DETEKSI *EXPLOIT REVERSE* HTTPS MENGGUNAKAN METODE *NAIVE BAYES*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer (S1)

OLEH:

RAFI FAJAR TSANI
09011382025115

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2024

LEMBAR PENGESAHAN

DETEKSI EXPLOIT *REVERSE* HTTPS MENGGUNAKAN METODE *NAIVE BAYES*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer (S1)

Oleh:
RAFI FAJAR TSANI
09011382025115

Palembang, 8 November 2024

Mengetahui,

Pembimbing I Tugas Akhir	Pembimbing II Tugas Akhir
Prof. Deris Stiawan, M.T, Ph.D.	**Nurul Afifah, M.Kom**
NIP. 197806172006041002	**NIP. 199211102023212049**

Ketua Jurusan Sistem Komputer

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

AUTHENTICATION PAGE

DETEKSI EXPLOIT *REVERSE* HTTPS MENGGUNAKAN METODE *NAIVE BAYES*

THESIS

Dept. Of Computer System

Bachelor's Degree

By:

RAFI FAJAR TSANI

09011382025115

Palembang, 7 November 2024

Know,

Supervisor

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

Co-Supervisor

Nurul Afifah, M.Kom
NIP. 199211102023212049

Ketua Jurusan Sistem Komputer

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

LEMBAR PERSETUJUAN

Telah di uji pada :

Hari : Jumat

Tanggal : 18 Oktober 2024

Tim Penguji :

1. **Ketua** : **Aditya Putra Perdana P, M.T**
2. **Penguji** : **Ahmad Heryanto, M.T**
3. **Pembimbing 1** : **Prof. Deris Stiawan, M.T., Ph.D**
4. **Pembimbing 2** : **Nurul Afifah, M.Kom**

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Rafi Fajar Tsani

NIM : 09011382025115

Judul : Deteksi Exploit Reverse HTTPS Menggunakan Metode Naive Bayes.

Hasil Pengecekan Software *Thenticate/Turnitin* : 11%

Menyatakan Bahwa Skirpsi saya merupakan hasil karya sendiri dan bukan penjiplakan atau plagiat. Apabila ditemukan unsur penjiplatan atau plagiat dalam Skirpsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun

Palembang, November 2024

Rafi Fajar Tsani

NIM. 09011382025115

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Puji dan syukur penulis ucapkan atas kehadirat Allah SWT. Yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan tugas akhir dengan judul **"Deteksi *Exploit Reverse* HTTPS Menggunakan Metode *Naive Bayes*"**

Pada penyusunan tugas akhir ini tidak terlepas dari peran berbagai pihak yang telah memberikan dukungan doa, semngat, motivasi dan bimbingan pada penulis. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT. yang telah memberikan nikmat Kesehatan dan Kesempatan kepada penulis dalam penyusunan tugas akhir ini.
2. Kedua orang tua tercinta yang selalu memberikan dukungan moral maupun finansial, serta do'a yang tiada hentinya.
3. Adik - Adik ku yang selalu memberikan semangat dan do'a.
4. Bapak Dr. Erwin, M.Si selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Prof. Dr. Ir. Bambang Tutuko, M.T. selaku Dosen Pembimbing Akademik.
7. Bapak Deris Stiawan, M.T., Ph.D., IPU., ASEAN-Eng., CPENT selaku Pembimbing I Tugas Akhir Penulis yang telah meluangkan waktu untuk membimbing dan memberikan motivasi selama pengerjaan Tugas Akhir.
8. Mbak Nurul Afifah, M.Kom. selaku Pembimbing II Tugas Akhir yang telah meluangkan waktu untuk membimbing penulis dalam pengerjaan Tugas Akhir dari awal laporan Tugas Akhir.
9. Mba Sari Anhar selaku admin yang telah membantu dalam proses administrasi Tugas Akhir Penulis.

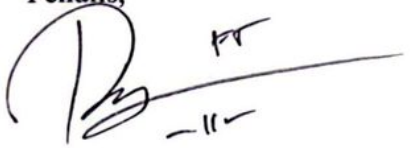
10. Teman-teman satu kelompok riset yang selalu memberikan semangat dan solusi kepada penulis yaitu Virginita Putri Lestari, Azzan Daffa AlKautsar, Alessandro Lumban Tungkup dan Bayu Cailendra
11. Teman-teman terdekat selama kuliah yang selalu support.
12. Teman-teman seperjuangan Jurusan Sistem Komputer Unggulan 2020.
13. Seluruh pihak yang tidak dapat penulis sebutkan satu per satu, yang telah memberikan semangat serta doa.
14. Almamater

Penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis dengan senang hati menerima kritik dan saran serta masukkan dari pembaca yang bersifat membangun agar lebih baik lagi dikemudian hari. Penulis berharap semoga laporan ini dapat bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya. Demikian yang dapat penulis sampaikan.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, November 2024

Penulis,



Rafi Fajar Tsani

NIM. 09011382025115

DETEKSI *EXPLOIT REVERSE* HTTPS MENGGUNAKAN METODE *NAIVE BAYES*

RAFI FAJAR TSANI (09011382025115)

Jurusan Sistem Komputer, Fakultas ilmu komputer

Universitas Sriwijaya

Email : 09011382025115@student.unsri.ac.ic

ABSTRAK

Keamanan aplikasi web berbasis protokol HTTPS (Hypertext Transfer Protocol Secure) menjadi semakin penting. Meskipun penggunaan protokol HTTPS memberikan lapisan keamanan tambahan melalui enkripsi data, tetap ada masalah terkait serangan keamanan, termasuk exploit reverse. Exploit reverse adalah taktik serangan yang dapat memungkinkan akses yang tidak sah ke aplikasi web dan dapat merusak integritas aplikasi web, penelitian ini memfokuskan pada pengembangan metode deteksi menggunakan pendekatan algoritma deteksi Naive Bayes. Algoritma ini dikenal efektif dalam konteks analisis teks dan deteksi data berbasis probabilitas. Penerapan Naive Bayes dalam deteksi exploit reverse diharapkan dapat memberikan solusi yang cerdas dan responsif terhadap ancaman keamanan pada aplikasi web berbasis HTTPS. Penelitian ini menggunakan dataset sebanyak 15.089 file .pcap mentah yang diproses dan diekstrak menjadi 3.280 sampel terlabel dalam format CSV, mencakup 2.124 data normal dan 1.155 data serangan yang berasal dari skenario Victim Reverse HTTPS yang dilakukan di Laboratorium COMNETS UNSRI. Hasil penelitian menunjukkan bahwa model tersebut mampu mencapai akurasi sebesar 93%.

Kata Kunci : *Exploit Revese, Naive Bayes*, Snort-IDS.

DETEKSI *EXPLOIT REVERSE* HTTPS MENGGUNAKAN METODE *NAIVE BAYES*

RAFI FAJAR TSANI (09011382025115)

Departement of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email : 09011382025115@student.unsri.ac.ic

ABSTRACT

The security of web applications based on the HTTPS (Hypertext Transfer Protocol Secure) protocol is becoming increasingly important. Although using the HTTPS protocol adds an extra layer of security through data encryption, there are still security threats, including reverse exploits. A reverse exploit is an attack tactic that can allow unauthorized access to a web application and compromise its integrity. This research focuses on developing a detection method using the Naive Bayes detection algorithm approach. This algorithm is known to be effective in text analysis and probability-based data detection. The application of Naive Bayes in reverse exploit detection is expected to provide an intelligent and responsive solution to security threats in HTTPS-based web applications. This study uses a dataset of 15,089 raw .pcap files, which were processed and extracted into 3,280 labeled samples in CSV format, consisting of 2,124 normal data and 1,155 attack data from a Victim Reverse HTTPS scenario conducted in the COMNETS UNSRI Laboratory. The research results show that the model achieved an accuracy of 93%.

Kata Kunci : *Exploit Revese, Naive Bayes*, Snort-IDS.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Analisis network traffic telah menjadi semakin penting di masa sekarang untuk memantau lalu lintas jaringan. Dalam beberapa tahun terakhir, administrator hanya memantau sejumlah kecil perangkat jaringan atau kurang dari seribu komputer. Analisis network traffic dapat mengembangkan skema pengendalian kemacetan network traffic dan untuk mengetahui paket normal dan berbahaya [1]. Skema ini menargetkan untuk menghindari kemacetan jaringan dengan mendistribusikan sumber daya jaringan sehubungan dengan lalu lintas yang diperkirakan.

Keamanan aplikasi web berbasis protokol HTTPS (Hypertext Transfer Protocol Secure) menjadi semakin penting. Meskipun penggunaan protokol HTTPS memberikan lapisan keamanan tambahan melalui enkripsi data, tetap ada masalah terkait serangan keamanan, termasuk exploit reverse. Exploit reverse adalah taktik serangan yang dapat memungkinkan akses yang tidak sah ke aplikasi web dan dapat merusak integritas aplikasi web [2]. Dalam situasi seperti ini, aplikasi web yang menggunakan protokol HTTPS tidak dapat dianggap aman sepenuhnya dari serangan, termasuk serangan *exploit reverse*. Oleh karena itu, penelitian ini berkonsentrasi pada pengembangan teknik deteksi yang dapat mengidentifikasi dan mencegah serangan exploit reverse yang mungkin terjadi dari trafik aplikasi web yang menggunakan protokol HTTPS.

Exploit Reverse HTTPS biasanya digunakan dalam serangan penetrasi atau pentesting. Exploit ini memanfaatkan kerentanan dalam sistem korban untuk membuat koneksi HTTPS yang terenkripsi ke sistem penyerang, memungkinkan penyerang untuk mendapatkan akses ke sistem korban tanpa diketahui oleh korban [3]. Dalam rangka menghadapi risiko tersebut, penelitian ini memfokuskan pada pengembangan metode deteksi menggunakan

pendekatan algoritma deteksi *Naive Bayes*. Algoritma ini dikenal efektif dalam konteks analisis teks dan deteksi data berbasis probabilitas. [4] Penerapan *Naive Bayes* dalam deteksi *exploit reverse* diharapkan dapat memberikan solusi yang cerdas dan responsif terhadap ancaman keamanan pada aplikasi web berbasis HTTPS.

Pendekatan yang diusung dalam penelitian ini mencakup penerapan metode *Dynamic Analysis*, sebuah pendekatan analisis yang memperhitungkan perubahan dan fluktuasi dalam data lalu lintas jaringan. [5] *Dynamic Analysis* memungkinkan sistem untuk beradaptasi dengan perubahan perilaku jaringan seiring waktu, yang penting untuk mendeteksi tanda-tanda serangan yang mungkin berkembang dan berubah seiring waktu. *Dynamic Analysis* dilakukan dengan menjalankan sampel malware pada ruang lingkup yang dikontrol dan diawasi selama operasinya. Dalam situasi seperti ini, metode terbaik untuk mendeteksi fungsi malware adalah *Dynamic Analysis*.

Naive Bayes (NB) merupakan salah satu data mining yang paling terkenal untuk deteksi dalam teknik machine learning yang didasarkan pada teorema Bayes dengan asumsi bahwa fitur-fitur (variabel independen) yang digunakan dalam model klasifikasi adalah independen satu sama lain. Naive Bayes bekerja dengan menghitung probabilitas posterior dari setiap kelas berdasarkan nilai fitur dan menggunakan teorema Bayes untuk menentukan kelas yang paling mungkin. [6] Metode ini cukup cepat dan mudah diimplementasikan, bahkan dengan jumlah data yang besar. [7] Dalam menghadapi kompleksitas dan dinamika serangan keamanan terhadap aplikasi web berbasis HTTPS, diperlukan pendekatan deteksi yang cerdas dan efektif. Salah satu model yang menjadi fokus dalam penelitian ini adalah metode *Naive Bayes*.

Menurut Penelitian mengenai “Twitter Spam Detection Using Naïve Bayes Classifier” [8] analisis metode memiliki ketepatan akurasi 95%. Dalam mendeteksi tweet atau tren jahat yang merugikan atau tidak diinginkan pengguna dalam dunia sosial saat ini dapat disimpulkan bahwa metode ini memberikan kinerja yang baik dalam mendeteksi spam.

Menurut penelitian mengenai "Short Message Service (SMS) Spam Detection and Classification Using Naïve Bayes" [9] analisis metode memiliki ketepatan akurasi 92%. Dalam mendeteksi dan mengklasifikasikan pesan spam SMS. Penelitian ini bertujuan untuk membantu masyarakat menghindari pesan-pesan yang menipu yang meminta informasi pribadi. Penelitian selanjutnya akan berfokus pada meningkatkan kinerja klasifikasi dengan set fitur tambahan.

Berdasarkan pembahasan diatas, penulis melakukan penelitian yang berjudul **"Deteksi *Exploit Reverse* HTTPS Menggunakan Metode *Naive Bayes*".** Diharapkan penelitian tugas akhir ini dapat menghasilkan nilai *accuracy, precission* dan *f1-score* yang baik sehingga dapat menjadi referensi untuk peneliti selanjutnya.

1.2 Rumusan Masalah

Berikut ini rumusan masalah penelitian Tugas Akhir yang akan dilakukan:

1. Bagaimana melakukan ekstraksi dataset *Reverse* HTTPS?
2. Bagaimana cara mengatasi Data Imbalance?
3. Bagaimana mendeteksi adanya serangan *Reverse* HTTPS?

1.3 Batasan Masalah

Berikut ini rumusan masalah penelitian Tugas Akhir yang akan dilakukan:

1. Penelitian ini menggunakan dataset pada *Mobile-Trojan Metasploit Traffic*, terutama pada skenario *Victim Reverse* HTTPS. Dataset ini mencakup jaringan WiFi, dan hanya hasil dari skenario 2 (Victim 2) yang akan dianalisis.
2. Penelitian ini akan berfokus pada penerapan metode deteksi berbasis *Dynamic Analysis* dan *Naive bayes* untuk menganalisis dan mendeteksi pola-pola karakteristik serangan.

3. Nilai performasi yang diukur adalah accuracy, precision, recall dan f1-score.

1.4 Tujuan Penelitian

Berikut ini merupakan tujuan dari penelitian Tugas Akhir yang dilakukan:

1. Melakukan ekstraksi dataset dengan format .pcap menjadi .csv menggunakan CICFlowMeter.
2. Menerapkan teknik Random Oversampling untuk mengatasi dataset imbalance pada dataset Reverse HTTPS
3. Menerapkan teknik *Snort – IDS* dan teknik *Naive Bayes* untuk mengetahui serangan malware Reverse HTTPS.

1.5 Manfaat Penelitian

Berikut ini merupakan manfaat dari penelitian Tugas Akhir yang dilakukan:

1. Menambahkan pemahaman mengenai proses ekstraksi dataset *CICFlowMeter.*
2. Dapat mengatasi permasalahan dataset yang tidak seimbang menggunakan teknik Random Oversampling.
3. Dapat Mengetahui serangan malware Reverse HTTPS dengan menggunakan Snort – IDS.

1.6 Metodologi Penelitian

Berikut ini metodologi yang digunakan dalam penelitian ini sebagai berikut:

1. Metode Studi Pustaka (Literature)

Pada tahapan ini memberikan landasan teoritis yang diperlukan untuk pemahaman model *Dynamic Analysis* dan *Naive Bayes*, karakteristik serangan *exploit reverse*, serta penggunaan model *Naive Bayes* dalam mendeteksi serangan pada aplikasi web berbasis HTTPS. Penelitian ini menggabungkan

konsep-konsep ini untuk mengembangkan metode deteksi yang dapat meningkatkan keamanan aplikasi berbasis HTTPS.

2. Metode Pengumpulan Data

Pengumpulan data dilakukan melalui proses perekaman *network traffic* pada aplikasi web berbasis HTTPS. Penggunaan tools monitoring jaringan seperti Wireshark akan membantu mengidentifikasi pola traffic yang mungkin mengindikasikan serangan *exploit reverse*. Data yang diperoleh akan menjadi dasar dalam melatih dan menguji model *Naive Bayes*.

3. Metode Pengolahan Data

Metode pengolahan data ini bertujuan memastikan dataset yang digunakan dalam penelitian memiliki kualitas baik dan siap untuk digunakan oleh model *Dynamic Analysis* dan *Naive Bayes*. Metode pengolahan dataset *Mobile-Trojan Metasploit Traffic* diarahkan untuk menyajikan dataset *Victim Reverse HTTPS* yang bersih, relevan, dan siap digunakan dalam pelatihan dan evaluasi model *Dynamic Analysis* dan *Naive Bayes*. Pada tahap ini diharapkan dapat meningkatkan akurasi dan kinerja model dalam mendeteksi serangan *exploit reverse* pada aplikasi berbasis HTTPS.

4. Metode Analisa

Metode ini dilakukan dengan menganalisa hasil yang didapat dari pengolahan data Tugas Akhir yang kemudian divalidasi untuk membuat kesimpulan.

5. Metode Kesimpulan dan Saran

Metode ini dilakukan setelah menganalisa penelitian secara keseluruhan untuk membuat kesimpulan Tugas Akhir serta memberikan saran yang dapat dijadikan referensi bagi peneliti selanjutnya.

1.7 Sistematika Penulisan

Berikut ini merupakan sistematika yang digunakan dalam penulisan Tugas Akhir ini:

BAB I PENDAHULUAN

Bab ini terdapat Latar Belakang penelitian yang dilakukan, Rumusan Masalah, Batasan Masalah, Tujuan Penelitan, Manfaat Penelitian, Metodologi Penelitian dan Sistematika Penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai Menjelaskan konsep dasar model *Naive Bayes*, review literatur tentang deteksi serangan *exploit reverse*, serta kajian-kajian terkini seputar penggunaan model *Dynamic Analysis dan Naive Bayes* dalam keamanan aplikasi web.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai Langkah-langkah (Metodologi) penelitian, Mendeskripsikan metode yang digunakan dalam penelitian, termasuk pemilihan dataset, langkah-langkah deteksi, dan evaluasi hasil.

BAB IV HASIL DAN ANALISA

Bab ini menjelaskan hasil dari proses pengolahan data yang sudah dilakukan, dan dari hasil tersebut akan dilakukan analisa untuk mendapatkan data yang akurat.

BAB V KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan yang yang didapatkan berdasarkan hasil dan analisa yang diperoleh setelah melakukan penelitian, kemudian memberikan saran agar dapat dilakukan pengembangan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] M. Joshi and T. H. Hadi, “A Review of Network Traffic Analysis and Prediction Techniques,” 2015.

[2] K. Kaushik, E. Studies, and S. Aggarwal, “A novel approach to generate a reverse shell: Exploitation and Prevention,” *Int. J. Intell. Commun. Comput. Networks*, vol. 2, no. 2, 2021, doi: 10.51735/ijiccn/001/33.

[3] Y. Liu, R. Cai, X. Yin, and S. Liu, “An Exploit Traffic Detection Method Based on Reverse Shell,” *Appl. Sci.*, vol. 13, no. 12, 2023, doi: 10.3390/app13127161.

[4] S. Wang, Z. Chen, Q. Yan, B. Yang, L. Peng, and Z. Jia, “A mobile malware detection method using behavior features in network traffic,” *J. Netw. Comput. Appl.*, vol. 133, no. December 2018, pp. 15–25, 2019, doi: 10.1016/j.jnca.2018.12.014.

[5] V. A. Manoppo, A. S. . Lumenta, and S. D. . Karouw, “Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi,” *Tek. Elektro Dan Komput.*, vol. 9, no. 3, p. 182, 2020.

[6] S. Chen, G. I. Webb, L. Liu, and X. Ma, “A novel selective naïve Bayes algorithm,” *Knowledge-Based Syst.*, vol. 192, p. 105361, 2020, doi: 10.1016/j.knosys.2019.105361.

[7] A. E. Wijaya, R. Bani, S. Sukarni, and S. A. Weighting, “Jurnal Teknologi Informasi dan Komunikasi STMIK Subang, Oktober 2019 ISSN: 2252-4517,” no. April, pp. 100–110, 2019.

[8] K. U. Santoshi, S. S. Bhavya, Y. B. Sri, and B. Venkateswarlu, “Twitter Spam Detection Using Naïve Bayes Classifier,” in *Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT 2021*, 2021, pp. 773–777. doi: 10.1109/ICICT50816.2021.9358579.

[9] C. B. Asaju and J. Ekorabon, “Short Message Service (Sms) Spam Detection and Classification Using Naïve Bayes,” vol. 11, no. 40, pp. 4931–

4936, 2021.

[10] X. Yun, J. Xie, S. Li, Y. Zhang, and P. Sun, “Detecting unknown HTTP-based malicious communication behavior via generated adversarial flows and hierarchical traffic features,” *Comput. Secur.*, vol. 121, p. 102834, 2022, doi: 10.1016/j.cose.2022.102834.

[11] B. A. Pratomo, P. Burnap, and G. Theodorakopoulos, “BLATTA: Early Exploit Detection on Network Traffic with Recurrent Neural Networks,” *Secur. Commun. Networks*, vol. 2020, no. Vm, 2020, doi: 10.1155/2020/8826038.

[12] F. Araujo, K. W. Hamlen, S. Biedermann, and S. Katzenbeisser, “From patches to honey-patches: Lightweight attacker misdirection, deception, and disinformation,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2014, pp. 942–953. doi: 10.1145/2660267.2660329.

[13] K. Hynek, D. Vekshin, J. Luxemburk, T. Cejka, and A. Wasicek, “Summary of DNS over HTTPS Abuse,” *IEEE Access*, vol. 10, pp. 54668–54680, 2022, doi: 10.1109/ACCESS.2022.3175497.

[14] D. Gengsheng, L. Zhe, Z. Jingjing, and F. Aiying, “Application research of HTTPS service architecture based on pan DNS in IPv6 transition stages,” *2017 9th Int. Conf. Adv. Infocomm Technol. ICAIT 2017*, pp. 84–89, 2018, doi: 10.1109/ICAIT.2017.8388894.

[15] T. Mokoena and T. Zuva, “Malware analysis and detection in enterprise systems,” *Proc. - 15th IEEE Int. Symp. Parallel Distrib. Process. with Appl. 16th IEEE Int. Conf. Ubiquitous Comput. Commun. ISPA/IUCC 2017*, pp. 1304–1310, 2018, doi: 10.1109/ISPA/IUCC.2017.00199.

[16] S. Chakrabarti, M. Chakraborty, and I. Mukhopadhyay, “Study of snort-based IDS,” *ICWET 2010 - Int. Conf. Work. Emerg. Trends Technol. 2010, Conf. Proc.*, no. February 2010, pp. 43–47, 2010, doi: 10.1145/1741906.1741914.

[17] J. Reynaldo, P. P. Adikara, and R. C. Wihandika, “Analisis Sentimen Mengenai Produk Toyota Avanza Menggunakan Metode Learning Vector Quantization Versi 3 (LVQ 3) dengan Seleksi Fitur Chi Square, Lexicon …,” *… Teknol. Inf. dan …*, vol. 4, no. 3, pp. 830–839, 2020.

[18] R. Das, S. K. Biswas, D. Devi, and B. Sarma, “An Oversampling Technique by Integrating Reverse Nearest Neighbor in SMOTE: Reverse-SMOTE,” *Proc. - Int. Conf. Smart Electron. Commun. ICOSEC 2020*, no. Icosec, pp. 1239–1244, 2020, doi: 10.1109/ICOSEC49089.2020.9215387.

[19] M. S. Shelke, P. R. Deshmukh, and P. V. K. Shandilya, “A Review on Imbalanced Data Handling Using Undersampling and Oversampling Technique,” *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 4, pp. 444–449, 2017, doi: 10.23883/ijrter.2017.3168.0uwxm.

[20] A. D. Wibisono, S. Dadi Rizkiono, and A. Wantoro, “Filtering Spam Email Menggunakan Metode Naive Bayes,” *TELEFORTECH J. Telemat. Inf. Technol.*, vol. 1, no. 1, 2020, doi: 10.33365/tft.v1i1.685.

[21] N. Pramesti, “Klasifikasi Persediaan Barang Menggunakan Naïve Bayes,” *J. Data Sci. Inform.*, vol. 1, no. 2, pp. 53–57, 2021.

[22] Rayuwati, Husna Gemasih, and Irma Nizar, “IMPLEMENTASI AlGORITMA NAIVE BAYES UNTUK MEMPREDIKSI TINGKAT PENYEBARAN COVID,” *Jural Ris. Rumpun Ilmu Tek.*, vol. 1, no. 1, pp. 38–46, 2022, doi: 10.55606/jurritek.v1i1.127.

[23] E. K. Ampomah, G. Nyame, Z. Qin, P. C. Addo, E. O. Gyamfi, and M. Gyan, “Stock market prediction with gaussian naïve bayes machine learning algorithm,” *Inform.*, vol. 45, no. 2, pp. 243–256, 2021, doi: 10.31449/inf.v45i2.3407.

[24] Nurul A’ayunnisa, Y. Salim, and H. Azis, “Analisis Performa Metode Gaussian Naïve Bayes untuk Klasifikasi Citra Tulisan Tangan Karakter Arab,” *Indones. J. Data Sci.*, vol. 3, no. 3, pp. 115–121, 2022, doi: 10.56705/ijodas.v3i3.54.

[25] A. O. Salau, T. A. Assegie, A. T. Akindadelo, and J. N. Eneh, “Evaluation of Bernoulli Naive Bayes model for detection of distributed denial of service attacks,” *Bull. Electr. Eng. Informatics*, vol. 12, no. 2, pp. 1203–1208, 2023, doi: 10.11591/eei.v12i2.4020.

[26] M. Heydarian, T. E. Doyle, and R. Samavi, “MLCM: Multi-Label Confusion Matrix,” *IEEE Access*, vol. 10, pp. 19083–19095, 2022, doi: 10.1109/ACCESS.2022.3151048.

[27] N. Khamphakdee, N. Benjamas, and S. Saiyod, “Improving intrusion detection system based on snort rules for network probe attacks detection with association rules technique of data mining,” *J. ICT Res. Appl.*, vol. 8, no. 3, pp. 234–250, 2015, doi: 10.5614/itbj.ict.res.appl.2015.8.3.4.