol. Res.*, vol. 10, no. 01, pp. 42–50, 2021, doi: 10.7753/ijcatr1001.1008.

[5] D. Stiawan, S. Sandra, E. Alzahrani, and R. Budiarto, "Comparative analysis of K-Means method and Naïve Bayes method for brute force attack visualization," *2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017*, pp. 177–182, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905286.

[6] S. Singh, A. S. M. Sanwar Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[7] M. Conti, G. Kumar, P. Nerurkar, R. Saha, and L. Vigneri, "A survey on security challenges and solutions in the IOTA," *J. Netw. Comput. Appl.*, vol. 203, no. April, p. 103383, 2022, doi: 10.1016/j.jnca.2022.103383.

[8] M. N. Halgamuge, "Optimization framework for Best Approver Selection Method (BASM) and Best Tip Selection Method (BTSM) for IOTA tangle network: Blockchain-enabled next generation Industrial IoT," *Comput. Networks*, vol. 199, no. August, p. 108418, 2021, doi: 10.1016/j.comnet.2021.108418.

[9] M. Uddin, A. A. Rahman, J. Memon, and N. Uddin, "Algorithm to detect intrusions using multi layer signature based model," *J. Appl. Sci. Res.*, vol. 8, no. 8, pp. 4457–4466, 2012.

[10] P. P. I. and V. V. and I. D. M. and M. D. Logothetis, "A Signature-based Intrusion Detection System for the Internet of Things," *IET Conf. Publ.*, vol. 2018, no. CP747, 2018, doi: 10.1049/cp.2018.1419.

[11] M. Nadeem, A. Arshad, S. Riaz, S. S. Band, and A. Mosavi, "Intercept the

cloud network from brute force and ddos attacks via intrusion detection and prevention system," *IEEE Access*, vol. 9, pp. 152300–152309, 2021, doi: 10.1109/ACCESS.2021.3126535.

[12] A. Waleed, A. F. Jamali, and A. Masood, "Which open-source IDS? Snort, Suricata or Zeek," *Comput. Networks*, vol. 213, no. June, p. 109116, 2022, doi: 10.1016/j.comnet.2022.109116.

[13] A. F. Otoom, W. Eleisah, and E. E. Abdallah, "Deep Learning for Accurate Detection of Brute Force attacks on IoT Networks," *Procedia Comput. Sci.*, vol. 220, pp. 291–298, 2023, doi: 10.1016/j.procs.2023.03.038.

[14] J. Luxemburk, K. Hynek, and T. Cejka, "Detection of HTTPS Brute-Force Attacks with Packet-Level Feature Set," *2021 IEEE 11th Annu. Comput. Commun. Work. Conf.*, pp. 114–122, 2021, doi: 10.1109/CCWC51732.2021.9375998.

[15] P. B. Pramudya, "Implementation of signature-based intrusion detection system using SNORT to prevent threats in network servers," *J. Soft Comput. Explor.*, vol. 3, no. 2, pp. 93–98, 2022, doi: 10.52465/joscex.v3i2.80.

[16] Y. C. Wang, Y. C. Houng, H. X. Chen, and S. M. Tseng, "Network Anomaly Intrusion Detection Based on Deep Learning Approach," *Sensors 2023, 23, 2171.*, 2023, doi: https://doi.org/ 10.3390/s23042171.

[17] K. Su, M. Moe, and T. Win, "Enhanced Honey Encryption Algorithm for Increasing Message Space against Brute Force Attack," *2018 15th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol.*, pp. 86–89, 2018, doi: 10.1109/ecticon.2018.8620050.

[18] M. Sairam and A. T. House, "Cyber Security at a Glance," *2019 Fifth Int. Conf. Sci. Technol. Eng. Math.*, vol. 1, pp. 240–245, 2019.

[19] T. Zheng, Q. Hong, T. Jianwei, Z. Hongyu, and L. Xi, "An Automated Brute Force Method Based on Webpage Static Analysis," *10th Int. Conf. Meas. Technol. Mechatronics Autom.*, pp. 100–103, 2018, doi: 10.1109/ICMTMA.2018.00031.

[20] M. Albahar, D. Alansari, and A. Jurcut, "An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities," *Electron. 2022, 11, 2991*, pp. 1–25, 2022.

[21] N. Sealey, A. Aijaz, and B. Holden, "IOTA Tangle 2 . 0 : Toward a Scalable , Decentralized , Smart , and Autonomous IoT Ecosystem," *2022 Int. Conf. Smart Appl. Commun. Netw.*, 2021.

[22] A. Blaise, M. Bouet, V. Conan, and S. Secci, "Detection of zero-day attacks : An unsupervised port-based approach ☆," vol. 180, no. June, 2020, doi: 10.1016/j.comnet.2020.107391.

[23] J. Díaz-Verdejo, J. Muñoz-Calle, A. E. Alonso, R. E. Alonso, and G.

Madinabeitia, “On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks,” *Appl. Sci.*, vol. 12, no. 2, 2022, doi: 10.3390/app12020852.

[24] C. Liang *et al.*, “Intrusion detection system for the internet of things based on blockchain and multi-agent systems,” *Electron.*, vol. 9, no. 7, 2020, doi: 10.3390/electronics9071120.

[25] Q. Hu, S. Yu, and M. Rizwan, “Analysing performance issues of open-source intrusion detection systems in high-speed networks,” *J. Inf. Secur. Appl.*, vol. 51, p. 102426, 2020, doi: 10.1016/j.jisa.2019.102426.

[26] R. Johari, I. Kaur, R. Tripathi, and K. Gupta, “Penetration Testing in IoT Network,” *2020 5th Int. Conf. Comput. Commun. Secur.*, 2020, doi: 10.1109/icccs49678.2020.9276853.

[27] M. Denis, C. Zena, and T. Hayajneh, “Penetration Testing : Concepts , Attack Methods , and Defense Strategies,” *2016 IEEE Long Isl. Syst. Appl. Technol. Conf.*, 2016, doi: 10.1109/lisat.2016.7494156.

[28] IOTA, “Welcome to HORNET.” https://wiki.iota.org/hornet/welcome/ (accessed Feb. 28, 2024).

[29] V. H. Dixit, A. Doupé, and Z. Zhao, “AIM-SDN : Attacking Information Mismanagement in SDN-datastores,” *2018 ACM SIGSAC Conf.*, 2018, doi: 10.1145/3243734.3243799.