International Journal of Data Science and Artificial Intelligence (IJDSAI)
Volume 02, Issue 06, November – December (2024)

RESEARCH ARTICLE

DOLO-ID: DINGO OPTIMIZED HIERARCHICAL AUTO-ASSOCIATIVE POLYNOMIAL CONVOLUTIONAL NEURAL NETWORKS FOR INTRUSION DETECTION

Abdullah Muhammad Noman [1, *], Sakiru Adebola Solarin[2] and Lye Chun Teck [3]

[1] Research scholar, Faculty of Business, Multimedia university,75450 Melka, Malaysia.
[2] Professor, Economics, Faculty of Business, Multimedia University Malaysia.
[3] Faculty of Business (FOB), Multimedia University (MMU), Malaysia.

[*]*Corresponding e-mail: abdullahnoman777@gmail.com*

Abstract – The Internet of Things (IoT) facilitates the seamless integration of diverse physical devices with the Internet, enabling groundbreaking applications across sectors such as defense, transportation, agriculture, and healthcare. These applications have gained significant traction due to their capacity to address real-time challenges efficiently. Nevertheless, IoT systems are inherently vulnerable to security threats, exposing them to various cyberattacks that can compromise their functionality and reliability. To address these challenges, a novel Dingo Optimized hierarchicaL Auto-Associative pOlynomial convolutional neural networks for Intrusion Detection (DOLO-ID) approach has been proposed to enhance security and detect intrusion effectively. The raw data is pre-processed through cleaning and normalization to enhance quality and usability. Feature selection is achieved using the Dingo Optimization which iteratively identifies and optimizes the most relevant features for classification tasks. The selected features are fed into a deep learning architecture incorporating a HAPP CNN Network for accurate classification of intrusions into categories such as attack or normal. The f1score, recall, precision, and accuracy of the proposed DOLO-ID method are 92.8%, 91%, 92% and 98.56% which is higher than the existing techniques.

Keywords *– Dingo Optimization, Internet of Things, Polynomial convolutional neural networks, Cyberattack, Preprocessing.*

1. INTRODUCTION

The rapid proliferation of the IoT has revolutionized industries by enabling seamless communication and automation across interconnected devices [1]. IoT has been widely adopted in numerous sectors including healthcare, smart homes, transportation, and industrial automation, owing to its ability to improve efficiency and enhance user experiences [2-5]. However, this widespread adoption has also introduced important security vulnerabilities, as IoT devices are often resource-constrained, lack robust security mechanisms, and are installed in diverse environments [6,7].

These vulnerabilities expose IoT networks to a wide range of cyber threats, namely data breaches, distributed denial-of-service (DDoS) attacks, and unauthorized access [8,9]. IDS have emerged as a critical component of IoT security frameworks developed to monitor network traffic and predict malicious activities in real time [10,11]. Traditional IDS frameworks however, face problems in the IoT landscape due to the heterogeneity and scalability of IoT networks as well as the evolving sophistication of cyberattacks [12-15]. To address these challenges, a novel DOLO-ID approach has been proposed to enhance the security and detecting intrusion effectively. The major contribution of the work are as follows,

- Initially, the raw data is collected from IoT sensors deployed on network devices. This raw data undergoes pre-processing utilizing data cleaning and normalization to enhance the data.
- Feature selection is performed using Dingo Optimization, which selects the most relevant features and iteratively optimizes the feature set for classification tasks.
- Finally selected features are then fed into a DL architecture comprising HAPP CNN Network classification of intrusion into categories such as attack and normal classes.
- The efficacy of the suggested approach is evaluated utilizing several parameters including F1-score, precision, accuracy, and recall.

The remaining portion of this research is organized as follows, the Literature survey is summarized in section 2, and Section 3 details the suggested framework. Section 4 details the result and discussion. The future work and conclusion are included in Section 5.

2. LITERATURE SURVEY

Various frameworks have been introduced by researchers for intrusion detection utilizing ML, and DL frameworks. A few recent techniques in intrusion detection are outlined in this section.

In 2023, Altunay, H.C. and Albayrak, Z., [16] suggested three different deep-learning models to enhance intrusion detection in IIoT networks. These models utilized CNN, LSTM, and a hybrid CNN + LSTM architecture. Notably, the CNN+LSTM hybrid model demonstrated remarkable performance. Using the UNSW-NB15 dataset, it obtained 92.9% accuracy for multiple classes and 93.21% effectiveness for binary categorization. These results underscore the effectiveness of DL approaches for securing IIoT networks against intrusions.

In 2023, Sanju, P., [17] suggested a metaheuristics-DL framework for enhancing intrusion detection in IoT systems. Inclusive, the suggested approach offerings a capable result for improving intrusion detection in IoT systems, and it has the potential to serve as a foundation for future research in this field.

In 2023, Elnakib, O., et al., [18] introduced an enhanced anomaly-combined Intrusion Detection Deep Learning Multi-class classification model (EIDM) that uses the CICIDS2017 dataset to categorize 15 traffic patterns, including 14 different forms of attacks, with a 95% accuracy rate. EIDM has produced reliable detection findings, according to a thorough comparison of efficiency metrics and classification accuracy between EIDM and numerous cutting-edge DL-based IDS.

In 2024, Nandanwar, H. and Katarya, R., [19] suggested a DL approach named AttackNet for the detection and classification of different botnet attacks in IIoT based on an adaptive-based CNN-GRU framework. The findings obtained an accuracy of 99.75% across ten classes, outperforming previous approaches by a substantial margin ranging from 3.2% to 16.07%.

In 2023, Altaf, T., et al., [20] introduced a GNN-based network IDS that optimizes the likelihood of incorporating structural elements of both legitimate and malevolent network traffic. In the datasets under consideration, the suggested model offers a 2% to 5% gain in precision, accuracy, recall, and F1, while requiring less training time and approach size.

Various intrusion detection techniques have shown potential from the literature survey, but several drawbacks persist [16, 19]. Many frameworks struggle with scalability and adaptability in diverse environments [17, 20]. To tackle these issues this paper introduced a novel DOLO-ID framework to enhance network security by accurately identifying and mitigating cyber threats which is mentioned in the following section

3. PROPOSED METHOD

In this section, a DOLO-ID technique has been proposed to accurately classify IoT attacks. Initially, the raw data is collected from IoT sensors deployed on network devices. This raw data undergoes pre-processing namely data cleaning and normalization to enhance the data. The feature selection process utilizes Dingo Optimization which select relevant features and optimizing the feature set iteratively for classification tasks. The selected features are then fed into a DL architecture comprising HAPP CNN Network classification of intrusion into categories such as attack and normal classes. Figure 1 shows the overall flow of suggested DOLO-ID.

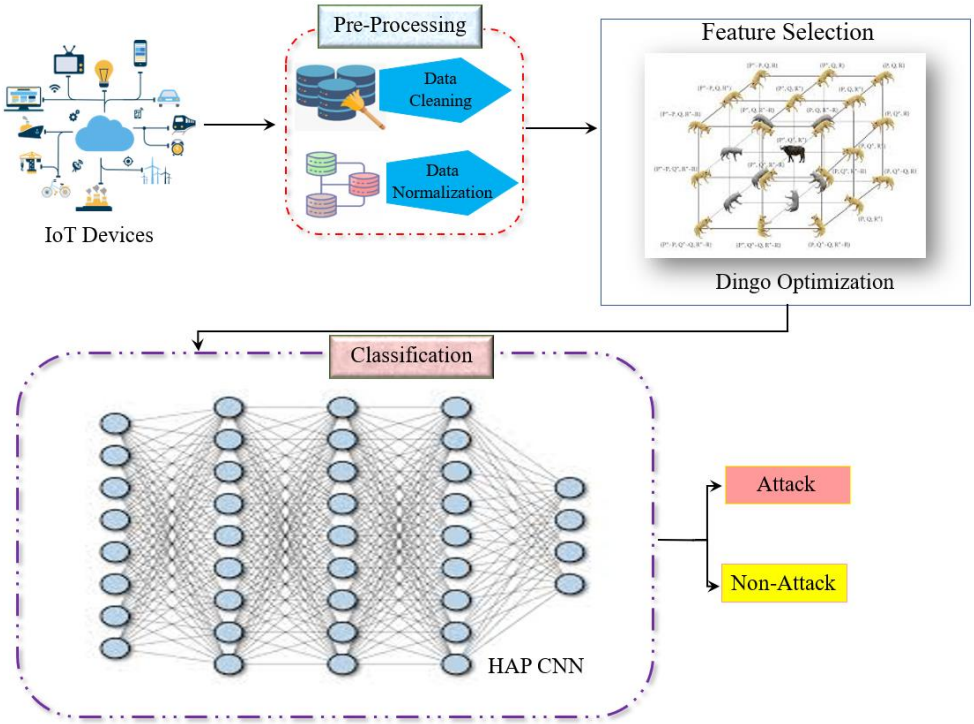

Figure 1. Block diagram of the suggested framework

3.1. Data Preprocessing

Preprocessing is the process of converting input data into a useful format by removing irrelevant data. The accuracy and efficiency of the model can only be increased by modifying and preparing the data to make it appropriate for the learning process.

Data Cleaning: Data cleaning implies correcting errors and detecting inconsistencies in the data to improve its quality. This process includes addressing null values using techniques such as median, interpolation and means and handling outliers by either removing them or transforming them into a more suitable range.

Data Normalization: Data normalization scales features to a standard range to increase the efficiency of DL models. In this work, the Standardized Scalar normalization technique is utilized, which transforms the data to have a mean of 0 and a variance of 1. These assurances that every feature contributes equally to the learning process and enhances detection results.

3.2. Feature selection via Dingo Optimization

Improved Dingo Optimization's optimization model is made for feature selection, which optimizes data and offers pertinent features. Finding the best real-world system solutions is a difficult task. because there are multiple excellent solutions available. (1) – (3) strengthen the persecution, scavenging, group assault, and survival.

$$\partial = (\mathrm{BF} - \mathrm{WF}) \tag{1}$$

$$\mathrm{Y} = \frac{\mathrm{mean(D(F-WF))}}{\mathrm{mean(D(F-BF))}} \tag{2}$$

$$\mathrm{UB} = \partial \times \left(\frac{\mathrm{q}}{\mathrm{Y}}\right) \tag{3}$$

The best and worst objective functions are denoted by the terms BF and WF, respectively, in this instance. Fitness is represented by F, distance by D, generality by Y and q, and arbitrarily by UB, which is a number between 0 and 1.

Step 1 - Group Attack: Dingoes hunt in packs, encircling their target using their tracking abilities. There is an equation that represents this.

$$\overrightarrow{\mathrm{D_b}}(\mathrm{l}+1) = \propto_1 \sum_{\mathrm{v}=1}^{\mathrm{ui}} \left(\frac{\overrightarrow{\emptyset \mathrm{k}(\mathrm{d})} - \mathrm{d}\vec{\mathrm{p}}(\mathrm{l})}{\mathrm{ui}}\right) - \vec{\mathrm{d}} \times (\mathrm{l}) \tag{4}$$

The expression $\overrightarrow{\mathrm{D_b}}(\mathrm{l}+1)$ represents the position of the feature, ui is a random number, $\mathrm{d}\vec{\mathrm{p}}$ represents the best iteration constructed utilizing the preceding iteration, $\vec{\mathrm{d}} \times (\mathrm{z})$ tends the search agent, $\emptyset\mathrm{k}(\mathrm{d})$ is the sub-set provided for all search agents and $\propto_1$ is a randomly generated number equally produced and displayed in a range of [-2, 2]. It has been updated in Equation (4).

Step 2 - Persecution: Dingoes frequently hunt tiny animals until they are within reach. Equation (5) provides an illustration of this behaviour.

$$\vec{\mathrm{d}}_\mathrm{p}(\mathrm{l}+1) = \vec{\mathrm{d}} \times (\mathrm{l}) + \propto_1 + \mathrm{f}^{\propto_2} \times (\vec{\mathrm{d}}_{\mathrm{q}_1}(\mathrm{l}) - \vec{\mathrm{d}}_\mathrm{p}(\mathrm{l})) \tag{5}$$

Here, the term $\vec{\mathrm{d}}_\mathrm{p}(\mathrm{l}+1)$ denotes a dingo movement within the search engine $\vec{\mathrm{d}}_\mathrm{p}(\mathrm{l})$.The derived random variable falls within [−1, 1] is represented as $\propto_2$, arbitrary number q_1 is updated in Equation (3) and $\vec{\mathrm{d}}_{\mathrm{q}_1}(\mathrm{l})$ represents the search agent for the qth interval.

Step 3 - Scavenger: Equation (6) describes the scavenging behavior of dingoes, which is thought of as an activity when they locate their meal.

$$\vec{\mathrm{d}}_\mathrm{p}(\mathrm{l}+1) = \frac{1}{2}[\mathrm{f}^{\propto_2} \times \vec{\mathrm{d}}_{\mathrm{q}_1}(\mathrm{l}) - (-1)^\sigma \times \vec{\mathrm{d}}_\mathrm{p}(\mathrm{l})] \tag{6}$$

The binary number, represented by the symbol σ, is produced spontaneously and is upgraded in Equation (3).

Step 4 - The dingo's survival rate is given in Equation (7).

$$\mathrm{surv(D)} = \frac{\mathrm{BF-F(D)}}{\mathrm{BF-WF}} \tag{7}$$

In the current generation, the least fitness function is represented as WF and BF represents the highest level of fitness. Fs(D) is the fitness value provided for Dth search features and also Equation (8) determines the minimal survival rate.

$$\vec{\mathrm{d}}_\mathrm{p}(\mathrm{l}+1) = \vec{\mathrm{d}} \times (\mathrm{l}) + \frac{1}{2}[\vec{\mathrm{d}}_{\mathrm{q}_1}(\mathrm{l}) - (-1)^\sigma \times \vec{\mathrm{d}}_{\mathrm{q}_2}(\mathrm{l})] \tag{8}$$

The chosen search agent for the numerical value q_1 and q_2 is stated as $\vec{\mathrm{d}}_{\mathrm{q}_1}(\mathrm{l})$ and $\vec{\mathrm{d}}_{\mathrm{q}_2}(\mathrm{l})$, correspondingly, and Equation (4) updates the random integers. Here, the lowest survival rate is indicated as $\vec{\mathrm{d}}_\mathrm{p}(\mathrm{l})$.

3.3. Classification via HAP-CNN

The selected features are classified into two categories such as Attack or Normal using the HAP-CNN, which is designed for high-dimensional data. This deep learning model enhances classification accuracy by introducing polynomial layers into a standard convolutional neural network (CNN), allowing it to capture complex data patterns with localized connectivity.

The HAP-CNN architecture employs a hierarchical structure that captures multiple feature levels while integrating auto-associative layers to learn and reconstruct input features, supporting both feature learning and noise reduction. By utilizing polynomial functions, it models complex relationships, allowing for non-linear transformations. Starting with an input layer that processes raw sensor data, each subsequent layer captures progressively abstract features. Trained on labelled data, the network maps sensor inputs to functional labels, minimizing prediction errors and enhancing classification performance. This design strengthens feature robustness without requiring major modifications to the traditional CNN structure.

Initially, the input feature-extracted data are fed into the input layer of HA-PCNN. The suggested polynomial function is then applied within the convolutional section after selecting the feature-extracted input data in the pooling layer, as described in Equation (9).

$$w_{\emptyset 1}(p,q,r,k) = w_{\emptyset 1}(p,q,r,k)^k; k = 1,2,3,\ldots.,K \tag{9}$$

Where, p, q, r denote the dimension and the input layer is implemented in the dimension r dimension. Here, the forward pass sustains normally the remainder of each

iteration, $\emptyset = 1,2,3,\ldots,S$ which means that the weight dimension is also different. Also, the FC layers are done based on this function and it is denoted as equation (10)

$$FC_{\lambda 1}(t,k) = FC_{\lambda 0}(t)^{k} \quad (10)$$

Where, $\lambda = 1,2,3,\ldots,K$ that is done for every iteration value. The polynomial layer is seen as the previous layer that has been modified by analyzing changes in backward propagation. This is because it has the same type of connections as it would have if there were no polynomials. The output layer loss is passed through the polynomial layer that is given by equation (11),

$$e_{\lambda prepoly}(t) = \sum_{k=1}^{K} e_{\lambda prepoly}(t,k) \quad (11)$$

In equation (11), $e_{\lambda prepoly}(t) \infty e_{\lambda prepoly}(t,k)$ is changed using the pooling and activation functions. Based on this, the error propagated backward function is given in equation (12),

$$e_{\lambda}(t,k) = \sum_{ly=1}^{LY} e_{\lambda}(ly) W_{\lambda}(ly,t,k) \quad (12)$$

In equation (12), ly denotes the layer and $e_{\lambda}(t,k) = e_{\lambda+1}(ly)$The weights (W) for the pre-polynomial layer are found by summing the locally integrated weights modified in the polynomial layer, which is given in equation (13),

$$W_{\lambda}(ly,t) = \sum_{k=1}^{K} W_{\lambda}(ly,t,k) \quad (13)$$

In this, the size of p is varied by summing the value into k based dimension, which can change the equation by varying the weights in the network that is given in equation (14)

$$\Delta W_{\lambda}(ly,t,k) = \eta e_{\lambda}(ly) g_{\lambda 2}(ly) g_{\lambda 1}(t,k) \quad (14)$$

In Equation (9), the parameter η represents the recognition or classification metric, while $g_{\lambda 2}$, and $g_{\lambda 1}$ denote the classified outcomes in the output layer ly. The HAP-CNN model leverages polynomial terms to enhance the network's dimensionality and improve the classification of intrusion detection data into Attack or Normal.

4. Result and Discussion

This section validates the performance and outcomes of the DOLO-ID approach security model by utilizing several evaluation parameters. The experimental findings of the research were implemented via Spyder, an Anaconda navigator executed on Windows 10 OS. The effectiveness of the DOLO-ID approach was calculated using the F1 score, accuracy specificity, recall, and precision.

4.1. Dataset Description

NSLKDD: The KDD99 dataset, created in 1999, quickly became a foundational resource for cyber security research. However, over time, researchers identified significant limitations, including high redundancy and an overwhelming number of records in both the training and validation sets. These issues create practical challenges for experimental use, as the dataset's size can hinder efficient analysis. To tackle these issues, the NSL-KDD dataset was developed in 2009 as an improved alternative. The NSL-KDD dataset lower redundancy and provides a more manageable size, making it a widely adopted standard in cyber security works.

4.2. Performance Metrics

The detection efficiency of the suggested approach is measured utilizing the performance metrics. The metrics are accuracy, f1score, precision, and recall. The parameters utilized to assess the suggested DOLO-ID approach findings are computed by utilizing the below equations:

$$Accuracy = \frac{T_p + T_N}{T_p + T_N + F_p + F_N} \quad (23)$$

$$Precision = \frac{T_p}{T_p + F_p} \quad (24)$$

$$Recall = \frac{T_p}{T_p + F_N} \quad (25)$$

$$F1Score = \frac{2 \times P_c \times R_c}{P_c + R_c} \quad (26)$$

4.3. Comparison Analysis

To validate the effectiveness of the DOLO-ID model, a comparative study was conducted against existing intrusion detection frameworks, including CNN+LSTM, EIDM, and GNN-IDS. These models were chosen due to their widespread adoption in intrusion detection and their relevance to IoT-based security frameworks. CNN+LSTM integrates convolutional and recurrent networks to capture spatial and sequential attack patterns, while EIDM employs anomaly-based multi-class classification. GNN-IDS leverages graph-based neural networks to optimize network traffic analysis. The proposed DOLO-ID approach is assessed utilizing precision, detection rate, recall, f1score, accuracy, and false alarm rate.

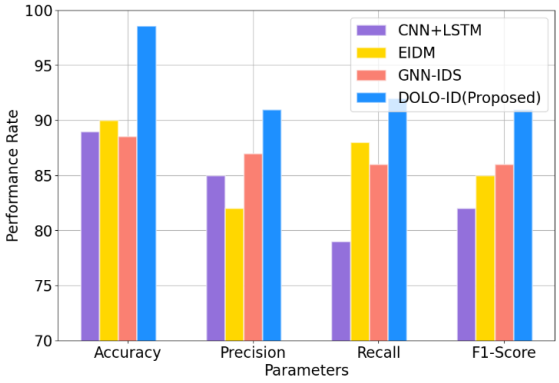

Figure 2. Performance Comparison

Figure 2 illustrates the performance of recall, accuracy, precision and f1score with the proposed and existing techniques. For each classification technique, the f1score, precision, accuracy and recall of the overall performance is evaluated using the TrP, TrN, FalP, and FalN. The f1score, recall, precision, and accuracy of the proposed DOLO-ID method are 92.8%, 91%, 92% and 98.56% which is higher than the existing techniques.

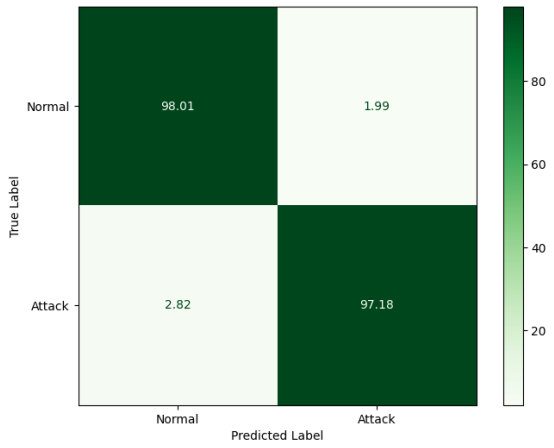

Figure 3. Confusion matrices for the NSL-KDD dataset

Figure 3 illustrates three confusion matrices for binary classification tasks across the datasets NSL-KDD, comparing predicted labels (Normal or Attack) with true labels. In suggested method accurately classifies 98.01% of normal and 97.18% of attack class.

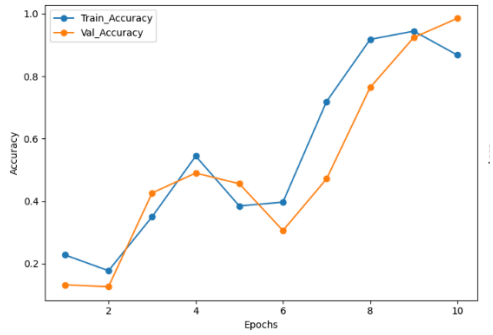

Figure 4. The accuracy curve of the suggested method

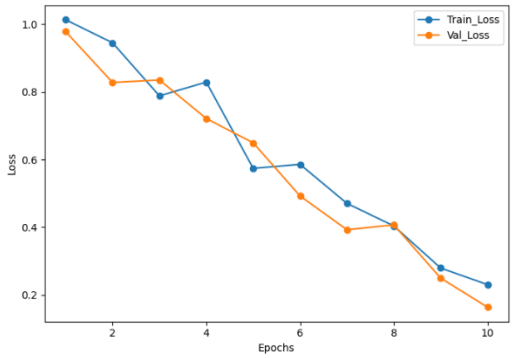

Figure 5. The loss curve of the suggested method

The suggested framework has attained an overall accuracy of 98.56% on the NSLKDD dataset. The classification of the validation and testing is illustrated through accuracy and loss plots of the suggested approach in Figures 4 and 5. These plots illustrate the model's performance highlighting its effectiveness in detecting intrusions. The low loss values also reflect successful learning with minimal overfitting during the training process.

5. CONCLUSION

In this paper, a DOLO-ID technique is proposed for classifying intrusion accurately in IoT. The use of the HAPP CNN Network further enhances the detection accuracy and minimizes false positives, effectively classifying traffic as either attack or normal. Experimental results demonstrate that DOLO-ID surpasses previous approaches regarding accuracy, computational efficiency, and scalability. The f1score, recall, precision, and accuracy of the suggested DOLO-ID method are 92.8%, 91%, 92% and 98.56% which is higher than the existing techniques. Future research could explore extending this framework to handle real-time detection and evolving attack patterns, ensuring continued relevance and effectiveness in securing IoT ecosystems. Real-time Intrusion Detection: Implementing the model in a live network environment to assess its adaptability to evolving cyber threats. Exploring additional benchmark datasets, such as CICIDS2017 and TON-IoT, to validate the generalizability of the approach. Enhancing the model with incremental learning capabilities to adapt to new attack patterns over time.

CONFLICTS OF INTEREST

This paper has no conflict of interest for publishing.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] A. Uzoka, E. Cadet, and P.U. Ojukwu, "The role of telecommunications in enabling Internet of Things (IoT) connectivity and applications," *Comprehensive Research and Reviews in Science and Technology*, vol. 2, no. 02, pp. 055-073, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] A.M. Banaamah, and I. Ahmad, "Intrusion detection in iot using deep learning," *Sensors*, vol. 22, no. 21, pp. 8417, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] M.A. Alsoufi, S. Razak, M.M. Siraj, I. Nafea, F.A. Ghaleb, F. Saeed, and M. Nasser, "Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review," *Applied sciences*, vol. 11, no. 18, pp. 8383, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] A.R. Khan, M. Kashif, R.H. Jhaveri, R. Raut, T. Saba, and S.A. Bahaj, "Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions," *Security and Communication Networks*, vol. 2022, no. 1, pp. 4016073, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, pp. 1177. 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] A.D. Jasim, "A survey of intrusion detection using deep learning in internet of things," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, pp. 83-93, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] P.L.S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T.H. Kim, "Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey," *IEEE Access*, vol. 10, pp.

121173-121192, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[8] I. Idrissi, M. Azizi, and O. Moussaoui, "IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review," In *2020 Fourth international conference on intelligent computing in data sciences (ICDS)*, pp. 1-10, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[9] M.A. Khan, M.A. Khan, S.U. Jan, J. Ahmad, S.S. Jamal, A.A. Shah, N. Pitropakis, and W.J. Buchanan, "A deep learning-based intrusion detection system for MQTT enabled IoT," *Sensors*, vol. 21, no. 21, pp. 7016, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[10] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671-2701, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[11] E.P. Nugroho, T. Djatna, I.S. Sitanggang, A. Buono, and I. Hermadi, "A review of intrusion detection system in IoT with machine learning approach: current and future research," In *2020 6th international conference on science in information technology (ICSITech)*, pp. 138-143, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[12] S. Fraihat, S. Makhadmeh, M. Awad, M.A. Al-Betar, and A. Al-Redhaei, "Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm," *Internet of Things*, vol. 22, pp. 100819, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[13] R. Balaji, S. Deepajothi, G. Prabaharan, T. Daniya, P. Karthikeyan, and S. Velliangiri, "Survey on intrusions detection system using deep learning in iot environment," In *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, pp. 195-199, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[14] P. Spadaccino, and F. Cuomo, "Intrusion Detection Systems for IoT: opportunities and challenges offered by Edge Computing and Machine Learning," *arXiv preprint arXiv:2012.01174*, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[15] R. Saadouni, C. Gherbi, Z. Aliouat, Y. Harbi, and A. Khacha, "Intrusion detection systems for IoT based on bio-inspired and machine learning techniques: a systematic review of the literature," *Cluster Computing*, pp. 1-27, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[16] H.C. Altunay, and Z. Albayrak, "A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks," *Engineering Science and Technology, an International Journal*, vol. 38, pp. 101322, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[17] P. Sanju, "Enhancing intrusion detection in IoT systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks," *Journal of Engineering Research*, vol. 11, no. 4, pp. 356-361, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[18] O. Elnakib, E. Shaaban, M. Mahmoud, and K. Emara, "EIDM: Deep learning model for IoT intrusion detection systems," *The Journal of Supercomputing*, vol. 79, no. 12, pp. 13241-13261, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[19] H. Nandanwar, and R. Katarya, "Deep learning enabled intrusion detection system for Industrial IOT environment," *Expert Systems with Applications*, vol. 249, pp. 123808, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[20] T. Altaf, X. Wang, W. Ni, G. Yu, R.P. Liu, and R. Braun, "A new concatenated Multigraph Neural Network for IoT intrusion detection," *Internet of Things*, vol. 22, pp. 100818, 2023. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Abdullah Muhammad Noman is a dedicated academic and researcher with a strong background in economics and data analysis. He completed his undergraduate studies at the prestigious Institute major in International Business Administration (IBA), and went on to earn an MPhil in International Economics and Finance from Multimedia University, Malaysia. Over the years, Abdullah has developed a specialized expertise in areas such as data analysis, econometric modelling, marketing, and data representation. Currently, Abdullah serves as a Lecturer of Economics, where he combines his passion for teaching with his commitment to advancing knowledge in his field. As a research scholar, he has been involved in several high-impact research projects, contributing to the development of innovative approaches to economic analysis and decision-making. With a keen interest in the application of econometric tools and techniques, Abdullah is focused on exploring complex economic issues through data-driven insights. His work blends academic rigor with practical application, positioning him as an influential voice in both the academic and research communities and the other authors may include biographies at the end of regular papers. In this section authors can include their studies number of publications they have and any achievements the authors have obtained. All the authors can include their photos as well as biographies, if they wish.

Sakiru Adebola Solarin is a Profossor of Economics at the Faculty of Business, Multimedia University Malaysia. He earned his Bachelor of Economics (BSc. Economics) with Honours from University of Ilorin, Nigeria; Master of Economics (MSc. Economics) from University of Lagos, Nigeria; Master of Islamic Finance and Banking from Insaniah University College (MIFB), and Doctor of Philosophy (Ph.D) in Economics from University Utara Malaysia. In terms of teaching, Dr. Solarin has been a teacher since 2009. He served as a tutor at University Utara Malaysia, while undergoing his PhD studies for the period, 2009-2012. Since 2012, he has been teaching at Multimedia University Malaysia. Since 2011, Dr. Solarin has been involved in many research areas, including Islamic Banking and Finance, Energy Economics, Tourism Economics, Defence Economics and Applied Econometrics. He has published his research works in the ISI-Web of Science (ISI-WoS), Scopus and other indexed journals such as Ecological Indicators, Renewable and Sustainable Energy Reviews, Economic Modelling, Current Issues in Tourism, Energy Policy, Energy, Quality and Quantity, Defence and Peace Economics, Natural Hazards, etc. Additionally, he is also a reviewer and editorial board member for many international and local scholarly journals.

Lye Chun Teck is attached to the Faculty of Business (FOB) at Multimedia University (MMU), Malaysia. He obtained a Bachelor Degree in Science with Education (B.Sc.Ed. Hons), majoring in Mathematics and minoring in physics, from the Universiti Malaya (UM); a Master of Science Degree (M.Sc.) majoring in Applied Statistics from Universiti Putra Malaysia (UPM); and a Doctor of Philosophy (Ph.D.) majoring in International Finance from Universiti Sains Malaysia (USM).

Arrived: 24.11.2024
Accepted: 30.12.2024