UNIVERSITAS
GADJAH MADA
Implementasi Analisis Data Honeypot Berbasis YARA dan Large Language Model Untuk Identifikasi Ancaman Siber
Emanuel Dananjaya Kusumadewa Biansa Dua, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR PUSTAKA

[1] K. Hobert, C. Lim, and E. Budiarto, "Enhancing Cyber Attribution through Behavior Similarity Detection on Linux Shell Honeypots with ATT&CK Framework," *Proc. - 2023 IEEE Int. Conf. Cryptogr. Informatics, Cybersecurity Cryptogr. Cybersecurity Roles, Prospect. Challenges, ICoCICs 2023*, pp. 139–144, 2023, doi: 10.1109/ICoCICs58778.2023.10276639.

[2] A. Ghourabi, T. Abbes, and A. Bouhoula, "Data analyzer based on data mining for honeypot router," *2010 ACS/IEEE Int. Conf. Comput. Syst. Appl. AICCSA 2010*, pp. 1–6, 2010, doi: 10.1109/AICCSA.2010.5587041.

[3] M. S. Tok, M. Dener, and M. Demirci, "Processing Honeypot Logs with Big Data and Data Visualization via Hadoop- Power BI Integration," in *15th International Conference on Information Security and Cryptography, ISCTURKEY 2022 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 49–54. doi: 10.1109/ISCTURKEY56345.2022.9931797.

[4] Ryandy, C. Lim, and K. E. Silaen, "XT-Pot: eXposing Threat Category of Honeypot-based attacks," *ACM Int. Conf. Proceeding Ser.*, no. September 2020, 2020, doi: 10.1145/3429789.3429868.

[5] D.--L. M. de G. Esteban, M. Hamdaqa, and M. Chouchen, *Mining the YARA Ecosystem: From Ad-Hoc Sharing to Data-Driven Threat Intelligence*, vol. 1, no. 1. arXiv, 2026. [Online]. Available: http://arxiv.org/abs/2603.14191

[6] V. Valeros and S. Garcia, "CTU Hornet 65 Niner: A network dataset of geographically distributed low-interaction honeypots," *Data Br.*, vol. 58, p. 111261, 2025, doi: 10.1016/j.dib.2024.111261.

[7] I. G. Adnyana, A. M. Dirgayusari, and K. J. Atmaja, "Data Visualization for Building a Cyber Attack Monitoring Dashboard Based on Honeypot," *Sinkron*, vol. 8, no. 4, pp. 2510–2518, 2024, doi: 10.33395/sinkron.v8i4.14144.

UNIVERSITAS
GADJAH MADA
Implementasi Analisis Data Honeypot Berbasis YARA dan Large Language Model Untuk Identifikasi Ancaman Siber
Emanuel Dananjaya Kusumadewa Biansa Dua, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

[8] R. A. Bridges, T. R. Mitchell, M. Muñoz, and T. Henriksson, "SoK: Honeypots & LLMs, More Than the Sum of Their Parts?," pp. 1–18, 2026, [Online]. Available: http://arxiv.org/abs/2510.25939

[9] A. Yudhistira and Y. Fitrisia, "Monitoring Log Server Dengan Elasticsearch, Logstash Dan Kibana (Elk)," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 8, no. 1, pp. 124–134, 2023, doi: 10.36341/rabit.v8i1.2975.

[10] Rakhmadi Rahman, A.Nurul Sairah, and Amanda Putri Heryanti, "Implementasi Sistem Monitoring Keamanan Jaringan Menggunakan Log Analysis," *J. Ris. Sist. Inf.*, vol. 3, no. 2, pp. 30–34, 2026, doi: 10.69714/fqg13p25.

[11] R. H. Mahdi and H. Trabelsi, "Detection of Malware by Using YARA Rules," *2024 21st Int. Multi-Conference Syst. Signals Devices, SSD 2024*, pp. 568–575, 2024, doi: 10.1109/SSD61670.2024.10549308.

[12] W. Sholihah, S. Pripambudi, and A. Mardiyono, "Log Event Management Server Menggunakan Elastic Search Logstash Kibana (ELK Stack)," *JTIM J. Teknol. Inf. dan Multimed.*, vol. 2, no. 1, pp. 12–20, 2020, doi: 10.35746/jtim.v2i1.79.

[13] S. Biswa, P. Wangmo, T. Rangdel, and T. Wangchuk, "Securing Network using Honeypots : A Comparative Study on Honeytrap and T-Pot," vol. VII, no. I, pp. 12–20, 2025.

[14] T. Human *et al.*, "D Ata S Haring I : P Rinciples of D Ata S Haring," *Methods*, pp. 2002–2002, 2003.

[15] M. Faris, M. Fuzi, M. F. Mazlan, M. Nabil, F. Jamaluddin, and I. Hazwam, "Performance analysis of network intrusion detection using T-Pot honeypots," *J. Comput. Res. Innov.*, vol. 9, no. 2, pp. 348–360, 2024, doi: 10.24191/jcrinn.v9i2.477.

[16] A. Balogh, M. Ersok, K. Eszter, and A. Banati, "Possibilities for Optimization of Real Time Attacker Profiling with Honeypots," *SACI, IEEE Int. Symp. Appl. Comput. Intell. Informatics*, no. 2025, pp. 111–116, 2025, doi: 10.1109/SACI66288.2025.11030113.

[17] R. Djap, C. Lim, K. E. Silaen, and A. Yusuf, "XB-Pot: Revealing Honeypot-

UNIVERSITAS
GADJAH MADA
Implementasi Analisis Data Honeypot Berbasis YARA dan Large Language Model Untuk Identifikasi Ancaman Siber
Emanuel Dananjaya Kusumadewa Biansa Dua, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

based Attacker's Behaviors," *2021 9th Int. Conf. Inf. Commun. Technol. ICoICT 2021*, pp. 550–555, 2021, doi: 10.1109/ICoICT52021.2021.9527422.

[18] D. McAlpine, J. Haseeb, and V. Kumar, "Explaining Cyber Attacks Captured on Honeypots Through Attacker Issued Commands," *2025 IEEE 35th Int. Telecommun. Networks Appl. Conf.*, pp. 1–4, 2025, doi: 10.1109/itnac66378.2025.11302674.

[19] K. Yıldırım, M. E. Demir, T. Keleş, A. M. Yıldız, Ş. Doğan, and T. Tuncer, "A YARA-based approach for detecting cyber security attack types," *Firat Univ. J. Exp. Comput. Eng.*, vol. 2, no. 2, pp. 55–68, 2023, doi: 10.5505/fujece.2023.09709.

[20] C. Nilă and V.-V. Patriciu, "LLMs for Web Reconnaissance Detection," *J. Mil. Technol.*, vol. 6, no. 2, pp. 41–46, 2023, doi: 10.32754/jmt.2023.2.07.

[21] A. Iyengar and A. Kundu, "Large Language Models and Computer Security," *Proc. - 2023 5th IEEE Int. Conf. Trust. Priv. Secur. Intell. Syst. Appl. TPS-ISA 2023*, pp. 307–313, 2023, doi: 10.1109/TPS-ISA58951.2023.00045.

[22] R. Purwoko, D. P. Febriyan, G. P. Adhe, W. S. Y. Laksito, S. Siswanti, and M. Hasbi, "JEPIN (Jurnal Edukasi dan Penelitian Informatika) Honeypot-as-a-Service dengan Kubernetes Cluster," *Jepin (Jurnal Edukasi dan Penelit. Inform.*, vol. 9, no. 2, pp. 204–2017, 2023.

[23] R. M. Campbell, K. Padayachee, and T. Masombuka, "A survey of honeypot research: Trends and opportunities," *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015*, pp. 208–212, 2016, doi: 10.1109/ICITST.2015.7412090.

[24] A. S. Nair, J. S. Mathew, A. S. Bhati, Mohana, and A. Chakkan, "Analyzing Cyber Attack Patterns and Detection Strategies Through T-Pot Honeypot Deployment," *Proc. 6th Int. Conf. Smart Electron. Commun. ICOSEC 2025*, pp. 1899–1903, 2025, doi: 10.1109/ICOSEC67334.2025.11459680.

[25] S. A. Raghul, G. Gayathri, R. Bhatt, and K. A. Varun Kumar, "Enhancing Cybersecurity Resilience: Integrating IDS with Advanced Honeypot Environments for Proactive Threat Detection," *Proc. 3rd Int. Conf. Appl.*

UNIVERSITAS
GADJAH MADA
Implementasi Analisis Data Honeypot Berbasis YARA dan Large Language Model Untuk Identifikasi Ancaman Siber
Emanuel Dananjaya Kusumadewa Biansa Dua, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Artif. Intell. Comput. ICAAIC 2024, pp. 1363–1368, 2024, doi: 10.1109/ICAAIC60222.2024.10575865.

[26] N. Naik, P. Jenkins, R. Cooke, J. Gillett, and Y. Jin, "Evaluating Automatically Generated YARA Rules and Enhancing Their Effectiveness," *2020 IEEE Symp. Ser. Comput. Intell. SSCI 2020*, pp. 1146–1153, 2020, doi: 10.1109/SSCI47803.2020.9308179.

[27] N. Naik, P. Jenkins, N. Savage, L. Yang, K. Naik, and J. Song, "Embedding Fuzzy Rules with YARA Rules for Performance Optimisation of Malware Analysis," *IEEE Int. Conf. Fuzzy Syst.*, vol. 2020-July, 2020, doi: 10.1109/FUZZ48607.2020.9177856.

[28] R. Stoleriu, A. Puncioiu, and I. Bica, "Cyber Attacks Detection Using Open Source ELK Stack," *Proc. 13th Int. Conf. Electron. Comput. Artif. Intell. ECAI 2021*, pp. 1–6, 2021, doi: 10.1109/ECAI52376.2021.9515120.

[29] M. Bajer, "Building an IoT data hub with elasticsearch, Logstash and Kibana," *Proc. - 2017 5th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2017*, vol. 2017-Janua, pp. 63–68, 2017, doi: 10.1109/FiCloudW.2017.101.

[30] F. Maymí, R. Bixler, R. Jones, and S. Lathrop, "Towards a definition of cyberspace tactics, techniques and procedures," *Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017*, vol. 2018-Janua, pp. 4674–4679, 2017, doi: 10.1109/BigData.2017.8258514.

[31] A. Abo-alian, M. Youssef, and N. L. Badr, "A data-driven approach to prioritize MITRE ATT&CK techniques for active directory adversary emulation," *Sci. Rep.*, vol. 15, no. 1, pp. 1–23, 2025, doi: 10.1038/s41598-025-12948-x.

[32] S. Kanj, G. Vila, and J. Pegueroles, "Automating the Detection of Evasive Windows Malware: An Evaluated YARA Rule Library for Anti-VM and Anti-Sandbox Techniques," *J. Cybersecurity Priv.*, vol. 6, no. 2, pp. 1–25, 2026, doi: 10.3390/jcp6020069.

[33] J. A. Christli, C. Lim, and Y. Andrew, "AI-Enhanced Honeypots: Leveraging LLM for Adaptive Cybersecurity Responses," *ICITEE 2024 - Proc. 16th Int.*

UNIVERSITAS
GADJAH MADA
Implementasi Analisis Data Honeypot Berbasis YARA dan Large Language Model Untuk Identifikasi Ancaman Siber
Emanuel Dananjaya Kusumadewa Biansa Dua, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Conf. Inf. Technol. Electr. Eng. 2024, pp. 451–456, 2024, doi: 10.1109/ICITEE62483.2024.10808265.

[34] IBM. "*What IS LLM*.". [Online]. Available: https://www.ibm.com/id-id/think/topics/large-language-models, Diakses: 21 Mei 2026

[35] A. R. Sajun, I. Zualkernan, and D. Sankalpa, "A Historical Survey of Advances in Transformer Architectures," *Appl. Sci.*, vol. 14, no. 10, 2024, doi: 10.3390/app14104316.

[36] Analytics Vidhya. "*LLM vs Agents: Choosing the Right Solution for Your Needs*". [Online]. Available: https://www.analyticsvidhya.com/articles/llm-vs-agents/, Diakses: 20 Mei 2026

[37] Larson, Alisa, MTS. 2024. "OpenAI". [Online]. Available: https://ebsco.com/research-starters/computer-science/openai, Diakses: 20 Mei 2026

[38] OpenAI *et al.*, *GPT-4 Technical Report*, vol. 4. 2024. [Online]. Available: http://arxiv.org/abs/2303.08774

[39] Ivan Belcic, Cole Stryker. "What is GPT-4o?". [Online]. Available: https://www.ibm.com/id-id/think/topics/gpt-4o, Diakses 21 Mei 2026

[40] A. Salem, S. Banescu, and A. Pretschner, "Maat: Automatically Analyzing VirusTotal for Accurate Labeling and Effective Malware Detection," *ACM Trans. Priv. Secur.*, vol. 24, no. 4, pp. 1–38, 2021, doi: 10.1145/3465361.

[41] A. S. Tanenbaum, *Distributed Systems: Principles and Paradigms*. 2006. [Online]. Available: http://www.amazon.de/Distributed-Systems-Principles-Paradigms-Tanenbaum/dp/B006V36H4S/ref=sr_1_5?ie=UTF8&qid=1352386184&sr=8-5

[42] K. W. Ross, J. F. Kurose. "Computer Networking: A Top-Down Approach", 8th Edition. New York, Addison Wesley, 2021.

[43] TIPHON, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS)," *Etsi Tr 101 329 V2.1.1*, vol. 1, pp. 1–37, 1999, [Online]. Available: https://www.etsi.org/deliver/etsi_tr/101300_101399/101329/02.01.01_60/tr

UNIVERSITAS
GADJAH MADA
Implementasi Analisis Data Honeypot Berbasis YARA dan Large Language Model Untuk Identifikasi Ancaman Siber
Emanuel Dananjaya Kusumadewa Biansa Dua, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

_101329v020101p.pdf

[44] C. Zhang and D. Qi, "How to parallelize Rsync," *J. Phys. Conf. Ser.*, vol. 1684, no. 1, 2020, doi: 10.1088/1742-6596/1684/1/012080.

[45] GeeksForGeeks. "*Rsync Algorithm - System Design*". [Online]. Available: https://www.geeksforgeeks.org/system-design/rsync-algorithm-system-design, Diakses: 21 Mei 2026

[46] GitHub, "Recommended Alert Thresholds — Monitoring Memory Usage," *GitHub Enterprise Server Documentation*, 2023. [Online]. Available: https://docs.github.com/en/enterprise-server@3.0/admin/enterprise-management/recommended-alert-thresholds