IoT Traffic Parameter Classification based on Optimized BPSO for Enabling Green Wireless Networks

Yasser Fouad
Department of Computer Science, Faculty of Computers and Information, Suez University, Suez, Egypt
yasser.ramadan@suezuni.edu.eg

Nehal E. Abdelaziz
Department of Computer Science, Faculty of Computers and Information, Suez University, Suez, Egypt
Nehal.master2020@gmail.com

Ahmed M. Elshewey
Department of Computer Science, Faculty of Computers and Information, Suez University, Suez, Egypt
ahmed.elshewey@fci.suezuni.edu.eg (corresponding author)

Received: 11 October 2024 | Revised: 27 October 2024 and 31 October 2024 | Accepted: 3 November 2024

ABSTRACT

The rapid expansion of artificial intelligence (AI) integrated with the Internet of Things (IoT) has fueled the development of various smart devices, particularly for smart city applications. However, the heterogeneity of these devices necessitates a robust communication network capable of maintaining a consistent traffic flow. This paper employs Machine Learning (ML) models to classify continuously received network parameters from diverse IoT devices, identifying necessary adjustments to enhance network performance. Key network traffic parameters, such as packet data, are transmitted through gateways via specialized tools. Six different ML techniques with default parameters were used: Decision Tree (DT), Random Forest (RF), Support Vector Machines (SVMs), K-Nearest Neighbors (KNN), Naive Bayes (NB), and Stochastic Gradient Descent Classifiers (SGDC), to classify the traffic of the environment (IoT / non IoT). The models' performance was evaluated in a real-time smart laboratory environment comprising 38 IoT devices from various vendors with the following metrics: Accuracy, F1-score, Recall and Precision. The RF model achieved the highest Accuracy of 95.6%. Also the Binary Particle Swarm Optimizer (BPSO) was used across the RF. The results demonstrated that the BPSO-RF with hyperparameter optimization enhanced the Accuracy from 95.6% to 99.4%.

Keywords-IoT; Network Traffic Classification; Machine Learning; BPSO

I. INTRODUCTION

IoT is a vast, interconnected network of smart devices, vehicles, appliances, and other gadgets equipped with sensors, software, and communications. It helps create communication channels and exchange data smoothly over the Internet. These electronic devices include typical home appliances, such as electronic thermostats and refrigerators, machines for industry, and even entire cities fitted with intelligent infrastructure. The technology for the communication market is currently experiencing a notable increase in the variety of connected smart devices. These devices are identified by their physical components that interact with sensors, enabling them to generate, exchange, and utilize data with little or no human involvement. The significance of smart devices has been growing in everyday life because of their ability to facilitate the gathering and analysis of IoT network data. This has led to the development of more intelligent environments, particularly in the domains of smart homes, buildings, traffic management, and urban areas [1]. IoT is based on the idea that the real and virtual worlds should be able to work together seamlessly, making things more efficient, easy, and automated. It is important to collect and analyze data from these interconnected devices, providing both companies and individuals with the opportunity to gain useful insights, make informed decisions, and enhance overall productivity. The IoT system model [2] is a conceptual framework that describes the structure and components of an IoT system. For example, a smart building facilitates user management, identification, and access to smart devices by means of shared data sent via various network protocols. The maintenance of confidentiality is also one of the highest priorities. IoT offers the ability of significant changes in many sectors, including medical care, logistics, agriculture, and production. It can enable remote monitoring of patients' health conditions in real-time, optimize supply chain logistics by tracking inventory levels automatically, enhance agricultural practices through precision farming techniques, and streamline production processes by leveraging predictive maintenance. The existence of different IoT protocols [3] means that there is not a single gateway for all devices, which makes it hard for a model to find different IoT device traffic in a heterogeneous network.

Recent research proposes learning-based techniques for identifying different IoT object traffic. However, along with the numerous benefits of IoT, challenges may emerge, such as data security concerns, privacy issues, interoperability between different IoT platforms or devices, and the need for robust infrastructure to support the massive influx of the data generated by these connected devices. In conclusion, IoT is a rapidly growing field that holds immense potential for transforming various aspects of people's lives [4]. With its ability to connect physical objects to the digital world through sensors and connectivity, IoT is set to revolutionize industries by enabling smarter decision-making processes and improving overall efficiency. Authors in [5] tested the feasibility of identifying IoT device types through the utilization of Nmap, a network scanning tool that involves probing open ports. A comprehensive analysis was conducted on a total of 19 IoT devices to establish a repository of port number combinations and corresponding signatures. Authors in [6] developed a unique framework called Stacked-Ensemble for the purpose of classifying IoT traffic. This framework utilizes IoT devices' features to describe incoming data and has the capability to effectively manage network traffic in real-time with a high Accuracy of 99.80%. However, it has some issues with normal traffic through different ports that cannot be detected. In [7], an IoT sentinel system was proposed that aims to detect and control communication among the IoT-entailed devices within the network. The system employs an RF classification model for identifying different objects. The devices are considered identical if they possess identical models and software versions. Upon the introduction of a novel device, it initiates its installation and configuration phases, thus mitigating the risk of potential compromise to the entire network. Such a solution reduces potential security breaches for the entirety of the network with an Accuracy of 96.6%. In [8], an IoT Sense system was introduced as a technological tool designed to discern and classify IoT objects, such as the frame, the packet, and the segment headers, by examining their network behavior. Each node was assigned an activity profile to detect any anomalies resulting from malicious activities, achieving an Accuracy of 95.6%.

A more comparable strategy was proposed in [9], namely a methodology for identifying IoT devices utilizing several ML algorithms, such as RF, DT, SVM, k-Nearest Neighbor (KNN), Neural Networks, and NB techniques, which obtained an overall Accuracy as high as 98.8%. Authors in [10] employed a framework which includes seven supervised ML algorithms, linear discriminant analysis, KNN, RFs, Multilayer Perceptron, Ada Boosting, DT, and Extreme Gradient Boosting, to classify IoT devices based on network traffic in a smart home according to their type of application. This framework reached a cumulative Accuracy of 96.5%. In [11], IoT device classes were identified based on traffic flow characteristics, including source Internet Protocol (IP) address, Media Access Control (MAC) address, destination IP address, source port number, and destination port number, attaining a cumulative Accuracy of 97.5%. Finally, RFs were utilized for traffic classification and device identification, incorporating essential features, like packet size, interarrival time, duration, priority, and pushing labels [12].

In the current study, ML techniques were deployed as predictive and classifier models. The employed algorithms were trained on a labeled dataset, consisting of different types of IoT traffic parameters. The proposed model has the capability to dynamically adopt the classification power, based on network real-time feedback, as a response to the growing features of IoT network traffic. The efficacy of the proposed model was assessed on the basis of empirical studies carried out using real datasets. The findings indicate that the ML-based classification strategy exhibits superior performance compared to conventional rule-based methods in terms of both Accuracy and efficiency when identifying traffic originated from normal end devices.

II. MATERIALS AND METHODS

A smart building utilizes technology to optimize performance by sharing information between different systems, automating processes, like heating, ventilation, and air conditioning. It monitors energy consumption and controls it through connectivity, involving connected objects and applications. The concept extends to living comfort, health, and safety, among other benefits. Smart buildings are interconnected systems, including smart objects like fire alarms, lighting, and cameras. In this paper, a smart IoT environment is used, which comprises multiple gadgets varied in nature, such as cameras, temperature sensors, IP telephones, and mobile phones that are interconnected via the internet. The proposed model focuses on characterizing the IoT traffic by collecting network traffic from various devices over multiple times, including autonomous and user-interacted traffic. The experiment employed 38 devices varied in type, software applications, and flow settings, as seen in Table I.

TABLE I. IOT DEVICES EMPLOYED IN THE EXPERIMENTAL SETTINGS.

IoT Node	Count	Flows generated
Printer	2	37156
PC	12	37900
Laptop	12	38800
Ip phone	5	33500
Tablet	2	33000
Temperature Sensor	1	32500
IP CAM	2	30500
Mobile	2	30900

These devices are connected using heterogeneous communication, namely wireless and wired. The gathered data from such networks, such as packets, frames and segments, as well as real traffic, are analyzed by ML techniques to identify objects that originate traffic. The model monitors network traffic to build the dataset employing Wireshark to perform a network traffic scan. It then creates a database, which entails information on IP addresses, MAC addresses, port numbers, and packet sizes. Data were gathered from a total of 38 objects, each belonging to one of 7 distinct types of devices. This information was then documented as packets and stored in PCAP files. The gathered data were converted into protocol sessions that are distinguished by a distinct triplet consisting of the source address, destination address, and protocol type.

A. Data Acquisition

In the current study, the employed dataset comprises actual network trace traffic records for the 38 IoT devices, acting as a network of D devices producing M traffic flows. The set T consists of traffic flows generated by different devices. Each traffic flow consists of a specific number of packets represented by P. On packet level, every record contains features, such as the interarrival time, source IP address, destination IP address, transport protocol of every packet flow, source port, destination port, Time to-Live (TTL) value, window size of the transport layer length of a packet, source Ethernet address, and destination Ethernet address.

1) Description of Features

- Device Level: This feature focuses on extracting the source and destination MAC addresses of the devices. Most of the features are directly obtained from the traffic traces. These attributes provide a distinct description of the IoT traffic that is not influenced by other features.
- Traffic flow level: This encompasses characteristics including source and destination IP addresses, protocol type, source, and destination port numbers, TTL information, and window size of a flow. This set can extract the packet-level properties of a specified flow.
- Packet level: This feature comprises the timestamp, interarrival time, and packet length. The interarrival time is the duration between the reception of one packet and the arrival of the next one. Its characteristics are studied by examining and extracting the time between successive incoming traffic packets, which follow a Gaussian distribution with an average rate of 1 packet per time unit.

Table II depicts the dataset features and their description.

TABLE II. DATASET FEATURES DESCRIPTION

No.	Features	Description
1	Interarrival time	Average time between two packets flow on the network.
2	Length	Packet length
3	Src.IP	Source IP address
4	Dst.IP	Destination IP address
5	Protocol	Traffic flow protocol
6	Src.Port	Client port
7	Dst.Port	Server port
8	TTL	Hops remains to destination
9	Window Size	Size of bytes that device can receive
10	Src. MAC	MAC address of source.
11	Dst. MAC	MAC address of destination.

B. Data Pre-Processing

Basic filtering of the dataset is conducted during data preprocessing to eliminate non-meaningful packets like ping and Domain Name System (DNS) requests. The TTL, window size, and packet length features are already in numerical format, but the interarrival time feature has been translated to seconds. It was noticed that certain features, such the 'set of port numbers', the 'set of IP addresses', and the 'set of MAC addresses', are nominal and multi-valued, meaning they have more than one value within a single data instance. In that case, the characteristics were translated into a numerical form using a two-step technique, since ML classifiers cannot handle such data. Data cleaning was performed first, through the utilization of nominal vectors in the Bag-of-Word (BoW) model. The BoW method treated all vector words equally. Thus, a relevance weighting system was suggested to give each word in the vector a prioritized level of importance. The missing values of features were filled by utilizing their mean value, and then the dataset was normalized between 0 and 1 deploying the MinMaxScaler method.

C. Feature Selection

The metaheuristic optimization BPSO method may identify appropriate characteristics for IoT traffic categorization. Every swarm particle might be a feature group. A particle's location is stored as a binary vector for 1 s for selected features and 0 s for rejected features. Fitness functions assess particle feature subset quality. This function usually employs a classification statistic, like Accuracy, Precision, or Recall, from the training data and specified characteristics. Particles travel around the search space depending on their position, velocity, and the best local and global positions. The particle's memory and the swarm's knowledge update the velocity, which controls mobility. It iterates for a certain number of generations. Particle placements and fitness values change with each repetition. Finally, the ideal feature subset particle with the highest fitness value is found. Figure 1 shows the BPSO optimizer technique.

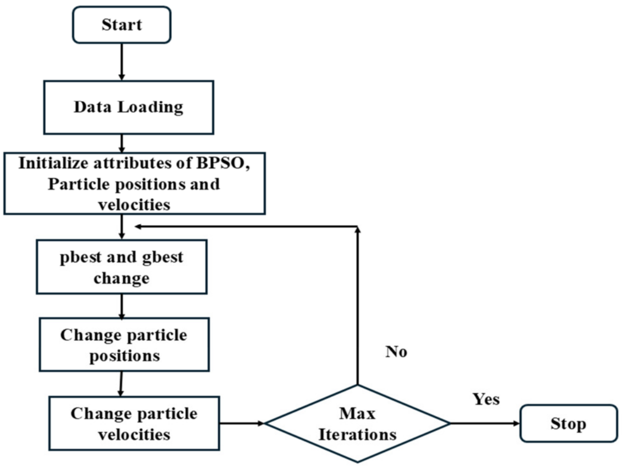
Start
Data Loading
Initialize attributes of BPSO, Particle positions and velocities
pbest and gbest change
Change particle positions
Change particle velocities
Max Iterations
No
Yes
Stop

Fig. 1. BPSO mechanism.

D. Proposed Model

The proposed model is designed to find the IoT objects in its surroundings. There are 8 steps followed to implement the optimized model (Figure 2):

- Dataset (packet) capturing.
- Translation of the characteristics into a numerical form using a two-step technique, such as 'set of port numbers ', 'set of IP addresses ', and 'set of MAC addresses '.
- Data cleaning through the utilization of nominal vectors in the BoW model.
- Filling in the missing feature values by utilizing their mean value and then normalizing the dataset between 0 and 1 using the MinMaxScaler method.
- Utilizing the BPSO for feature selection.
- Data partition, training, and testing sets.
- Using DT, RF, SVMs, NN, NB, and SGDC models.
- Evaluating the performance of the models.

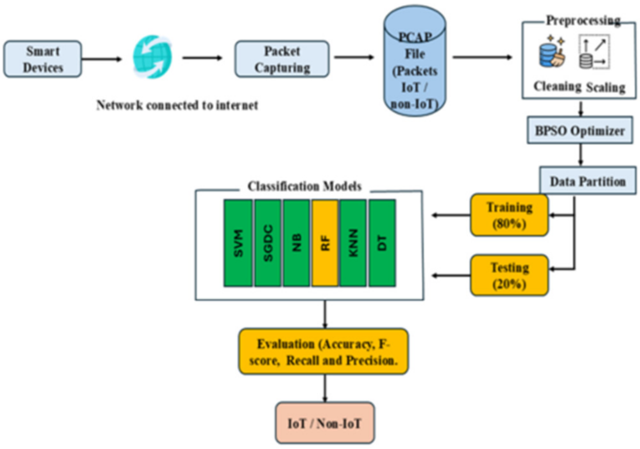

Fig. 2. The steps of the proposed model.

III. RESULTS AND DISCUSSION

The experiments were carried out utilizing Jupyter Notebook version 6.4.6, which is a Python-based software program designed for data analysis and visualization. The studies were carried out using a computer running Microsoft Windows 10, equipped with an Intel Core i7 central processing unit and 16 GB RAM. Accuracy, Recall, Precision, and F1-score, were employed to validate the model:

$$\text{Accuracy} = \frac{TPos + TNeg}{TPos + FPos + FNeg + TNeg} \quad (1)$$

$$\text{Precision} = \frac{TPos}{TPos + FPos} \quad (2)$$

$$\text{Recall} = \frac{TPos}{TPos + FNeg} \quad (3)$$

$$\text{F1-score} = \frac{2 \cdot \text{Recall} \cdot \text{Precision}}{\text{Recall+Precision}} \quad (4)$$

where *TPos*, *TNeg*, *FPos*, and *FNeg* represent true positives, true negatives, false positives, and false negatives, respectively.

The Scikit-learn library was used to extract features from the PCAP files and subsequently convert them into a dataset [13, 14]. The model was subsequently constructed employing ML techniques in order to forecast and discern the types of IoT objects. Six Scikit-learn-based classification algorithms were used in this study to figure out the types of IoT traffic: RF, SVM, KNN, SGDC, DT, and NB. The employed methodology is founded upon the principles of multiclass supervised learning. Specifically, it treats the task of identifying IoT items as a classification challenge. The dataset consists of a compilation of numerical numbers that are linked to specific attributes and observations. The performance evaluation findings of the considered ML models, are presented in Table III.

TABLE III. ML-MODELS RESULTS

Models	Accuracy	F1-score	Recall	Precision
RF	99.9	99.8	99.4	98.9
KNN	95.5	95.3	95.2	94.8
NB	91.4	91.2	91	91.2
SGDC	78.4	78	77.5	78.2
DT	99	99.6	98.7	98.8
SVM	88.6	88.3	88.5	88.3

The results demonstrate that the RF and DT models worked best on the test dataset. The RF achieved an Accuracy of 99.9%, F1-score of 99.8%, a Recall of 99.4%, and Precision of 98.9%. The DT model achieved commendable performance, securing the second position in terms of its high metric scores. The KNN model was ranked third regarding its performance metrics, the NB model was ranked fourth, and the SVM model ranked fifth. The SGDC model yielded the least favorable outcomes. The results can be seen in Figure 3.

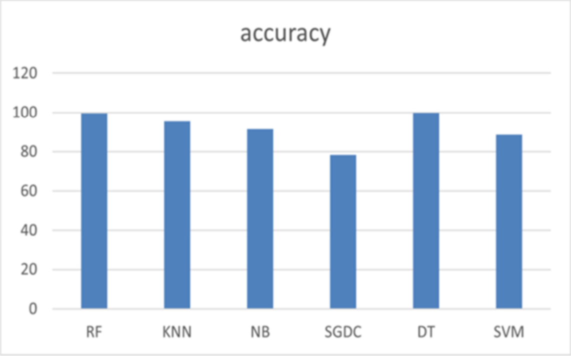

Fig. 3. Model evaluations – accuracy.

The dataset, which consisted of 600,900 entries, was partitioned into training and test sets. The performance of these sets was assessed using Scikit-learn metrics. To establish the reliability of the research, a comparison between the performance of BPSO-RF and that of other algorithms was conducted (Table IV). The comparative study constructed and analyzed numerous optimization techniques, including Genetic Algorithm (GA), Simulated Annealing (SA), and Differential Evolution (DE) (Table V).

TABLE IV. PERFORMANCE OF BPSO AGAINST OTHER ALGORITHMS.

Model	Accuracy
BPSO-RF	96.5%
GA	90.5%
SA	89.6%
DE	90.4%

TABLE V. COMPARATIVE ANALYSIS WITH OTHER WORKS.

Ref.	Dataset	Outcome
Proposed	38 devices, traffic flow with 11 attributes.	RF and KNN achieved high Accuracy 99.9 and 99%, respectively
[15]	47 attributes and 2102 features.	Accuracy using PSO equal to 96%
[16]	Multiple real IoT traffic records.	Accuracy can reach 98% with the proposed approach (LS2-BHBA)
[17]	8 malware datasets.	NRO_SVM achieved Accuracy rate of 97.8%

IV. CONCLUSION AND FUTURE WORK

The goal of this study was to identify Internet of Things (IoT) objects by analyzing network traffic data using the Wireshark tool. The data were collected and analyzed manually to extract network flow characteristics, allowing the development of exploitable properties through learning algorithms and deploying intelligent infrastructure to simulate the environment for real-world data collection.

As α first step, Machine Learning (ML) models that could sort and name the connected IoT devices in the operational environments were created. The constructed dataset was subjected to six distinct classification techniques, namely Decision Tree (DT), Random Forest (RF), Support Vector Machines (SVMs), K-Nearest Neighbors (KNN), Naive Bayes (NB), and Stochastic Gradient Descent Classifiers (SGDC). The results of the measurements demonstrate that both the DT and RF models showed outstanding efficacy, with RF attaining an impressive Accuracy of 99.9% when BPSO was used for feature selection. Findings indicated that the DT and RF models exhibited greater Accuracy in classifying and detecting services within the network traffic of various IoT devices, in the vast majority of instances.

The smart environment has emerged as a vulnerable entity susceptible to cyber-attacks, thereby compromising the privacy and security of its users [18-23]. The existing methodology employed within the operational context in the current study demonstrates efficacy in the identification and detection of intelligent entities. However, it is imperative to acknowledge that this technique is deficient in terms of ensuring robust security, mostly attributable to the elevated cyber-security vulnerabilities prevalent in IoT networks. Henceforth, forthcoming endeavors will prioritize the examination of IoT security in order to discern and address security concerns arising from IoT devices [24-28].

REFERENCES

[1] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of Things: A General Overview between Architectures, Protocols and Applications," *Information*, vol. 12, no. 2, Feb. 2021, Art. no. 87, https://doi.org/10.3390/info12020087.

[2] L. Elhaloui, S. Elfilali, M. Tabaa, and E. H. Benlahmer, "Toward a Monitoring System Based on IoT Devices for Smart Buildings," in *Advances on Smart and Soft Computing*, Singapore, 2021, pp. 285–293, https://doi.org/10.1007/978-981-15-6048-4_25.

[3] F. Aljuaydi, B. Behera, A. Elshewey, and Z. Tarek, "A Deep Learning Prediction Model to Predict Sustainable Development in Saudi Arabia," *Applied Mathematics & Information Sciences*, vol. 18, pp. 1345–1366, Sep. 2024, https://doi.org/10.18576/amis/180615.

[4] S. Naik and V. Maral, "Cyber security — IoT," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Feb. 2017, pp. 764–767, https://doi.org/10.1109/RTEICT.2017.8256700.

[5] A. Sivanathan, H. H. Gharakheili, and V. Sivaraman, "Can We Classify an IoT Device using TCP Port Scan?," in *2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS)*, Sep. 2018, pp. 1–4, https://doi.org/10.1109/ICIAFS.2018.8913346.

[6] M. Snehi and A. Bhandari, "A Novel Distributed Stack Ensembled Meta-Learning-Based Optimized Classification Framework for Real-time Prolific IoT Traffic Streams," *Arabian Journal for Science and Engineering*, vol. 47, no. 8, pp. 9907–9930, Aug. 2022, https://doi.org/10.1007/s13369-021-06472-z.

[7] A. M. Elshewey, A. A. Alhussan, D. S. Khafaga, E. S. M. Elkenawy, and Z. Tarek, "EEG-based optimization of eye state classification using modified-BER metaheuristic algorithm," *Scientific Reports*, vol. 14, no. 1, Oct. 2024, Art. no. 24489, https://doi.org/10.1038/s41598-024-74475-5.

[8] B. Bezawada, M. Bachani, J. Peterson, H. Shirazi, I. Ray, and I. Ray, "Behavioral Fingerprinting of IoT Devices," in *Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security*, New York, NY, USA, Jan. 2018, pp. 41–50, https://doi.org/10.1145/3266444.3266452.

[9] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, "Network Traffic Classifier With Convolutional and Recurrent Neural Networks for Internet of Things," *IEEE Access*, vol. 5, pp. 18042–18050, 2017, https://doi.org/10.1109/ACCESS.2017.2747560.

[10] I. Cvitić, D. Peraković, M. Periša, and M. D. Stojanović, "Novel Classification of IoT Devices Based on Traffic Flow Features," *Journal of Organizational and End User Computing (JOEUC)*, vol. 33, no. 6, pp. 1–20, 2021, https://doi.org/10.4018/JOEUC.20211101.oa12.

[11] E. S. M. Elkenawy, A. A. Alhussan, D. S. Khafaga, Z. Tarek, and A. M. Elshewey, "Greylag goose optimization and multilayer perceptron for enhancing lung cancer classification," *Scientific Reports*, vol. 14, no. 1, Oct. 2024, Art. no. 23784, https://doi.org/10.1038/s41598-024-72013-x.

[12] M. Aria, C. Cuccurullo, and A. Gnasso, "A comparison among interpretative proposals for Random Forests," *Machine Learning with Applications*, vol. 6, Dec. 2021, Art. no. 100094, https://doi.org/10.1016/j.mlwa.2021.100094.

[13] Y. Fouad, A. M. Osman, S. A. Z. Hassan, H. M. El-Bakry, and A. M. Elshewey, "Adaptive Visual Sentiment Prediction Model Based on Event Concepts and Object Detection Techniques in Social Media," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 14, no. 7, 2023, https://doi.org/10.14569/IJACSA.2023.0140728.

[14] A. M. Elshewey *et al.*, "Optimizing HCV Disease Prediction in Egypt: The hyOPTGB Framework," *Diagnostics*, vol. 13, no. 22, Jan. 2023, Art. no. 3439, https://doi.org/10.3390/diagnostics13223439.

[15] S. T. Mrudula *et al.*, "Internet of things and optimized knn based intelligent transportation system for traffic flow prediction in smart

cities," *Measurement: Sensors*, vol. 35, Oct. 2024, Art. no. 101297, https://doi.org/10.1016/j.measen.2024.101297.

[16] B. Wang, H. Kang, G. Sun, and J. Li, "Efficient traffic-based IoT device identification using a feature selection approach with Lévy flight-based sine chaotic sub-swarm binary honey badger algorithm," *Applied Soft Computing*, vol. 155, Apr. 2024, Art. no. 111455, https://doi.org/10.1016/j.asoc.2024.111455.

[17] I. Ahmad, Z. Wan, A. Ahmad, and S. S. Ullah, "A Hybrid Optimization Model for Efficient Detection and Classification of Malware in the Internet of Things," *Mathematics*, vol. 12, no. 10, Jan. 2024, Art. no. 1437, https://doi.org/10.3390/math12101437.

[18] Z. Tarek *et al.*, "An Optimized Model Based on Deep Learning and Gated Recurrent Unit for COVID-19 Death Prediction," *Biomimetics*, vol. 8, no. 7, Nov. 2023, Art. no. 552, https://doi.org/10.3390/biomimetics8070552.

[19] E. H. Alkhammash *et al.*, "Application of Machine Learning to Predict COVID-19 Spread via an Optimized BPSO Model," *Biomimetics*, vol. 8, no. 6, Oct. 2023, Art. no. 457, https://doi.org/10.3390/biomimetics8060457.

[20] M. Y. Shams, E. S. M. El-kenawy, A. Ibrahim, and A. M. Elshewey, "A hybrid dipper throated optimization algorithm and particle swarm optimization (DTPSO) model for hepatocellular carcinoma (HCC) prediction," *Biomedical Signal Processing and Control*, vol. 85, Aug. 2023, Art. no. 104908, https://doi.org/10.1016/j.bspc.2023.104908.

[21] A. M. Elshewey, M. Y. Shams, N. El-Rashidy, A. M. Elhady, S. M. Shohieb, and Z. Tarek, "Bayesian Optimization with Support Vector Machine Model for Parkinson Disease Classification," *Sensors*, vol. 23, no. 4, Jan. 2023, Art. no. 2085, https://doi.org/10.3390/s23042085.

[22] A. M. Elshewey and A. M. Osman, "Orthopedic disease classification based on breadth-first search algorithm," *Scientific Reports*, vol. 14, no. 1, Oct. 2024, Art. no. 23368, https://doi.org/10.1038/s41598-024-73559-6.

[23] M. Y. Shams, A. M. Elshewey, E. S. M. El-kenawy, A. Ibrahim, F. M. Talaat, and Z. Tarek, "Water quality prediction using machine learning models based on grid search method," *Multimed Tools Appl*, vol. 83, no. 12, pp. 35307–35334, Apr. 2024, doi: 10.1007/s11042-023-16737-4.

[24] M. Eed, A. A. Alhussan, A. S. T. Qenawy, A. M. Osman, A. M. Elshewey, and R. Arnous, "Potato Consumption Forecasting Based on a Hybrid Stacked Deep Learning Model," *Potato Research*, Jul. 2024, https://doi.org/10.1007/s11540-024-09764-7.

[25] A. A. Abdelhamid, A. A. Alhussan, A. S. T. Qenawy, A. M. Osman, A. M. Elshewey, and M. Eed, "Potato Harvesting Prediction Using an Improved ResNet-59 Model," *Potato Research*, Aug. 2024, https://doi.org/10.1007/s11540-024-09773-6.

[26] S. A. Alzakari, A. A. Alhussan, A. S. T. Qenawy, and A. M. Elshewey, "Early Detection of Potato Disease Using an Enhanced Convolutional Neural Network-Long Short-Term Memory Deep Learning Model," *Potato Research*, Jul. 2024, https://doi.org/10.1007/s11540-024-09760-x.

[27] S. A. Alzakari, A. A. Alhussan, A.-S. T. Qenawy, A. M. Elshewey, and M. Eed, "An Enhanced Long Short-Term Memory Recurrent Neural Network Deep Learning Model for Potato Price Prediction," *Potato Research*, Jun. 2024, https://doi.org/10.1007/s11540-024-09744-x.

[28] B. Mopuru and Y. Pachipala, "Advancing IoT Security: Integrative Machine Learning Models for Enhanced Intrusion Detection in Wireless Sensor Networks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14840–14847, Aug. 2024, https://doi.org/10.48084/etasr.7641.