TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 23, No. 1, February 2025, pp. 81~89
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v23i1.25857

Swarm intelligence for intrusion detection systems in internet of things environments

Apri Siswanto[1], Akmar Efendi[1], Jaroji[2], Fajar Ratnawati[2]
[1]Department of Informatics Engineering, Faculty of Engineering, Universitas Islam Riau, Pekanbaru, Indonesia
[2]Department of Informatic Engineering, Politeknik Negeri Bengkalis, Bengkalis, Indonesia

Article Info

Article history:

Received Nov 13, 2023
Revised Oct 29, 2024
Accepted Nov 6, 2024

Keywords:

Internet of things
Intrusion detection systems
Network security
Pigeon inspired optimization
Swarm intelligence

ABSTRACT

The rise of the internet of things (IoT) technology has brought new security challenges, necessitating robust intrusion detection systems (IDS). This research applies swarm intelligence (SI) principles, specifically the pigeon inspired optimization (PIO) algorithm, to enhance IDS effectiveness in IoT environments. Drawing on the behavior of social species, SI fosters decentralized control and emergent behavior from simple rules. These principles guide the PIO algorithm, making it apt for optimizing IDS. We utilize two comprehensive IoT datasets – the Canadian Institute for Cybersecurity (CIC) IoT dataset 2023 and the IoT dataset for IDS, aiming to boost the IDS's capability to detect illicit attacks. By adapting the PIO algorithm, our IDS learns from the environment, adapts to evolving threats, and mitigates false-positive rates. Preliminary tests show that our SI-based IDS outperforms traditional systems' accuracy, speed, and adaptability. This research advances SI applications in IoT security, contributing to developing more resilient IDS and ultimately enhancing IoT network security against a range of cyber threats.

Corresponding Author:

Apri Siswanto
Department of Informatics Engineering, Faculty of Engineering, Universitas Islam Riau
Pekanbaru, Indonesia
Email: aprisiswanto@eng.uir.ac.id

1. INTRODUCTION

The internet of things (IoT) technology has rapidly expanded, becoming a core component in various sectors such as home automation, healthcare, transportation, and more. This expansive network of connected devices provides vast opportunities for efficiency, automation, and new applications. However, the accelerated growth and adoption of IoT technology have given rise to numerous security threats, making IoT networks a lucrative target for cyber-attacks [1], [2]. In the rapidly evolving IoT landscape, securing networks and devices from malicious intrusions is paramount [3]-[5]. While effective to an extent, traditional methods often need to improve in addressing the dynamic and decentralized nature of IoT environments. With this challenge in mind, the researchers turned to the principles of swarm intelligence (SI), a paradigm inspired by the behaviour of social species [6], [7].

SI mimics the behaviour of social species like birds and ants, where complex group behaviours emerge from simple local interactions among individuals [8]. It offers an inherently adaptive and distributed approach to problem-solving, highly suited to the dynamic world of IoT. One of the cornerstones of SI is decentralized control. Since IoT involves many devices interacting within a network, a decentralized approach brings several benefits to the table. It heightens resilience against attacks and circumvents single points of failure [9]. Inspiration from nature, the pigeon inspired optimization (PIO) algorithm was chosen. Pigeons exhibit extraordinary navigation skills in the natural world, capable of finding their way home across vast distances with remarkable accuracy [10]. The PIO algorithm emulates these natural orientation and navigation mechanisms to find optimal solutions in a problem space [11].

A prime concern in intrusion detection systems (IDS) is the constant evolution of security threats in the IoT environment [12]. Algorithms need to be adaptive. The PIO, with its roots in the adaptability of pigeons, can learn and adjust to new threats more efficiently than many traditional algorithms [13]. Furthermore, any IDS's objective is to minimize false positives [14]. Algorithms like PIO, which can be optimized with training data, might deliver superior results in distinguishing between legitimate and suspicious network traffic. For that matter, efficiency and speed are of the essence. While SI might sound complex on paper, algorithms like PIO are often crafted with an eye on efficiency and swiftness—both crucial for real-time intrusion detection [15]. By weaving together these advantages, the PIO algorithm based on SI emerges as a reasonable choice for bolstering the efficacy of IDS in IoT environments.

IDS have become indispensable tools for safeguarding IoT environments [16], [17]. These systems detect illicit activities within a network, such as attempts to compromise system integrity, confidentiality, or availability. However, the dynamic and complex nature of IoT networks and the unique characteristics of IoT devices present considerable challenges for traditional IDS. Consequently, there is a pressing need to develop advanced IDS capable of effectively identifying and mitigating illegitimate attacks in IoT environments. In addressing this need, the principles of SI provide a promising approach. SI, a branch of artificial intelligence, is inspired by the social behaviors of certain species and their ability to solve complex problems collectively [18]. This research focuses on the application of the PIO algorithm, a specific manifestation of SI, to enhance the effectiveness of IDS in IoT environments.

The PIO algorithm simulates the homing behavior and navigational skills of pigeons. This makes it particularly well-suited for optimizing the feature selection process in IDS, leading to improved classification of network traffic and heightened detection of illegitimate activities [19]. In this study, we harness two comprehensive IoT datasets - the Canadian Institute for Cybersecurity (CIC) IoT Dataset 2023 and the IoT Dataset for IDS to develop and validate our SI-based IDS. By examining a wide array of network traffic scenarios and attack types, these datasets enable us to assess the system's effectiveness in a realistic context.

Although IDS SI shows better accuracy than traditional systems, can help reduce false positives and is suitable for the evolving IoT threat landscape, the current SI are still drawbacks. For example, implementing SI, especially for those unfamiliar with it, can introduce additional layers of complexity to the IDS. Then, running algorithms based on SI may require more computational resources. While promising, SI in IoT security is still in its nascent stages compared to traditional methods. Real-world implementations and tests are required to fully validate its effectiveness. As with any machine learning or optimization algorithm, there's a risk of overfitting to a specific dataset, making it less effective against unseen threats. Continuous learning and adaptation means the system needs to be constantly monitored and updated to ensure it's learning correctly.

Our goal is to significantly enhance the ability of IDS to detect illegitimate attacks in IoT environments by leveraging the power of the PIO algorithm and the principles of SI. Preliminary tests suggest promising results, as our SI-based IDS outperforms traditional systems in accuracy, speed, and adaptability. This research also contributes to the understanding and application of SI in IoT security, providing a robust solution for enhancing the detection capabilities of IDS in IoT environments. The findings from this study hold substantial potential for ensuring safer, more secure IoT networks capable of mitigating a broad range of cyber threats.

2. METHOD

The research method utilizes the PIO algorithm. This section describes the application of PIO in our research, particularly regarding feature selection for our machine learning model, with an adjustment in the activation function used. The first step involves defining the optimization problem, which, in this context, is identifying the most informative features from the dataset that can enhance the effectiveness of our IDS for IoT environments. The PIO algorithm, taking inspiration from the navigational prowess of pigeons, serves as our main tool for feature selection. PIO optimizes the model's performance function with the chosen features. Each feature is represented as a dove in this algorithm. As the PIO algorithm iterates, every dove modifies its position and speed following certain rules, optimizing the selected features. In each iteration of the PIO algorithm, the pigeons update their position and speed according to pre-defined rules [19]. The performance of each pigeon is assessed based on the chosen features, intending to optimize the model's performance function with these selected features. In some cases, the selected features may still include negative values, which are undesirable. To tackle this issue, we introduce the Sigmoid activation function into the PIO algorithm [20]. The Sigmoid activation function maps any input value into the range between 0 and 1, effectively ensuring that all output values from the model fall within this range.

We enhance the feature selection process's effectiveness by incorporating the Sigmoid activation into the PIO algorithm. As the Sigmoid function ensures that all output values fall within the range 0-1, all selected features will be within this range and hence, will be more meaningful for the model's performance. This methodology, which applies the PIO algorithm for feature selection and integrates the Sigmoid activation function, assures the efficiency and accuracy of our IDS in identifying intrusions in IoT environments. It enables our model to learn effectively from the environment and adapt to evolving security threats, contributing to the safety of IoT networks.

2.1. Related works

The importance of feature selection in machine learning and predictive modeling has been widely discussed in the literature [21], [22]. Feature selection, which refers to selecting a subset of relevant features for model construction, is crucial in optimizing a machine learning model's performance [23]. Much research has also been devoted to applying feature selection in IDS for IoT environments. Researchers have proposed various methodologies to enhance the performance of IDS systems by improving feature selection processes, including PIO [14]. A research paper on "An improved PIO feature selection algorithm for IoT network intrusion" introduced an enhanced version of PIO, LS-PIO, which uses a local search algorithm to optimize the feature selection process further [19]. Similarly, another study titled "Feature Selection using Pigeon Inspired Optimizer for Intrusion Detection System" discusses the successful implementation of PIO for feature selection in IDS [24].

While these works highlight the importance of feature selection and demonstrate the applicability of PIO for this purpose, our research aims to further optimize this process by introducing an adjustment in the activation function used in the PIO algorithm. This approach, which incorporates the Sigmoid activation function, ensure that the selected features fall within the range of 0-1. Thereby improving the effectiveness of the feature selection process and, in turn, the performance of the IDS in identifying intrusions in IoT environments.

2.2. Intrusion detection systems

IDS are crucial for network security [25], with significant advancements in the last five years to address threats like DDoS attacks, as highlighted by Zargar *et al.* [26]. Zhou *et al.* [27] improved IDS by using a combination of feature selection and ensemble strategies, enhancing accuracy and detection speed. Ho *et al.* [28] developed a CNN-based IDS model that reduced false positives in large-scale networks. Agarwal *et al.* [29] used machine learning to boost DDoS detection accuracy. Rawat *et al.* [30] demonstrated that deep learning outperforms classical machine learning in IDS performance.

IDS can be categorized into two types: network intrusion detection systems (NIDS) and host intrusion detection systems (HIDS). NIDS monitors network traffic to detect known attacks, while HIDS checks system files for anomalies within internal networks, as outlined by various sources [31], [32]. In the IoT context, IDS are increasingly important for protecting interconnected devices and ensuring the integrity of sensitive data they handle.

2.3. Feature selection

Feature selection is pivotal in data analysis, specifically during the pre-processing phase. The primary aim of this technique is to minimize the volume of features or attributes used in a data model, usually by discarding irrelevant or redundant data. The ultimate goal of feature selection is to pinpoint the most influential features from an expansive set of data attributes [33]. The feature selection technique addresses the issue of a situation where an excessively high number of features employed in an analysis or model degrades the algorithm's performance and lengthens processing time. Only the most relevant features contributing significantly to the target class are retained by applying feature selection methods. This boosts the model's performance and accelerates the processing time [34]. Feature selection is an indispensable step in the machine learning process as it notably enhances the accuracy and efficiency of the model while concurrently mitigating the risk of overfitting. The workflow of the feature selection process can be seen in Figure 1 feature selection process.

The feature selection process in SI for IDS in IoT environments involve several key stages. It begins with dataset selection, where appropriate datasets are chosen to ensure effective intrusion detection. Data sampling then extracts a representative subset of the dataset for processing. Data pre-processing follows, transforming and cleaning the data. The gain information method is used for feature selection, identifying the most informative features to improve IDS accuracy and efficiency. After feature selection, the classification stage uses these features to detect intrusions. Finally, performance analysis evaluates the IDS using metrics like accuracy, recall, and precision to ensure effectiveness. Overall, this process enhances the IDS by focusing on relevant features and performance evaluation.

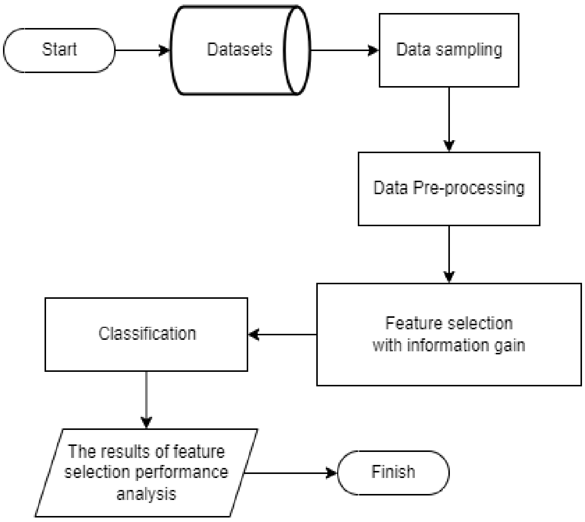

Start
Datasets
Data sampling
Data Pre-processing
Feature selection with information gain
Classification
The results of feature selection performance analysis
Finish

Figure 1. Feature selection process

2.4. Dataset

In this study, we utilize two distinct datasets to validate our research. The first one is the CIC IoT dataset 2023 [34], developed by the Canadian Institute for Cybersecurity. This dataset reflects a comprehensive selection of real-world IoT network traffic and attack scenarios, covering various IoT devices and different types of attacks. It offers a broad scope for evaluating the performance and robustness of our IDS model. The dataset includes approximately 2 million records and consists of 75 features such as source and destination IP addresses, packet length, timestamp, protocol type, and other network-related features relevant to IoT environments. With a data size of roughly 20 GB, it simulates common IoT attacks, including denial of service (DoS), man in the middle (MitM), and password attacks. Its relevance lies in its ability to provide a rich mix of benign and malicious IoT traffic, ensuring our IDS model is tested under conditions that closely resemble real-world IoT environments.

The second dataset is the IoT dataset for IDS [35], which is renowned for its depth and variety. This dataset includes interactions between multiple IoT devices, normal network behaviors, and various intrusion or attack instances. Specifically designed for the research and development of IDS, it provides valuable insights for evaluating and improving IDS models in an IoT context. With over 1.5 million records and 68 features, it focuses on both basic network attributes such as IP addresses and packet sizes, as well as more intricate details like packet sequences in a connection and byte order within a packet. The dataset size is approximately 15 GB, and it covers a wide range of IoT-specific attack vectors, such as side-channel attacks, network spoofing, and malware targeting IoT devices. Its comprehensive nature makes it an excellent foundation for testing IDS systems, making it an ideal choice for our research. Both datasets, with their diverse and comprehensive data, provide an excellent platform for developing and validating our IDS model, particularly in an IoT environment. Their extensive data, encompassing both normal and malicious network behaviors, allows us to effectively train our model and evaluate its performance under various conditions and attack scenarios.

2.5. Swarm intelligence

SI is a concept derived from the collective behavior of decentralized, self-organized systems. These systems usually consist of a population of simple agents interacting with each other and their environment. Inspiration is often drawn from nature, particularly biological systems. Examples of SI in nature include ant colonies, bird flocking, animal herding, and more. SI is widely applied in optimization algorithms, including the PIO algorithm [36]. PIO is an algorithm inspired by the navigational behavior of pigeons. In nature, pigeons have remarkable navigation abilities to find their way back to their nests from distant locations.

In the context of feature selection in machine learning, the PIO works to seek out the most informative feature combinations from a dataset. Each “pigeon” in the algorithm represents a feature and explores the search space for the best features. Each pigeon adjusts its position and velocity based on specific rules at each algorithm iteration, aiming to optimize the features chosen. PIO is used in feature selection because this algorithm can find the optimal solution in a vast and complex search space, as often faced in machine learning.

The PIO is effective at searching for and discovering the most informative features that can enhance the effectiveness of our machine learning model. Furthermore, the PIO also has high flexibility and adaptability, allowing it to adapt to data and environment changes. Therefore, the PIO is a good choice for the feature selection process in our machine-learning model [37].

2.6. Modified pigeon inspired optimization for feature selection with sigmoid

When dealing with IDS datasets, artificial neural networks (ANNs) are an effective means for data analysis and detecting anomalous patterns [16]. In this context, the PIO algorithm is crucial in identifying optimal parameters for the ANN, enhancing the model's predictive accuracy. Feature selection techniques can be applied to hone in on the most relevant features, allowing the ANN to concentrate its computational power on these important attributes and reduce the data dimensionality [38]. The Sigmoid function is commonly employed as an activation function in ANNs [39]. This function maps any input value into a range between 0 and 1. The output of the Sigmoid function forms an S-shaped curve, which is useful for producing binary outputs for binary classification problems. Moreover, the Sigmoid function helps manage the 'exploding gradient' issue and facilitates efficient and effective training of the ANN. Although the Sigmoid function can suffer from the 'vanishing gradient' problem during backpropagation, it's a viable choice for certain types of ANNs and specific datasets

3. RESULTS AND DISCUSSION

Employing a quantitative method, this research focuses on harnessing SI for IDS within the IoT environments. Its key merits include performance quantification, dataset appraisal, and the practical implications of the findings. The deductive reasoning approach has been chosen for this study as it is most apt for evaluating the suggested solution.

The study's structure comprises three essential stages: pre-processing, where the data is readied for analysis; processing via the PIO technique, which exemplifies SI principles; and evaluation, where the effectiveness of the IDS is assessed. Each phase's significance and intricate workings will be further elaborated upon in the forthcoming segments. This structured approach allows for an exhaustive examination and facilitates a comprehensive understanding of the potency of SI in enhancing the efficacy of IDS within IoT environments.

3.1. Pre-processing phase

In the realm of SI for IDS within the IoT environments, pre-processing is a crucial step. This phase ensures that the input data is streamlined and filtered to eliminate irrelevant or redundant elements, including duplicate packets, recognized benign traffic, and data that does not contribute to the intrusion detection capabilities. The first crucial process within this phase is the filtering step. It involves the removal of any unnecessary data, leaving only what can be effectively utilized by the PIO algorithm. This could include converting all IP addresses into a canonical form, aligning timestamps to a uniform time zone, and other similar normalization activities that make the data more accessible for the detection algorithm.

Following this, we undertake the feature extraction process. All relevant features that can feed into the SI-based detection algorithm are extracted from the processed data. This could involve statistical features like average packet size, connections per second or structural features like the sequence of packets in a connection or byte order within a packet. These features are critical for effectively working the PIO algorithm within the IDS. Simultaneously, data normalization is carried out. All symbolic data is translated into numeric values, making it suitable for analysis by the algorithm. The class field input is adjusted to binary values - 0 or 1 - where 0 denotes a normal record, and 1 indicates an attack record, regardless of the type of attack. Thus, the pre-processing phase effectively prepares the data for subsequent processing via the PIO technique, setting the foundation for an efficient IDS within IoT environments.

3.2. Processing phase

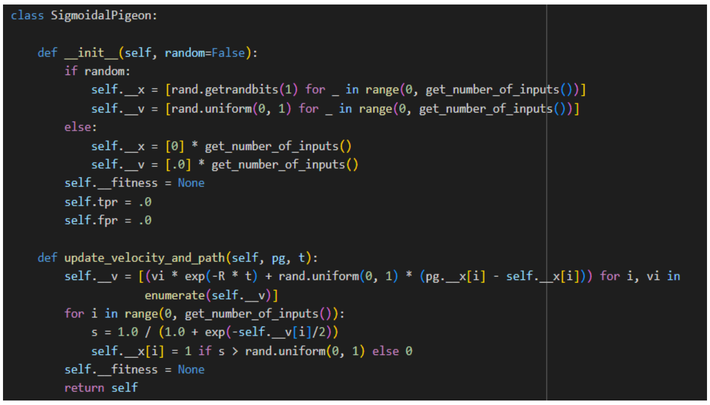
In applying SI for IDS in the IoT environments, the processing phase takes the modified and streamlined data from the pre-processing phase. It begins to analyze it using a tailored PIO algorithm. The PIO algorithm employed here has been innovatively adapted to enhance its feature selection capabilities. While the conventional PIO algorithm has shown promising results in tackling various optimization problems within feature selection, our study further rectifies certain limitations within the conventional approach. The key modification approached with the Sigmoid activation function. The Sigmoid activation function represented mathematically as (1) [39]:

$$f(x) = 1/(1 + exp(-x) \quad (1)$$

Has proven to be particularly effective for deep learning applications. It transforms its real-valued input to the range (0, 1), which can be used for binary classification. Each data input is subjected to the Sigmoid activation function in this tailored algorithm, transforming it into a value between 0 and 1. Following this, the PIO algorithm is leveraged to optimize weights and biases to minimize the error in each iteration. The fusion of these two techniques is designed to allow the neural network to learn swiftly and deliver high accuracy in performing classification or regression tasks.

The integration of Sigmoid activation and PIO into the IDS within the IoT environment is expected to expedite learning algorithms effectively and provide a reliable classification or regression analysis [40]. To elaborate, the algorithm below demonstrates the operation of this modified PIO approach. The unique structure and process help in crafting an optimized SI for IDS in IoT environments.

In Figure 2, Sigmoid_PIO algoritm showing our code presents an implementation of Sigmoid_PIO, a modified version of the PIO algorithm. In the init method, a new instance of the SigmoidPigeon class is created with random or zero values assigned to the bird's position and velocity. This sets the initial state of the algorithm before the optimization process starts. The update velocity and path method is important in updating the bird's position and velocity based on the Sigmoid function. the Sigmoid function maps the input to a value between 0 and 1. In doing so, the position and speed of the bird is adjusted using the Sigmoid function, ensuring that the value falls within this range.



```
class SigmoidalPigeon:

    def __init__(self, random=False):
        if random:
            self.__x = [rand.getrandbits(1) for _ in range(0, get_number_of_inputs())]
            self.__v = [rand.uniform(0, 1) for _ in range(0, get_number_of_inputs())]
        else:
            self.__x = [0] * get_number_of_inputs()
            self.__v = [.0] * get_number_of_inputs()
        self.__fitness = None
        self.tpr = .0
        self.fpr = .0

    def update_velocity_and_path(self, pg, t):
        self.__v = [(vi * exp(-R * t) + rand.uniform(0, 1) * (pg.__x[i] - self.__x[i])) for i, vi in
                  enumerate(self.__v)]
        for i in range(0, get_number_of_inputs()):
            s = 1.0 / (1.0 + exp(-self.__v[i]/2))
            self.__x[i] = 1 if s > rand.uniform(0, 1) else 0
        self.__fitness = None
        return self
```

Figure 2. Sigmoid_PIO algoritm

- Performance metrics

Table 1 comparison between PIO and Sigmoid_PIO with data sets CIC IoT dataset 2023 shows a comparison between the PIO and Sigmoid_PIO approaches using the CIC IoT dataset 2023. Through this table, it can be observed that the Sigmoid_PIO method outperforms the PIO method. For the PIO method, the true positive rate is 0.871, the false positive rate is 0.095, the accuracy is 0.811, and the F-Score is 0.855. In contrast, the Sigmoid_PIO method exhibits a higher true positive rate of 0.927, a slightly higher false positive rate of 0.098, but a significant improvement in accuracy, achieving 0.945, and an F-Score of 0.930. Therefore, based on this data, the Sigmoid_PIO seems to deliver better results in detecting IoT attacks on the CIC IoT dataset 2023 compared to the PIO method.

Table 1. Comparison between PIO and Sigmoid_PIO with data sets CIC IoT dataset 2023

Approach	True positive rate	False positive rate	Accuracy	F-Score
PIO	0.871	0.095	0.811	0.855
Sigmoid_PIO	0.927	0.098	0.945	0.930

Table 2 comparison between PIO and Sigmoid_PIO with data sets IoT dataset for IDS presents a comparison of the PIO and Sigmoid_PIO methods utilizing the IoT dataset for IDS. The PIO method displays a true positive rate of 0.863, a false positive rate of 0.094, an accuracy of 0.803, and an F-Score of 0.834. In contrast, the Sigmoid_PIO method manifests superior performance with a higher true positive rate of 0.927, although it shows a substantially higher false positive rate of 0.906. However, it achieves an increased accuracy of 0.928 and an improved F-Score of 0.902. Accordingly, based on the provided data, the Sigmoid_PIO offers improved performance in identifying IoT threats on the IoT dataset for IDS compared to the PIO method, despite its higher false positive rate.

Table 2. Comparison between PIO and Sigmoid_PIO with data sets IoT dataset for IDS

Approach	True positive rate	False positive rate	Accuracy	F-Score
PIO	0.863	0.094	0.803	0.834
Sigmoid_PIO	0.927	0.906	0.928	0902

4. CONCLUSION

Compared to the PIO method, the Sigmoid_PIO method consistently achieved higher true positive rates on both the CIC IoT Dataset 2023 and IoT dataset for IDS. This suggests that it could be more effective at correctly identifying true intrusions, an important feature for intrusion detection systems. In conclusion, the findings suggest that SI methods, specifically Sigmoid_PIO, could be aluable tools for intrusion detection in IoT environments.

ACKNOWLEDGEMENTS

The research is funded by the Universitas Islam Riau (Ref :564/KONTRAK/P-PT/DPPM-UIR/06-2023).

REFERENCES

[1] M. A. Amanullah *et al.*, "Deep learning and big data technologies for IoT security," *Computer Communications*, vol. 151, pp. 495-517, 2020, doi: 10.1016/j.comcom.2020.01.016.

[2] D. Thakur, J. K. Saini, and S. Srinivasan, "DeepThink IoT: The Strength of Deep Learning in Internet of Things," *Artificial Intelligence Review*, vol. 56, no. 12, pp. 14663–14730, 2023, doi: 10.1007/s10462-023-10513-4.

[3] E. A. Kadir, M. Abdurrahman, S. K. A. Rahim, A. Arsad, S. L. Rosa, and A. Siswanto, "Oil Well Monitoring System Based on IoT Technology and Machine Learning," *2022 7th International Conference on Informatics and Computing, ICIC 2022*. IEEE, pp. 1–6, 2022, doi: 10.1109/ICIC56845.2022.10006948.

[4] A. E. Omolara *et al.*, "The internet of things security: A survey encompassing unexplored areas and new insights," *Computers and Security*, vol. 112, p. 102494, 2022, doi: 10.1016/j.cose.2021.102494.

[5] P. R. Kannari, N. S. Chowdary, and R. L. Biradar, "An anomaly-based intrusion detection system using recursive feature elimination technique for improved attack detection," *Theoretical Computer Science*, vol. 931, pp. 56–64, 2022, doi: 10.1016/j.tcs.2022.07.030.

[6] P. Kumar, S. Chauhan, and L. K. Awasthi, "Artificial Intelligence in Healthcare: Review, Ethics, Trust Challenges & Future Research Directions," *Engineering Applications of Artificial Intelligence*, vol. 120, p. 105894, 2023, doi: 10.1016/j.engappai.2023.105894.

[7] S. S. Tripathy *et al.*, "State-of-the-Art Load Balancing Algorithms for Mist-Fog-Cloud Assisted Paradigm: A Review and Future Directions," *Archives of Computational Methods in Engineering*, vol. 30, no. 4, pp. 2725–2760, 2023, doi: 10.1007/s11831-023-09885-1.

[8] R. Rai, "Swarm Intelligence and Bio-Inspired Computation," *Research Notes on Computing and Communication Sciences: Applied Soft Computing: Techniques and Applications*. Apple Academic Press, pp. 1–22, 2022, doi: 10.1201/9781003186885-1.

[9] L. Abualigah, D. Falcone, and A. Forestiero, "Swarm Intelligence to Face IoT Challenges," *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, p. 4254194, May 2023, doi: 10.1155/2023/4254194.

[10] J. Webster, *Animal Welfare: Understanding Sentient Minds and Why It Matters*. Wiley, 2022, doi: 10.1002/9781119857099.

[11] J. Liu, S. Anavatti, M. Garratt, K. C. Tan, and H. A. Abbass, "A survey, taxonomy and progress evaluation of three decades of swarm optimisation," *Artificial Intelligence Review*, vol. 55, no. 5, pp. 3607–3725, 2022, doi: 10.1007/s10462-021-10095-z.

[12] R. F. Mansour, "Blockchain assisted clustering with Intrusion Detection System for Industrial Internet of Things environment," *Expert Systems with Applications*, vol. 207, p. 117995, 2022, doi: 10.1016/j.eswa.2022.117995.

[13] M. Torky, I. Gad, and A. E. Hassanien, "Explainable AI Model for Recognizing Financial Crisis Roots Based on Pigeon Optimization and Gradient Boosting Model," *International Journal of Computational Intelligence Systems*, vol. 16, no. 1, 2023, doi: 10.1007/s44196-023-00222-9.

[14] A. Alzaqebah, I. Aljarah, O. Al-Kadi, and R. Damaševičius, "A Modified Grey Wolf Optimization Algorithm for an Intrusion Detection System," *Mathematics*, vol. 10, no. 6, p. 999, 2022, doi: 10.3390/math10060999.

[15] O. Abualghanam, H. Alazzam, B. Elshqeirat, M. Qatawneh, and M. A. Almaiah, "Real-Time Detection System for Data Exfiltration over DNS Tunneling Using Machine Learning," *Electronics (Switzerland)*, vol. 12, no. 6, p. 1467, 2023, doi: 10.3390/electronics12061467.

[16] A. Thakkar and R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, 2021, doi: 10.1007/s11831-020-09496-0.

[17] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975–990, 2020, doi: 10.3745/JIPS.03.0144.

[18] M. H. Nasir, S. A. Khan, M. M. Khan, and M. Fatima, "Swarm Intelligence inspired Intrusion Detection Systems — A systematic literature review," *Computer Networks*, vol. 205, p. 108708, 2022, doi: 10.1016/j.comnet.2021.108708.

[19] O. A. Alghanam, W. Almobaideen, M. Saadeh, and O. Adwan, "An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning," *Expert Systems with Applications*, vol. 213, p. 118745, 2023, doi: 10.1016/j.eswa.2022.118745.

[20] S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *Journal of Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00379-6.

[21] M. M. Rahman, O. L. Usman, R. C. Muniyandi, S. Sahran, S. Mohamed, and R. A. Razak, “A review of machine learning methods of feature selection and classification for autism spectrum disorder,” *Brain Sciences*, vol. 10, no. 12, pp. 1–23, Dec. 2020, doi: 10.3390/brainsci10120949.

[22] J. Brownlee, *Data Preparation for Machine Learning: Data Cleaning, Feature Selection, and Data Transforms in Python*. Machine Learning Mastery, 2020.

[23] V. N. Gopal, F. Al-Turjman, R. Kumar, L. Anand, and M. Rajesh, “Feature selection and classification in breast cancer prediction using IoT and machine learning,” *Measurement: Journal of the International Measurement Confederation*, vol. 178, p. 109442, 2021, doi: 10.1016/j.measurement.2021.109442.

[24] H. Alazzam, A. Sharieh, and K. E. Sabri, “A feature selection algorithm for intrusion detection system based on Pigeon Inspired Optimizer,” *Expert Systems with Applications*, vol. 148, p. 113249, 2020, doi: 10.1016/j.eswa.2020.113249.

[25] A. Tedyyana, O. Ghazali, and O. W. Purbo, “A real-time hypertext transfer protocol intrusion detection system on web server,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 21, no. 3, pp. 566–573, 2023, doi: 10.12928/TELKOMNIKA.v21i3.24938.

[26] S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks,” *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013, doi: 10.1109/SURV.2013.031413.00127.

[27] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, “Building an efficient intrusion detection system based on feature selection and ensemble classifier,” *Computer Networks*, vol. 174, p. 107247, 2020, doi: 10.1016/j.comnet.2020.107247.

[28] S. Ho, S. Al Jufout, K. Dajani, and M. Mozumdar, “A Novel Intrusion Detection Model for Detecting Known and Innovative Cyberattacks Using Convolutional Neural Network,” *IEEE Open Journal of the Computer Society*, vol. 2, pp. 14–25, 2021, doi: 10.1109/OJCS.2021.3050917.

[29] A. Agarwal, M. Khari, and R. Singh, “Detection of DDOS Attack using Deep Learning Model in Cloud Storage Application,” *Wireless Personal Communications*, vol. 127, no. 1, pp. 419–439, 2022, doi: 10.1007/s11277-021-08271-z.

[30] S. Rawat, A. Srinivasan, V. Ravi, and U. Ghosh, “Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network,” *Internet Technology Letters*, vol. 5, no. 1, 2022, doi: 10.1002/itl2.232.

[31] A. Tedyyana and O. Ghazali, “Teler real-time http intrusion detection at website with nginx web server,” *International Journal on Informatics Visualization*, vol. 5, no. 3, pp. 327–332, 2021, doi: 10.30630/joiv.5.3.510.

[32] A. Chawla, B. Lee, S. Fallon, and P. Jacob, “Host Based Intrusion Detection System with Combined CNN/RNN Model,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, LNAI. Springer International Publishing, vol. 11329, pp. 149–158, 2019, doi: 10.1007/978-3-030-13453-2_12.

[33] K. A. Taher, B. M. Y. Jisan, and M. M. Rahman, “Network intrusion detection using supervised machine learning technique with feature selection,” *1st International Conference on Robotics, Electrical and Signal Processing Techniques, ICREST 2019*. IEEE, pp. 643–646, 2019, doi: 10.1109/ICREST.2019.8644161.

[34] U. M. Khaire and R. Dhanalakshmi, “Stability of feature selection algorithm: A review,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 4, pp. 1060–1073, 2022, doi: 10.1016/j.jksuci.2019.06.012.

[35] A. Alhowaide, I. Alsmadi, and J. Tang, “Features Quality Impact on Cyber Physical Security Systems,” *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2019*. IEEE, pp. 332–339, 2019, doi: 10.1109/IEMCON.2019.8936280.

[36] J. Tang, G. Liu, and Q. Pan, “A Review on Representative Swarm Intelligence Algorithms for Solving Optimization Problems: Applications and Trends,” *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 10, pp. 1627–1643, 2021, doi: 10.1109/JAS.2021.1004129.

[37] A. Sharma, S. Shoval, A. Sharma, and J. K. Pandey, “Path Planning for Multiple Targets Interception by the Swarm of UAVs based on Swarm Intelligence Algorithms: A Review,” *IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)*, vol. 39, no. 3, pp. 675–697, 2022, doi: 10.1080/02564602.2021.1894250.

[38] Y. Yin *et al.*, “IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset,” *Journal of Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00694-8.

[39] M. O. Oluwayemi, O. A. Fadipe-Joseph, and U. A. Ezeafulukwe, “Certain subclass of univalent functions involving modified sigmoid function,” *Journal of Physics: Conference Series*, vol. 1212, no. 1, p. 12005, 2019, doi: 10.1088/1742-6596/1212/1/012005.

[40] P. TS and P. Shrinivasacharya, “Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security,” *Global Transitions Proceedings*, vol. 2, no. 2, pp. 448–454, 2021, doi: 10.1016/j.gltp.2021.08.017.

BIOGRAPHIES OF AUTHORS

Apri Siswanto is Senior lecturer at Informatics Department, Faculty of Engineering, Universitas Islam Riau, Pekanbaru, Indonesia. He holds a Ph.D. degree in Computer Science with specialization in Biometric, Security and Internet of Things from School of Computing, Universiti Utara Malaysia. His research areas are networking, security, biometrics, and internet of things system. He is head of Department of Informatics Engineering, Universitas Islam Riau. His research interests include routing and switching, security, biometrics security, and internet of thing system. He can be contacted at email: aprisiswanto@eng.uir.ac.id.

Akmar Efendi received the B.Sc. and Master degree in computer science from the Universitas Putra Indonesia, Padang, West Sumatra. He is Deputy Dean of student affairs, alumni and cooperation in Faculty of Engineering, Universitas Islam Riau. He is also managing editor Journal of Inovtek Polbeng Seri Informatika. His research interest includes data science, programming, and information system. He can be contacted at email: akmarefendi@eng.uir.ac.id.

Jaroji received the B.Sc. from Sekolah Tinggi Ilmu Komputer Pelita Indonesia and Master degree in Computer Science from the Universitas Putra Indonesia, Padang, West Sumatra. He is a lecturer in the Politeknik Bengkalis in information systems security study program. His research interest includes artificial intelligence, machine learning, deep learning, computer programming, and software engineering. He can be contacted at email: jaroji@polbeng.ac.id.

Fajar Ratnawati received the B.Sc. from STMIK AKAKOM Yogyakarta and Master degree in computer science from the Universitas Gadjah Mada Yogyakarta. She is a lecturer in the Politeknik Bengkalis in software engineering study program. Her research interest includes artificial intelligence, computer programming, and software engineering. She can be contacted at email: fajar@polbeng.ac.id.