Analisis *Insider Threat* pada Sistem Keamanan Rumah Cerdas Menggunakan Malicious Traffic Monitoring

Dedy Hariyadi[1], Cici Finansia[2]
[1] Teknologi Informasi, Universitas Jenderal Acmad Yani Yogyakarta
[2] Teknik Industri, Universitas Jenderal Acmad Yani Yogyakarta
[1]dedy@unjaya.ac.id, [2]cifinansia@gmail.com

ABSTRAK

Ancaman serangan siber semakin banyak dan kompleks, berdasarkan catatan Badan Siber dan Sandi Negara (BSSN) bahwa di Indonesia pada tahun 2022 terdapat anomali trafik atau malicious traffic ratusan juta. Berdasarkan sumber ancaman maka dapat serangan siber dapat dikategorikan serangan siber yang bersumber dari internal (*insider threat*) dan serangan siber yang bersumber dari luar (outsider threat). Saat ini serangan siber tidak hanya dari luar atau outsider karena serangan siber dapat bersumber dari perangkat yang digunakan atau kebiasaan pengguna dalam mengakses internet. Untuk mendeteksi ancaman serangan siber pada ekosistem rumah cerdas menggunakan penelitian ini mengadopsi metode *Network Development Life Cycle* (NDLC). Berdasarkan hasil analisis pada ekosistem rumah memungkinkan diterapkan teknik *port mirroring* pada router. Sehingga pada perancangan mengggunakan Miktorik dan MalTrail sebagai sensor deteksi *malicious traffic* untuk mengetahui aktivitas anomali. Hasil dari penelitian ini menunjukan bahwa ancaman serangan siber yang bersumber dari internal dapat disebabkan dari kebiasaan pengguna dalam mengakses internet. Sedangkan perangkat cerdas yang terpasang dalam penelitian ini tidak ditemukan adanya *malicious traffic* atau aktivitas anomali. Maka penelitian ini masih perlu dilakukan improvisasi menggunakan teknik *network packet capture.*

Kata kunci: *Malicious Traffic*, *Port Mirroring*, Mikrotik, MalTrail, Serangan Siber.

ABSTRACT

The threat of cyber attacks is increasing and complex, based on the records of the Badan Siber dan Sandi Negara (BSSN) that in Indonesia in 2022 there were hundreds of millions of traffic anomalies or malicious traffic. Based on the source of the threat, cyber attacks can be categorized as insider threats and outsider threats. Currently, cyber attacks are not only from outside or outsiders, because cyber attacks can originate from the devices used or user habits in accessing the Internet. To detect the threat of cyber-attacks on the smart home ecosystem, this research adopts the Network Development Life Cycle (NDLC) method. Based on the analysis results in the home ecosystem, it is possible to apply the port mirroring technique on the router. Thus, the design uses Miktorik and MalTrail as malicious traffic detection sensors to find out anomalous activities. The results of this study show that the threat of cyber-attacks from internal sources can be caused by user habits in accessing the Internet. Although the smart devices installed in this study did not detect any malicious traffic or anomalous activity. Therefore, this research still needs to be improvised using network packet capture techniques.

Keywords: *Malicious Traffic, Port Mirroring, Mikrotik, MalTrail, Cyber Attack.*

1. PENDAHULUAN

Serangan siber ditinjau dari sumber serangan dapat dikategorikan menjadi dua, yaitu *outsider threat* dan *insider threat* [1]. Untuk mendeteksi penyerang baik yang berkategori *outsider threat* dan *insider threat* memerlukan sensor sesuai dengan kebutuhan masing-masing. Sensor yang terpasang disesuaikan dengan kategori serangan [2]. Penyerang dalam melakukan serangan dapat memanfaatkan perangkat yang terpasang pada suatu ekosistem, sebagai contoh pada perangkat

Internet of Things (IoT). Oleh sebab itu peneliti dari Universitas Ahmad Dahlan dalam melakukan investigasi *insider threat* menggunakan pendekatan forensik digital. Dalam penelitian tersebut ditemukan bahwa perangkat IoT dapat disisipi *malware*. Artinya *insider threat* dapat melakukan serangan siber dengan menanamkan *malware* pada perangkat IoT [3]. *Malware* yang terpasang pada perangkat IoT dapat melakukan serangan siber berupa *Distributed Denial of Server* (DDoS). Perangkat IoT ini digunakan sebagai Robot atau Bot untuk melakukan serangan siber berupa DDoS. Peneliti dari California State University menyatakan bahwa serangan DDoS yang bersumber dari perangkat IoT terdeteksi menggunakan *Mirai Malware* dengan teknik *DNS Flooding* dan *HTTP Flooding* [4]. Maka untuk mengantisipasi serangan DDoS yang bersumber dari perangkat IoT peneliti dari Punjabi University perlu adanya solusi dalam sistem pertahanan ekosistem IoT [5].

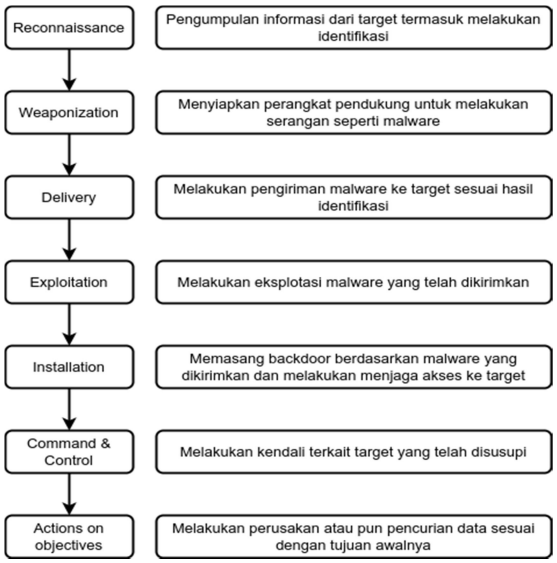
Ekosistem IoT yang terdiri dari sensor nirkabel, perangkat lunak, aktuator, dan perangkat komputer yang terintegrasi dan dioperasikan melalui jaringan internet. Pada ekosistem IoT memungkinkan tanpa campur tangan manusia dan otomatis dalam pengoperasianya. Namun, hal ini berpotensi adanya celah serangan siber yang bersumber dari ekosistem IoT [6]. Peneliti dari University of South Africa mengusulkan perlu adanya sistem pertahanan pada ekosistem IoT yang menggunakan pendekatan Taktik, Teknik, dan Prosedur (TTP) untuk menanggulangi serangan yang bersumber dari *insider threat* [7].

Ancaman yang ditimbulkan oleh *insider threat* pada prinsipnya semakin meningkat tidak terkecuali pada ekosistem IoT. Untuk mencegah serangan oleh *insider threat* perlu adanya solusi untuk meningkatkan sistem pertahanan, seperti *Data Leak Protection* dan *Security Incident Event Management*. Data yang terkumpul pada sistem pertahanan tersebut dilakukan analisis lebih lanjut seperti jumlah data, tipe data, dan karakteristik data untuk mencegah kebocoran data yang disebabkan oleh *insider threat* [8]. Analisis tersebut untuk mengetahui lebih lanjut terkait motivasi dari *insider threat*, yaitu terkait aktivitas yang disengaja oleh pengimplementasi ekosistem IoT atau aktivitas yang disisipi oleh pabrik [9]. Maka penelitian selanjutnya dilakukan evaluasi terkait serangan DDoS yang bersumber dari *insider threat* baik *cryptojacking malware* atau *Mirai Botnet*. Dalam penelitian tersebut menguji beberapa perangkat IoT dalam melakukan serangan DDoS untuk mengetahui karakteristik serangannya [10].

Berdasarkan penelitian sebelumnya serangan tidak hanya dari luar ekosistem rumah cerdas (*outsider*) tetapi juga terjadi dari jaringan internal ekosistem rumah cerdas (*insider*). Namun, pada penelitian sebelumnya tentang keamanan siber pada ekosistem rumah cerdas belum dilakukan penelitian lebih lanjut terkait serangan siber yang bersumber dari jaringan internal. Oleh sebab pada artikel ini diusulkan analisis serangan siber yang bersumber dari jaringan internal menggunakan teknik *Switched Port Analyzer* atau *Port Mirroring* pada eksosistem rumah cerdas.

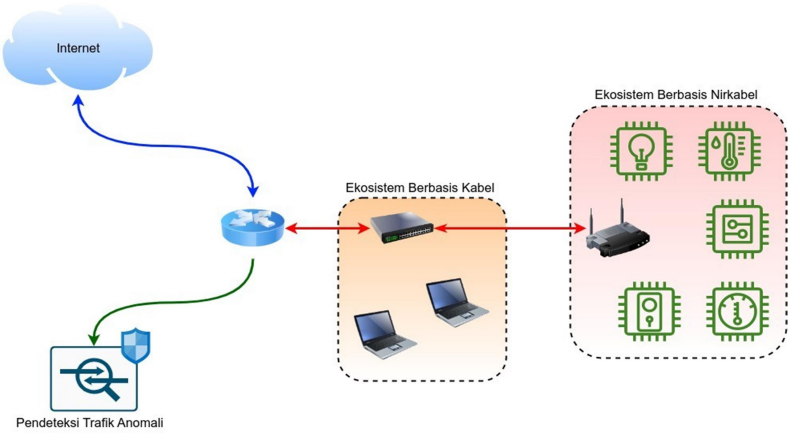
2. METODOLOGI PENELITIAN

Badan Siber dan Sandi Negara (BSSN) pada tahun 2022 mencatat bahwa terdapat trafik anomali pada jaringan internet Indonesia sebanyak 976.426.996. Anomali ini merupakan bentuk serangan siber yang masuk ke Indonesia berdasarkan sensor yang telah terpasang. Dari 976.426.996 serangan siber, serangan terbanyak kategorinya adalah Botnet dengan jumlah serangan sebanyak 254.260.339 [11]. Botnet merupakan aplikasi komputer yang bersifat jahat (*malware*) dengan rancangan untuk berkomunikasi melalui internet dengan aplikasi serupa untuk melakukan serangan siber. Saat ini Botnet dapat dikatakan malware yang paling sering melakukan serangan ke jaringan internet [12]. Menurut Lockheed Martin Corporation, Industri Pertahanan yang berpusat di Amerika Serikat mengusulkan kerangka kerja untuk membatasi ruang gerak penyerang atau *threat actor* dengan memahami 7 tahapan perilakunya yaitu, *reconnaissance, weaponization, delivery, exploitation, installation, command & control*, dan *action on objectives (steal confidential data),* seperti pada Gambar 1 [13]. Dalam usulan Lockheed Martin Corporation upaya membatasi ruang gerak *threat actor* dengan melakukan deteksi yaitu pemasangan sistempendeteksi dari tahapan *weaponization* [14].



Gambar 1. Model Cyber Kill Chain

Penelitian sebelumnya dalam mendeteksi threat actor dengan aktivitas crytopjacking pada suatu sistem dan jaringan komputer menggunakan metode pencatatan malicious traffic menggunakan Maltrail [15]. Sedangkan pada penelitian ini menggunakan metode yang serupa dengan penelitian sebelum, yaitu memanfaatkan pemantauan malicious traffic pada ekosistem rumah cerdas. Metode ini adalah bagian memutus rantai berdasarkan model cyber kill chain. Sehingga objek yang dipantau yaitu perangkat IoT yang terpasang pada ekosistem rumah cerdas dengan berbagai merk dapat dipantau lalu lintas jaringannya. Adapun topologi jaringan yang digunakan dalam penelitian ini seperti pada Gambar 2.



Gambar 2. Topologi Pemantauan *Malicious Traffic*

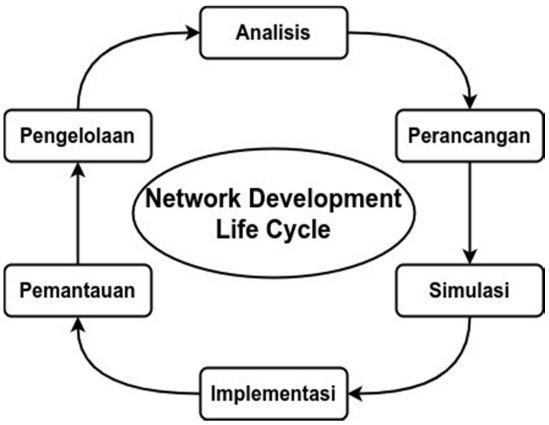
Untuk mendukung penelitian ini maka perangkat pendukung yang diperlukan diantaranya, sensor, router, access point, dan perangkat IoT yang biasa terpasang pada rumah cerdas. Perangkat IoT dipantau selama 24 jam untuk mengetahui potensi *malicious traffic* dari aktivitas perangkat selama terhubung ke jaringan. Tabel 1 merupakan kebeutuhan perangkat pendukung penelitian.

Tabel 1. Kebutuhan Alat dan Fungsi

Perangkat	Fungs
Raspberry Pi 3	Perangkat yang memantau aktivitas jaringan perangkat IoT. Sistem operasi yang terpasang adalah Raspbian dengan perangkat lunak pemantau jaringan, Maltrail.
Komputer/ Laptop	Perangkat untuk mengakses Maltrail pada Raspberry Pi 3 secara *remote*.
Router Wireless RB931-2nD (hAP-Mini)	Perangkat yang mengelola lalu lintas jaringan termasuk melakukan penyalinan lalu lintas ke Raspberry Pi 3.
GL.iNet GL-MT1300	Wireless Access Point yang menghubungkan perangkat IoT.
Bardi Doorlock with Handle (Lite Version)	Gagang pintu untuk keamanan ruangan yang terhubung penggunaannya melalui platform Bardi.
Philips Smart LED A.E27	Lampu cerdas yang terhubung penggunaannya melalui platform Wiz.
Avaro Smart Bulb 12W	Lampu cerdas yang terhubung penggunaannya melalui platform Avaro.
ACOME Smart Bulb AL01 14W	Lampu cerdas yang terhubung penggunaannya melalui platform Avaro.
Lanberg Smart Power Strip SM01-WPS34	Lampu cerdas yang terhubung penggunaannya melalui platform Tuya Smart Life.

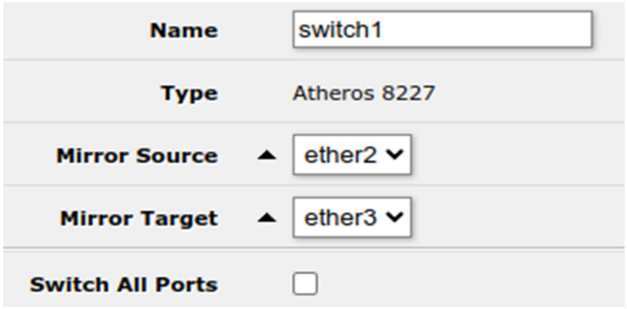
3. HASIL DAN PEMBAHASAN

Network Development Life Cycle (NDLC) adalah metodologi yang digunakan dalam rekayasa dan manajemen jaringan untuk memandu perencanaan, desain, implementasi, dan pemeliharaan sistem komputer dan jaringan yang terstruktur, sistematis, dan efisien. Dasar pemikiran di balik NDLC adalah pemahaman bahwa jaringan adalah sistem kompleks yang memerlukan perencanaan dan pengelolaan yang cermat untuk mencapai fungsionalitas dan kinerja yang optimal. NDLC terdiri dari beberapa fase yang saling berhubungan yang membentuk siklus berkelanjutan, diantaranya analisis, perancangan, simulasi, implementasi, pemantauan, dan pengelolaan, seperti pada Gambar 3 [16].



Gambar 3. ***Network Development Life Cycle***

Berdasarkan analisis, untuk melakukan *malicious traffic monitoring* menggunakan perangkat yang mendukung protokol penyalinan seperti di Cisco menggunakan SPAN (*Switched Protocol Analyzer*) atau Mikrotik menggunakan *Port Mirroring* [17]. Maka pada perancangan penelitian ini menggunakan fitur *Port Mirroring* pada Mikrotik dengan mendefinisikan *port* jaringan internal dan port *malicious traffic monitoring*. Tahapan mensimulasi protokol penyalinan menggunakan Mikrotik, *port* untuk jaringan internal adalah *ether2* dan *port* untuk *malicious traffic monitoring* adalah *ether3*, adapun konfigurasi pada perangkat Mikrotik seperti pada Gambar 4. Selanjutnya lalu lintas yang tersalin dilakukan pemantauan *malicious traffic* menggunakan sensor berbasis *Intrusion Detection System* (IDS), perangkat lunak yang berfungsi sebagai pemantauan lalu lintas yang mendeteksi aktivitas mencurigakan. Pada penelitian ini menggunakan IDS yang bersumber data dari Audit Trail [18].



Gambar 4. Konfigurasi ***Port Mirroring***

Perangkat lunak yang berfungsi sebagai IDS pada penelitian ini adalah MalTrail, yaitu sebuah sistem deteksi lalu lintas berbahaya yang menggunakan daftar hitam yang tersedia secara publik dan serta jejak statis yang dikumpulkan dari berbagai laporan antivirus dan daftar yang dicatat khusus. Daftar hitam ini dapat juga berdasarkan temuan *Threat Hunter* yang dipublikasi melalui *Information Threat Sharing* yang selanjutnya diolah dan dianalisis. Informasi ini mencakup alamat IP, nama domain, dan URL [18], [19]. Pemantuan perangkat IoT seperti pada Tabel 1selama 24 jam nonstop dengan bergantian atau satu per satu. Pemantauan yang dilakukan dengan melakukan beberapa aktivitas seperti mematikan perangkat, menghidupkan perangkat, dan mengubah *mode* dari perangkat pengendali dalam hal ini adalah ponsel cerdas. Kelima perangkat tersebut juga dipantau *malicious traffic* melalui

MalTrail terkait akses ke beberapa *endpoint* dari masing-masing perangkat IoT yang berbasis protokol http, seperti pada Tabel 2.

Tabel 2. *Endpoint* Perangkat IoT

Perangkat	*Endpoint*
Bardi Doorlock with Handle (Lite Version)	- bardismartlife.app.tuya.com - bardismartlife.applink.smart321.com
Philips Smart LED A.E27	- apptoapp.wiz.world - alexa-to-app.dev.wiz.world - alexa-to-app.wiz.world - invite.wiz.world
Avaro Smart Bulb 12W	- comx01.app.tuya.com - comx01.applink.smart321.com
ACOME Smart Bulb AL01 14W	- comx01.app.tuya.com - comx01.applink.smart321.com
Lanberg Smart Power Strip SM01-WPS34	- smartlife.app.tuya.com - smartlife.applink.smart321.com

Lampu pintar Avaro dan ACOME dikendalikan menggunakan aplikasi yang sama, yaitu platform Avaro. Maka kedua lampu tersebut memiliki *endpoint* yang sama comx01.app.tuya.com dan comx01.applink.smart321.com. Namun, pada prinsipnya 4 dari 5 perangkat cerdas berbasiskanteknologi dari Tuya maka *endpoint*-nya menuju ke domain utama Tuya [20]. Berdasarkan Tabel 2 dilakukan pemantauan terhadap ke-5 perangkat cerdas menggunakan MalTrail satu per satu selama 24 jam. Hasil dari pemantauan tidak terdapat aktivitas yang mecurigakan yang bagian dari *malicious traffic*, sebagai contoh Gambar 5 sedangkan Tabel 3 merupakan rangkuman catatan aktivitas pemantauan dari *malicious traffic* yang menunjukan hasil tidak aktivitas mencurigakan pada lalu lintas jaringan ekosistem rumah cerdas.

Gambar 5. *Malcious Traffic* pada MalTrail

Tabel 3. Aktivitas *Malicious Traffic*

Perangkat	IP Address	Aktivitas Anomali
Bardi Doorlock with Handle (Lite Version)	192.168.1.47	0
Philips Smart LED A.E27	192.168.1.42	0
Avaro Smart Bulb 12W	192.168.1.38	0
ACOME Smart Bulb AL01 14W	192.168.1.41	0
Lanberg Smart Power Strip SM01-WPS34	192.168.1.40	0

4. KESIMPULAN

Ancaman serangan siber tidak hanya bersumber dari luar saja, pada penelitian ini menunjukan bahwa ancaman serangan siber juga terjadi di sistem komputer dan jaringan internal. Artinya ancaman serangan siber dapat dikategorikan berdasarkan sumber ancamannya makaterbagi menjadi dua, *insider threat* dan *outsider threat*. Hal ini menunjukan ancaman serangan siber semakin kompleks karena harus melihat dari dua sisi. Sehingga dalam proses mengamankan sistem komputer dan jaringan dari dua sisi, yaitu dari dalam dan luar ekosistem diperlukan sebuah deteksi serangan siber. Adapun bentuk atau upaya serangan dari dalam dapat disebabkan oleh aktivitas pengguna saat melakukan akses internet. Dengan pemasangan sensor lalu lintas jaringan mengunakan MalTrail dapat mengetahui upaya serangan siber dari sisi internal ekosistemrumah cerdas sejak dini.

Namun, pada penelitian ini belum terbukti ancaman serangan siber dari perangkat cerdas atau perangkat IoT. Maka disarankan untuk penelitian selanjutnya perlu dilakukan analisis lebih lanjut menggunaan *network packet capture* atau menggunakan pendekatan forensik jaringan. Walaupun saat ini belum ditemukan potensi ancaman serangan siber tetapi tetap harus mewaspadai berbagai bentuk potensi ancaman serangan siber yang semakin kompleks.

DAFTAR PUSTAKA

[1] X. Jin, C. Katsis, F. Sang, J. Sun, A. Kundu, and R. Kompella, “Edge Security: Challengesand Issues,” 2022, doi: 10.48550/ARXIV.2206.07164.

[2] F. A. Saputra, M. Salman, J. A. N. Hasim, I. U. Nadhori, and K. Ramli, “The Next-Generation NIDS Platform: Cloud-Based Snort NIDS Using Containers and Big Data,” *BigData Cogn. Comput.*, vol. 6, no. 1, p. 19, Feb. 2022, doi: 10.3390/bdcc6010019.

[3] E. Haryanto and I. Riadi, “Forensik Internet Of Things pada Device Level berbasis Embedded System,” *J. Teknol. Inf. Dan Ilmu Komput.*, vol. 6, no. 6, p. 703, Dec. 2019, doi:10.25126/jtiik.2019661828.

[4] T. G. Palla and S. Tayeb, “Intelligent Mirai Malware Detection in IoT Devices,” in *2021 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA: IEEE, May 2021, pp. 0420–0426.doi: 10.1109/AIIoT52608.2021.9454215.

[5] M. Snehi and A. Bhandari, “Apprehending Mirai Botnet Philosophy and Smart LearningModels for IoT-DDoS Detection,” 2021.

[6] S. Madan, S. Sofat, and D. Bansal, “Tools and Techniques for Collection and Analysis ofInternet-of-Things malware: A systematic state-of-art review,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9867–9888, Nov. 2022, doi: 10.1016/j.jksuci.2021.12.016.

[7] S. Chaipa, E. K. Ngassam, and S. Shawren, “Towards a New Taxonomy of Insider Threats,”in *2022 IST-Africa Conference (IST-Africa)*, Ireland: IEEE, May 2022, pp. 1–

10. doi: 10.23919/IST-Africa56635.2022.9845581.

[8] J. Kim and H. Chang, "An Exploratory Study of Security Data Analysis Method for InsiderThreat Prevention," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, Republic of: IEEE, Oct. 2022, pp. 611–613. doi: 10.1109/ICTC55196.2022.9952395.

[9] J. R. Schoenherr, "Insider Threats and Individual Differences: Intention and UnintentionalMotivations," *IEEE Trans. Technol. Soc.*, vol. 3, no. 3, pp. 175–184, Sep. 2022, doi: 10.1109/TTS.2022.3192767.

[10] A. Borys, A. Kamruzzaman, H. N. Thakur, J. C. Brickley, M. L. Ali, and K. Thakur, "An Evaluation of IoT DDoS Cryptojacking Malware and Mirai Botnet," in *2022 IEEE World AIIoT Congress (AIIoT)*, Seattle, WA, USA: IEEE, Jun. 2022, pp. 725–729. doi: 10.1109/AIIoT54504.2022.9817163.

[11] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2022," Badan Siberdan Sandi Negara, 2023.

[12] E. Alomari, S. Manickam, B. B. Gupta, P. Singh, and M. Anbar, "Design, deployment anduse of HTTP-based botnet (HBB) testbed," in *16th International Conference on Advanced Communication Technology*, Pyeongchang, Korea (South): Global IT Research Institute (GIRI), Feb. 2014, pp. 1265–1269. doi: 10.1109/ICACT.2014.6779162.

[13] R. Kumar, S. Singh, and R. Kela, "A Quantitative Security Risk Analysis Framework for Modelling and Analyzing Advanced Persistent Threats," in *Foundations and Practice of Security*, vol. 12637, G. Nicolescu, A. Tria, J. M. Fernandez, J.-Y. Marion, and J. Garcia-Alfaro, Eds., in Lecture Notes in Computer Science, vol. 12637. , Cham: Springer International Publishing, 2021, pp. 29–46. doi: 10.1007/978-3-030-70881-8_3.

[14] Lockheed Martin Corporation, "Seven Ways to Apply the Cyber Kill Chain with a ThreatIntelligence Platform," Lockheed Martin Corporation, 2015.

[15] A. I. Wicaksono, R. Sahtyawan, and D. Hariyadi, "Network Forensic of Cryptocurrency Miners," *Compiler*, vol. 11, no. 2, p. 97, Dec. 2022, doi: 10.28989/compiler.v11i2.1369.

[16] D. Siswanto, G. Priyandoko, N. Tjahjono, R. S. Putri, N. B. Sabela, and M. I. Muzakki, "Development of Information and Communication Technology Infrastructure in School using an Approach of the Network Development Life Cycle Method," *J. Phys. Conf. Ser.*, vol. 1908, no. 1, p. 012026, Jun. 2021, doi: 10.1088/1742-6596/1908/1/012026.

[17] D. Hariyadi, M. A. Nugroho, C. B. Setiwan, and A. I. Wicaksono, "Hybrid Acquisition padaForensik Digital Berbasis ISO/IEC 27037:2012 Menggunakan Port Mirroring dan Single Board Computer," *J. Inf. Syst. Manag. JOISM*, vol. 5, no. 1, 2023.

[18] A. N. Cahyo, R. Hidayat, and D. Adhipta, "Performance Comparison of Intrusion DetectionSystem-based Anomaly Detection using Artificial Neural Network and Support Vector Machine," presented at the Proceedings of The 12th International Conference on Synchrotron Radiation Instrumentation – SRI2015, New York, NY USA, 2016, p. 070011.doi: 10.1063/1.4958506.

[19] M. Sahrom Abu, S. Rahayu Selamat, A. Ariffin, and R. Yusof, "Cyber Threat Intelligence –Issue and Challenges," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 10, no. 1, p. 371, Apr. 2018, doi: 10.11591/ijeecs.v10.i1.pp371-379.

[20] W. Zhang, Y. Zhang, H. Fan, Y. Gao, and W. Dong, "A Low-code Development Framework for Cloud-native Edge Systems," *ACM Trans. Internet Technol.*, vol. 23, no. 1,pp. 1–22, Feb. 2023, doi: 10.1145/3563215.