Machine learning for network defense: automated DDoS detection with telegram notification integration

Agus Tedyyana[1,2], Osman Ghazali[2], Onno W. Purbo[3]
[1]Department of Informatic Engineering, Politeknik Negeri Bengkalis, Bengkalis, Indonesia
[2]School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, Sintok, Malaysia
[3]Department of Informatic, Institute Technology Tangerang Selatan, South Tangerang, Indonesia

Article Info

Article history:

Received Jan 2, 2024
Revised Jan 15, 2024
Accepted Feb 16, 2024

Keywords:

Cybersecurity
DDoS
IDS
Machine learning
Telegram bot

ABSTRACT

As the prevalence and sophistication of distributed denial of service (DDoS) attacks escalate, the imperative for advanced defense mechanisms becomes paramount, especially in rapidly growing digital landscapes like Indonesia. This research presents the development of an innovative intrusion detection system (IDS) that harnesses machine learning (ML) algorithms to automate the detection of DDoS attacks in real time. By monitoring TCP streams, the system utilizes ML-enhanced IDS components to identify malicious traffic patterns indicative of DDoS activities. An automatic alert is dispatched to network administrators via Telegram upon detection, ensuring immediate awareness and facilitating swift countermeasures. Additionally, the system embodies a self-improving architecture by retraining its ML model with newly encountered attack data, thus continuously refining its detection capabilities. The system's efficacy, marked by its adaptive learning and proactive notification system, not only contributes to the fortification of network security but also underscores the potential for ML in cybersecurity within Indonesia’s expanding digital domain. The deployment of this system is anticipated to significantly bolster cybersecurity infrastructure by addressing the urgent need for advanced and responsive defense strategies against the evolving landscape of cyber threats.

Corresponding Author:

Agus Tedyyana
Department of Informatics Engineering, Politeknik Negeri Bengkalis
Bengkalis, Riau, Indonesia
Email: agustedyyana@polbeng.ac.id

1. INTRODUCTION

In the ever-growing digital era, the internet has become a vital component in everyday life and the business world. Connecting billions of people around the world, facilitating communications, business transactions, and access to information. However, deep reliance on digital technologies also carries significant cybersecurity risks, impacting individuals, organizations, and even state stability [1]. The current global landscape shows that cybersecurity threats are becoming increasingly complex and fast-moving. The rise of cloud computing, the internet of things (IoT), and the use of mobile technology have expanded the attack reach for cybercriminals [2]. Ransomware attacks, data breaches, and attacks on critical infrastructure have caused huge financial losses as well as social and political disruption worldwide [3]. Especially in Indonesia, the rapid growth of internet access [3] has placed this country as a major target for cyber attacks. According to data from the National Cyber and Crypto Agency, Indonesia has experienced a significant increase in cyber-attacks, ranging from phishing and malware to DDoS attacks that threaten the government, financial, and business sectors. Handling cyber security in Indonesia still faces various challenges, including a lack of resources and expertise to fight increasingly sophisticated attacks [4].

As Indonesia grapples with these challenges, the need for strong cybersecurity measures becomes increasingly important [5]. The country's journey towards digital resilience is not just about adopting advanced technologies but also about cultivating a culture of cyber awareness and building a strong foundation of skilled professionals dedicated to safeguarding the nation's digital borders. This effort is not only about national security but is an important aspect of ensuring Indonesia's continued growth and prosperity in the digital era.

Distributed denial of service (DDoS) attacks has emerged as one of the most significant threats in the ever-evolving internet era [6]. This is not just an ordinary cybersecurity incident; DDoS attacks have the potential to drastically disrupt business operations and damage a developing digital economy, as experienced by Indonesia. DDoS attacks are now not only more frequent but also larger and more complex. Cybercriminals use botnets consisting of thousands, even millions, of infected devices to send overwhelming and unauthorized traffic to targets, resulting in overloads and ultimately making services unavailable to legitimate users. The impact of a DDoS attack on a business can be severe [7]. This includes service disruptions, lost revenue, and reputational damage [8]. For companies that depend on an online presence, such as e-commerce, online banking services, and digital service providers, the effects can be devastating. Furthermore, attacks on critical infrastructure, such as financial, health, or utility systems, can have much broader consequences, affecting the economy and social stability as a whole. Given the risks associated with DDoS attacks, organizations and governments in Indonesia need to develop strong defense strategies. This includes implementing security solutions capable of proactively detecting and countering attacks, as well as effective incident response plans to minimize damage when an attack occurs.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks [9]. In an era where almost all aspects of life depend on digital technology, cyber security has become a crucial component for protecting personal data, business information, and critical infrastructure from cyber threats. Cybersecurity is not only about protecting information from unauthorized access but also about ensuring the integrity and availability of that information. In today's digital context, where the volume and sophistication of cyber-attacks continue to increase, the importance of cyber security cannot be underestimated [10]. With the development of technologies such as cloud computing, the IoT, and artificial intelligence (AI), the cyber environment is becoming increasingly complex and vulnerable to attacks [11]. Data protection is a top priority for individuals, organizations, and governments, as cyberattacks can not only cause financial loss but can also damage reputation and public trust [12].

Web servers, as an integral part of the internet infrastructure [13], are often the main targets of cyber-attacks. Web servers store critical data and serve as a gateway between users and organizations, making them valuable targets for threat actors. Attacks on web servers can take the form of DDoS [14], SQL injection [15], cross-site scripting attacks [16], and various other forms, that aim to steal data, disrupt services, or spread malware. This increase in attacks has serious implications. First, there is a direct impact on the security of users' personal information and data. Second, such attacks can hinder business operations, causing significant financial losses and service disruptions. Third, cyberattacks against web servers can damage an organization's trust and reputation, which may have long-term consequences. Finally, these attacks also pose legal and compliance challenges, especially in the context of regulations such as general data protection regulation (GDPR) in Europe, which require the protection of personal data [17].

Facing the scale and complexity of networks in Indonesia [18], the need for automated and efficient network security solutions becomes very important. In an increasingly connected world, where cyberattacks can occur at any time and from anywhere, manual responses are no longer sufficient. This is a realm where ML plays a crucial role, especially in the context of DDoS attack detection. The use of ML algorithms in cybersecurity systems enables automatic and intelligent detection of suspicious patterns in network traffic. These algorithms, which continually learn and adapt based on data, can identify unusual behavior that may signal an attempted DDoS attack. This ability to learn from historical and current data makes attack detection more precise and responsive, significantly improving an organization's ability to identify attacks before they cause damage. By implementing machine learning (ML) technology, organizations in Indonesia can take proactive steps in their network security. It's not just about warding off attacks when they occur, but also about anticipating and preventing attacks before they get too far. ML helps in building systems that are not only responsive but also predictive, providing a more dynamic, multi-layered defense against DDoS attacks [19]. Additionally, the integration of ML in DDoS detection enables continuous adaptation to new tactics used by cybercriminals. As cyber threats evolve, ML algorithms also evolve, learning from the latest attacks and adapting to increase their effectiveness.

The integration of real-time notifications [20] through applications such as Telegram is a key component in increasing the responsiveness and effectiveness of cyber security systems, especially in dealing with DDoS attacks. In the context of network security in Indonesia, where cyberattacks are becoming more frequent and sophisticated, the ability to respond quickly is important. The advantage of using telegram [21], or a similar platform in this context is its ability to provide instant notifications and be accessible across multiple devices. Network administrators, who may not always be in front of their computer screens, can receive these alerts on their smartphones, enabling quick responses even when they are on the move. This fast response is crucial because in the world of cybersecurity, every second counts. By knowing about an attack as soon as possible, security teams can immediately activate mitigation protocols to minimize the impact. This could mean redirecting traffic, applying filters, or taking other pre-planned actions. Apart from speed, this real-time notification integration also helps in team coordination. When an attack occurs, effective communication between team members is key. Telegram can be used not only for initial notification but also for follow-up communication during mitigation efforts, ensuring all team members are up-to-date with the current situation [22].

2. METHOD

A DDoS attack is not merely a disruption, it's a weapon. The objective of such a cyber attack is singular and destructive, to bring a targeted server to its knees, rendering it inaccessible to legitimate users who depend on its services. As the server buckles under the strain, services stutter and stall. Websites become unreachable, transactions fail mid-process, and communication breaks down. The ripple effect can be catastrophic, not just for the entity that owns the server, but for users, customers, and sometimes entire segments of the internet. The purpose of a DDoS attack can vary. It may be to damage a competitor, to make a political statement, to extort, or simply to sow chaos [23]. Regardless of the motive, the endgame is the same: to disrupt, to deny service, to force a digital blackout.

Figure 1 DDoS attack illustration, in the digital world, there exists a duality of flows: one originating from real users seeking information, services, and connections, and another, dark and ominous, orchestrated by compromised attacker computers. On one side, we have the attacker computers, now usurped and commandeered by malicious actors, turned into pawns in a sinister game of cyber warfare. They unleash a deluge of malicious traffic, a digital tempest with a singular aim: to cripple the stability and availability of the targeted server. The server in the crosshairs of this assault is the lifeblood of online services, perhaps an e-commerce website, a news portal, or even critical infrastructure underpinning a city or a nation. The DDoS attack depicted in the illustration floods the server with so many fraudulent requests that it can no longer discern friend from foe, legitimate traffic from the onslaught. On the other side, the real users, oblivious to the maelstrom, continue their attempts to connect. They send forth their requests, hoping to access services they rely on, but their clean and legitimate traffic is lost in the chaos of the attack. Ultimately, they are met with a digital void: a notice that the service they sought to reach is now offline. The server, once powerful and unassailable, is now exhausted and overwhelmed, compelled to declare itself "out of resources" and "SERVICE OFFLINE". This is not merely a technical failure; it is a defeat in the battle of cybersecurity, a reminder that in this digital era, unseen forces can impact real life in very tangible and destructive ways.

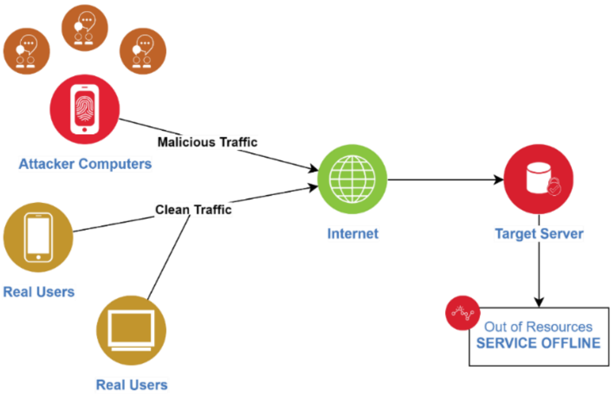


Figure 1. DDoS attack illustration

In the face of increasingly sophisticated cyber threats, conventional approaches to intrusion detection are starting to show their limits [24]. They are hampered by large data volumes and the complexity of new attacks. This is where ML with its ability to process and analyze big data, promises to shift the paradigm. Feature selection becomes very important in this context, by identifying and selecting the most significant features from the data, ML can reduce noise and increase the speed and accuracy of detection [25]. This method is similar to selecting the most useful senses when we are trying to understand a complex environment. Algorithms such as pigeon-inspired optimization (PIO) can optimize this feature selection process by 'teaching' the ML model to recognize the most informative features and ignore others, thereby improving intrusion detection performance [26].

The integration of ML into IDS is a significant step forward in strengthening networks. This integration process involves several steps: data collection, network traffic data is collected, including legitimate packets and potentially malicious network activity. This involves creating a comprehensive database for model training and testing. Data processing and preparation, the collected data must be processed and prepared, which includes normalization, noise removal, and feature selection. Feature selection, as discussed, is an important process for improving the efficiency and effectiveness of ML models. Model training, ML models are created and trained using prepared data. Learning methods such as supervised, unsupervised, or reinforcement learning can be applied depending on the type of data and specific goals of the IDS. Model integration, after training, the model must be integrated into the existing IDS infrastructure. This may involve adapting the system to support decision-making processes driven by ML models.

While battling increasingly complex cyber threats, cybersecurity experts are looking toward the technological horizon with the single goal of creating smarter and more robust intrusion detection systems. An initial step in achieving this goal was the use of the CICIDS 2018 dataset, a broad and detailed data collection that depicts network traffic during simulated cyberattacks. starting from the CICIDS 2018 dataset as information-rich raw material [27]. This process begins with data pre-processing, a critical step in which the data is cleaned of anomalies such as null or infinite values and conversion labels into a numeric format that ML algorithms can understand. This step ensures that the data we have is free from distortion and ready for further analysis.

Figure 2 data preprocessing, explains the feature selection process, where analytical expertise is applied to sort out the most relevant and significant features of a strategic decision that can determine the success or failure of future models. With the right features, our model has a better chance of capturing the essence of complex intrusion patterns. Then, our ML models are rigorously drilled, and fed data that has been carefully selected and processed. This is the phase where the model starts to 'learn' from the data, identifying attack patterns and differentiating them from normal traffic. This careful training is key to developing systems that can be trusted to detect threats. After the training was completed, we were not immediately satisfied. The model must undergo a testing evaluation to ensure that it is truly capable of meeting real-world demands. Using rigorous metrics, we assess model performance, looking for evidence of intelligence and accuracy that will determine its success in the field. Finally, when the model has been proven and tested, we 'export' or export the model, carefully packaging it for deployment in a real environment where it will stand as a first line of defense against intrusion attacks.

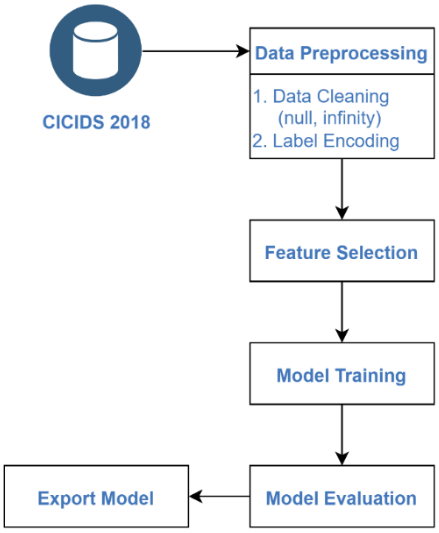


Figure 2. Data preprocessing

3. RESULTS AND DISCUSSION

The model was trained using the preprocessed CICIDS 2018 dataset, and the feature selection process identified a set of predictors that were highly indicative of intrusive activities. Various ML algorithms were employed, including decision trees, support vector machines, and neural networks, each evaluated using a set of performance metrics such as accuracy, precision, recall, and F1-score. The model's overall accuracy is very high at 99.77%, and it achieves an excellent F1-score of 98.70%, suggesting a very effective balance between precision and recall, which is desirable in many applications, especially in fields like cybersecurity where both catching as many real threats as possible (high true positive rate (TPR)) and minimizing disruption from false alarms (low false positive rate (FPR)) are crucial.

This model is the core of an intrusion detection system equipped with ML, as seen from the process of analyzing transmission control protocol (TCP) flows entering the server. Once a DDoS attack is identified by the model, the system automatically sends a notification via Telegram, allowing immediate action to address the potential threat. This process illustrates the practical application of ML models that have high precision and recall in DDoS detection, ensuring better network security by reducing the number of false alarms that can disrupt network operations. The success of the model in detecting attacks accurately and efficiently shows the great potential of applying ML technology in cyber defense.

Figure 3 implementation of the ML model to IDS explains how to implement the ML model to IDS. The process starts with the attackers trying to attack the server. The server, which serves as the core of the protected infrastructure, analyzes TCP flows to identify suspicious traffic [28]. An ML-enhanced IDS continuously monitors this data flow, looking for patterns that correspond to known attacks or abnormal behavior. Once an incident is detected, the IDS system stores the results in a database. This stored information is not only important for security audits and investigations but also for enriching datasets used for retraining ML models. Furthermore, the system periodically re-trains the ML model with new datasets obtained from recent incidents to increase the accuracy of cyber attack detection. The updated model is then uploaded back to the IDS to improve the effectiveness of intrusion detection. If the IDS system detects an intrusion, it will send an alert via telegram, which is an instant messaging platform used to notify security teams in real time. This allows them to immediately take necessary actions to respond to the threat.

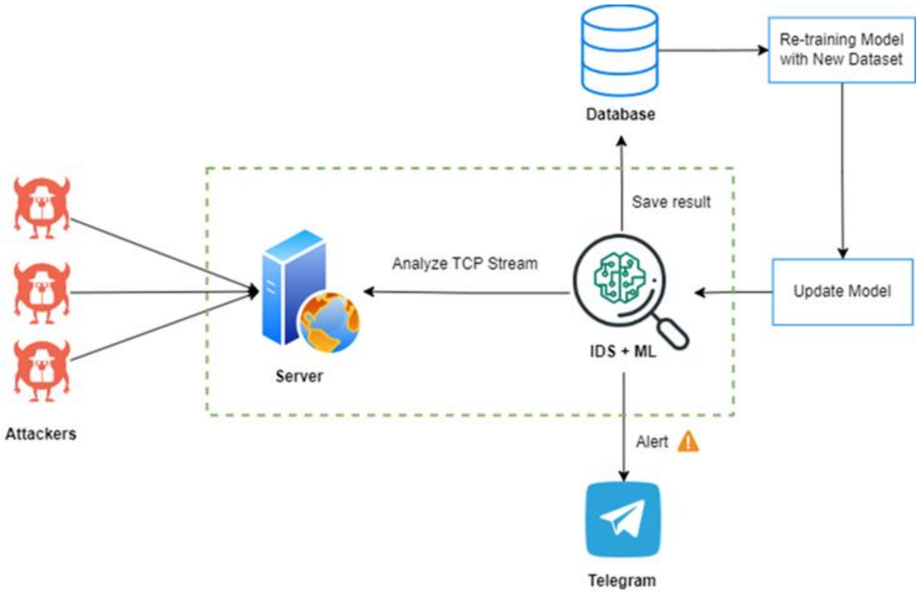


Figure 3. Implementation of ML model to IDS

Figure 4 process flow diagram for a DDoS detection system, we have developed and evaluated a system that uses ML to automatically identify DDoS attacks. The workflow illustrated in the provided diagram shows the methodology we implemented to achieve this goal. From Figure 4 process flow diagram for a DDoS detection system, it can be explained that the process begins with creating a TCP listener, which functions as a supervisor that observes network traffic. This allows the system to capture and compute TCP streams, parsing incoming data to extract relevant information. This data is very important because it is the foundation used by ML models to make predictions about traffic. Once the relevant data is extracted, the next step is to utilize it as input for our ML model. This trained model is then tasked with analyzing the data and producing predictions, which serve as results that determine whether the observed traffic is a DDoS attack or not. When the model predicts a DDoS attack, the system automatically sends a notification via Telegram, which provides real-time information to network managers or security teams. This allows them to act quickly in response to potential threats. On the other hand, if the model predicts that the traffic is safe, no notification is sent, which reduces the potential for disruption from false alarms. In addition, all events and results from our detection system, whether positive or negative, are recorded in a new database. This database is an important resource for tracking and analyzing attacks, as well as for improving ML models for the future. The results we discuss show that our system can accurately detect DDoS attacks and send timely notifications. This has significant implications for improving network security in Indonesia, given the rapid growth in internet use and the increase in cyber attacks. The system promises to be a step forward in network defense technology, integrating artificial intelligence with existing communications tools to respond effectively to cybersecurity threats.

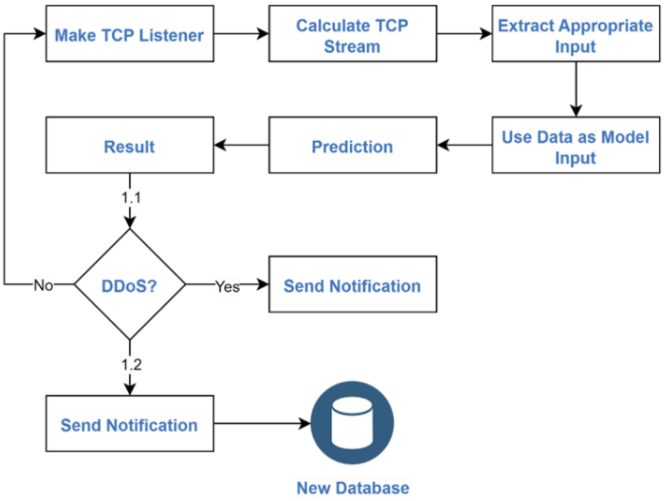
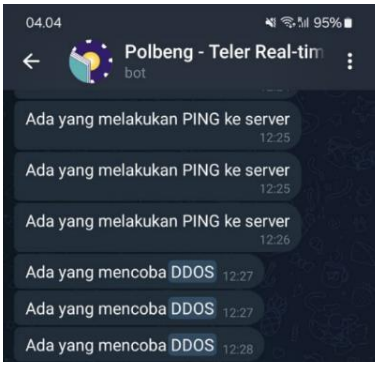


Figure 4. Process flow diagram for a DDoS detection system

Figure 5 telegram bot notification explains telegram bot have been configured to provide real-time notifications regarding network activity, especially those related to potential DDoS attacks. This ties in closely with the previous narrative explaining how an intrusion detection system enhanced with ML can provide notifications when it detects a DDoS attack. The use of telegram bots in this system shows how integration between cybersecurity technology and communication platforms can increase responsiveness in dealing with cyber threats. This underscores the importance of having systems that are not only sophisticated in attack detection but also rapid in providing alerts, allowing for a rapid and coordinated response, which is a critical aspect of maintaining network integrity and security.


04.04 95%
Polbeng - Teler Real-tim
bot

Ada yang melakukan PING ke server 12:25

Ada yang melakukan PING ke server 12:25

Ada yang melakukan PING ke server 12:26

Ada yang mencoba DDOS 12:27

Ada yang mencoba DDOS 12:27

Ada yang mencoba DDOS 12:28

Figure 5. Telegram bot notification

4. CONCLUSION

This research has successfully developed an intrusion detection system that integrates ML to automate the detection of DDoS attacks. From the illustration provided, we can conclude that the system operates by monitoring the TCP stream incoming to the server. This data stream is analyzed by an IDS component enhanced with ML algorithms to identify attack patterns. Once an attack is detected, the system automatically saves the results to a database and sends an alert through Telegram, providing a rapid and effective response that enables network administrators to take necessary actions. Furthermore, the system is designed to learn from new attacks by re-training the model with updated datasets, ensuring that the detection mechanism adapts to the latest threats and becomes more accurate over time. Thus, the proposed system offers a sustainable and dynamic cybersecurity solution that not only enhances real-time attack detection but also strengthens network defense through continuous learning and adaptation to ever-evolving cyber threats. The implementation of this system is expected to be significant in fortifying cybersecurity infrastructure, especially in the face of DDoS attacks in Indonesia, leveraging the growth of internet technology and the need for more sophisticated cybersecurity measures.

REFERENCES

[1] A. Candra, S. Suhardi, and P. D. Persadha, “Indonesia facing the threat of cyber warfare: a strategy analysis,” *Jurnal Pertahanan: Media Informasi ttg Kajian & Strategi Pertahanan yang Mengedepankan Identity, Nasionalism & Integrity*, vol. 7, no. 3, p. 441, Dec. 2021, doi: 10.33172/jp.v7i3.1424.

[2] M. Watney, “Cybersecurity threats to and cyberattacks on critical infrastructure: a legal perspective,” *European Conference on Information Warfare and Security, ECCWS*, vol. 2022-June, no. 1, pp. 319–327, Jun. 2022, doi: 10.34190/eccws.21.1.196.

[3] M. Sarnovsky and J. Paralic, “Hierarchical intrusion detection using machine learning and knowledge model,” *Symmetry*, vol. 12, no. 2, p. 203, Feb. 2020, doi: 10.3390/sym12020203.

[4] D. Rusminingsih and S. Viphindrartin, “Internet user and income consumption in an effort to empower MSMEs in Indonesia,” *SPLASH Magz*, vol. 1, no. 2, pp. 74–79, Apr. 2021, doi: 10.54204/splashmagzvol1no1pp74to79.

[5] H. Wijayanto and I. A. Prabowo, “Cybersecurity vulnerability behavior scale in college during the COVID-19 pandemic,” *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 9, no. 3, pp. 395–399, Nov. 2020, doi: 10.32736/sisfokom.v9i3.1021.

[6] A. Azhari, A. W. Muhammad, and C. F. M. Foozy, “Machine learning-based distributed denial of service attack detection on intrusion detection system regarding to feature selection,” *International Journal of Artificial Intelligence Research*, vol. 4, no. 1, Feb. 2020, doi: 10.29099/ijair.v4i1.156.

[7] A. Cheema, M. Tariq, A. Hafiz, M. M. Khan, F. Ahmad, and M. Anwar, “Prevention techniques against distributed denial of service attacks in heterogeneous networks: a systematic review,” *Security and Communication Networks*, vol. 2022, pp. 1–15, May 2022, doi: 10.1155/2022/8379532.

[8] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, “DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison,” *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.

[9] V. G. V and A. K. Ghosh, “Enhancing cyber security measures for online learning platforms,” *International Journal of Computer Science and Engineering*, vol. 8, no. 11, pp. 1–5, Nov. 2021, doi: 10.14445/23488387/ijcse-v8i11p101.

[10] A. Mukhopadhyay, S. Chatterjee, K. K. Bagchi, P. J. Kirs, and G. K. Shukla, “Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance,” *Information Systems Frontiers*, vol. 21, no. 5, pp. 997–1018, Oct. 2019, doi: 10.1007/s10796-017-9808-5.

[11] D. S. Gupta, S. H. Islam, M. S. Obaidat, P. Vijayakumar, N. Kumar, and Y. Park, “A provably secure and lightweight identity-based two-party authenticated key agreement protocol for IIoT environments,” *IEEE Systems Journal*, vol. 15, no. 2, pp. 1732–1741, Jun. 2021, doi: 10.1109/JSYST.2020.3004551.

[12] Y. Rupa, “Privacy of data against the challenges of information technology from the perspective of the normative regulation of GDPAR; aspects of security during the processing of personal data,” in *ICSIT 2022 - 13th International Conference on Society and Information Technologies, Proceedings*, Mar. 2022, pp. 74–78, doi: 10.54808/ICSIT2022.01.74.

[13] A. Solanki, A. Parekh, G. Chawda, and M. G. S., “Lightron : a GUI integrated, rust based web server,” *International Journal of Scientific Research in Science and Technology*, pp. 554–560, Aug. 2021, doi: 10.32628/cseit2174127.

[14] P. P. do Nascimento, P. Pereira, J. M. Mialaret, I. Ferreira, and P. Maciel, “A methodology for selecting hardware performance counters for supporting non-intrusive diagnostic of flood DDoS attacks on web servers,” *Computers and Security*, vol. 110, p. 102434, Nov. 2021, doi: 10.1016/j.cose.2021.102434.

[15] G. S. Oreku, “A study of online database servers: the case of SQL - injection, how evil that could be?,” *Asian Journal of Research in Computer Science*, pp. 198–211, Dec. 2022, doi: 10.9734/ajrcos/2022/v14i4304.

[16] R. W. Kadhim and M. T. Gaata, “A hybrid of CNN and LSTM methods for securing web application against cross-site scripting attack,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 2, pp. 1022–1029, Feb. 2020, doi: 10.11591/ijeecs.v21.i2.pp1022-1029.

[17] W. Presthus and H. Sørum, “Consumer perspectives on information privacy following the implementation of the GDPR,” *International Journal of Information Systems and Project Management*, vol. 7, no. 3, pp. 19–34, Oct. 2019, doi: 10.12821/ijispm070302.

[18] A. Yudiastuti, F. D. Murwani, Sudarmiatin, and A. Hermawan, “Network perspective in the internationalization of Indonesian SMEs in the era of indutrial revolution 4.0,” *International Journal of Science, Technology & Management*, vol. 2, no. 4, pp. 1073–1081, Jul. 2021, doi: 10.46729/ijstm.v2i4.242.

[19] A. Agrawal, R. Singh, M. Khari, S. Vimal, and S. Lim, “Autoencoder for design of mitigation model for DDOS attacks via M-DBNN,” *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–14, Apr. 2022, doi: 10.1155/2022/9855022.

[20] H. Te Wu, “Establish a digital real-time learning system with push notifications,” *Frontiers in Psychology*, vol. 13, Feb. 2022, doi: 10.3389/fpsyg.2022.767389.

[21] R. Parlika and A. Pratama, “The online test application uses telegram bots version 1.0,” *Journal of Physics: Conference Series*, vol. 1569, no. 2, p. 022042, Jul. 2020, doi: 10.1088/1742-6596/1569/2/022042.

[22] A. Urman, J. C. T. Ho, and S. Katz, “Analyzing protest mobilization on telegram: the case of 2019 anti-extradition bill movement in Hong Kong,” *PLoS ONE*, vol. 16, no. 10 October, p. e0256675, Oct. 2021, doi: 10.1371/journal.pone.0256675.

[23] W. Zhao, H. Sun, and D. Zhang, “Research on DDoS attack detection method based on deep neural network model in SDN,” in *Proceedings - 2022 International Conference on Networking and Network Applications, NaNA 2022*, Dec. 2022, pp. 184–188, doi: 10.1109/NaNA56854.2022.00038.

[24] R. Lalduhsaka, N. Bora, and A. K. Khan, “Anomaly-based intrusion detection using machine learning: an ensemble approach,” *International Journal of Information Security and Privacy*, vol. 16, no. 1, pp. 1–15, Oct. 2022, doi: 10.4018/IJISP.311466.

[25] M. A. H. Azmi, C. F. M. Foozy, K. A. M. Sukri, N. A. Abdullah, I. R. A. Hamid, and H. Amnur, “Feature selection approach to detect DDoS attack using machine learning algorithms,” *International Journal on Informatics Visualization*, vol. 5, no. 4, pp. 395–401, Dec. 2021, doi: 10.30630/JOIV.5.4.734.

[26] J. S. Pan, A. Q. Tian, S. C. Chu, and J. B. Li, “Improved binary pigeon-inspired optimization and its application for feature selection,” *Applied Intelligence*, vol. 51, no. 12, pp. 8661–8679, Dec. 2021, doi: 10.1007/s10489-021-02302-9.

[27] M. P. Bharati and S. Tamane, “NIDS-network intrusion detection system based on deep and machine learning frameworks with CICIDS2018 using cloud computing,” in *Proceedings of the 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing, ICSIDEMPC 2020*, Oct. 2020, pp. 27–30, doi: 10.1109/ICSIDEMPC49020.2020.9299584.

[28] G. Vardoyan, C. V. Hollot, and D. Towsley, “Towards stability analysis of data transport mechanisms: a fluid model and its applications,” *IEEE/ACM Transactions on Networking*, vol. 29, no. 4, pp. 1730–1744, Aug. 2021, doi: 10.1109/TNET.2021.3075837.

BIOGRAPHIES OF AUTHORS

Agus Tedyyana is a senior lecturer at the Politeknik Negeri Bengkalis, Bengkalis, Riau, Indonesia. He has an educational background in computer science. He has worked in education as a lecturer since 2014. He has been continuing his Doctoral (Ph.D.) studies at the Universiti Utara Malaysia (UUM) Campus in Kedah Darul Aman, Malaysia, since early 2020. His research interests are in computer security. He can be contacted at email: agustedyyana@polbeng.ac.id.

Prof. Osman Ghazali is a Professor and the Dean of the School of Computing, Universiti Utara Malaysia. He holds a Ph.D. in Information Technology (Networking) from Awang Had Salleh Graduate School, Universiti Utara Malaysia (AHSGS). His research interests are internetworking, cloud computing, and information security. He has more than 100 publications as refereed book chapters and refereed technical papers in journals and conferences. He is a senior member of the inter Networks Research Laboratory (IRL). He is also a member of the IEEE and the ACM. He can be contacted at email: osman@uum.edu.my.

Prof. Onno W. Purbo graduated from the Department of Electrical Engineering, Bandung Institute of Technology, in 1987. In 1989, he completed his postgraduate education at McMaster University, Canada, in the field of semiconductor laser. Five years later, he received his Ph.D. from the University of Waterloo. Canada, in the field of Integrated Circuit Technology for satellites, In November 2020, he received the Postel Service Award from the Internet Society. Postel Service Award was given to Onno for his outstanding contribution to the development of internet technology in Indonesia. He can be contacted at email: onno@indo.net.id.