Sensors & Transducers, Vol. 263, Issue 4, December 2023, pp. 82-88

www.sensorsportal.com

Sensors & Transducers

Published by IFSA Publishing, S. L., 2023
http://www.sensorsportal.com

Intrusion Detection in IoT-based Cyber-physical System Using Machine Learning

[1, 2, *] Stephen Afrifa, [3, 4, 5, *] Vijayakumar Varadarajan, [2] Peter Appiahene and [1] Tao Zhang

[1] Department of Information and Communication Engineering, Tianjin University, Tianjin 300072, China
[2] Department of Information Technology and Decision Sciences, University of Energy and Natural Resources, Sunyani 00233, Ghana
[3] School of Computer Science and Engineering, University of New South Wales, Sydney, NSW 2052, Australia
[4] International Divisions, Ajeenkya D. Y. Patil University, Pune 412105, India
[5] School of Information Technology, Swiss School of Business Management, 1213 Geneva, Switzerland
E-mail: afrifastephen@tju.edu.cn, vijayakumar.varadarajan@gmail.com

Received: 19 October 2023 / Accepted: 14 December 2023 / Published: 21 December 2023

Abstract: The use of Internet of Things (IoT) devices is a result of the massive number of messages carried through the internet. One of the most serious IoT threats is the botnet attack, which aims to commit legitimate, profitable, and effective cybercrimes. Because of the ramifications of hostile acts in computing, communication, and cyber-physical systems (CPS), researchers are encouraged to develop effective Intrusion Detection Systems (IDSs). Intelligent-powered intrusion detection solutions ideal for deployment in IoT-based cyber-physical settings are created using cutting-edge learning algorithms. In this study, three machine learning (ML) approaches are employed to develop a system that recognizes legal or malicious communication in linked computer networks. The results showed that random forest (RF) fared the best, with a coefficient of determination (R^2) of 0.9965 and error scores of 0.0015 for root mean square error (RMSE), 0.0522 for mean absolute error (MAE), and 0.0872 for mean absolute percentage error (MAPE). Despite the models achieved significant results, it was suggested that RF be used when detecting legal or malicious networks in IoT-connected computer networks. This study is crucial for making informed decisions that will lead to long-term growth in industrial and educational networks.

Keywords: Machine learning, IoT, CPS, Intrusion detection, Botnet detection, Network traffic.

1. Introduction

Cyber Physical Systems (CPS) are a symbiotic combination of computing, networking, and physical processes. CPS simulates several systems, including intelligent critical infrastructures [1]. Indeed, the widespread incorporation of CPS into critical infrastructures has expanded their importance in ensuring economic progress, and as a result, their security and resilience have become critical in many facets of modern life. Researchers and developers established a way to achieve Industry 4.0 goals by merging machine learning (ML) technologies with industrial processes that contain intelligence [2]. The

Internet of Things (IoT) is a network of millions of physical items that connect to the Internet and perform activities automatically with little human interaction [3]. The next part of information security that we will look at is the use of automated reasoning. They have demonstrated their devotion since artificial intelligence guesses such as machine learning and deep learning offer significant potential to provide services to the IoT with their security challenges and criticality while handling heterogeneous information.

The IoT technologies and their integration with CPS enable better monitoring, control, and administration of these systems [4]. However, due to the nature of integrated IoT devices, such systems are becoming increasingly prone to component failures as well as security breaches [5], because the underlying communication protocols used may introduce new vulnerabilities into the system. To secure network resources in a conventional cyber physical system, firewalls and intrusion detection systems (IDSs) are installed as layers [6], with the firewall serving as the first layer of infrastructure and the IDS serving as the second layer of defense. An intrusion detection system (IDS) examines, manages, analyzes, and reports on any unusual events in the system and network activity [7].

Criminals may consider blacking out a business by assaulting it through a connected power meter situated within the business. They may even carry out larger attacks, such as forcing a power plant to shut down via its computer system, resulting in a total blackout. Some assaults use linked gadgets to gain access to bigger networks, such as the Internet. A connected object added to a secure infrastructure can create a new attack surface. The linked object can act as a relay for a large-scale attack. There are a lot of security breaches that have been witnessed since computing devices are interconnected for information sharing, and the Internet of things is amongst them. The first Mirai attack was encountered on Sep 2016 on the Brain Krebs website (A well-known security blogger) [8]. The second Mirai attack was encountered on Oct 2016 on Dyn (a DNS service provider) [9]. This DDoS attack made the internet service not available for its customers for several hours. All of these reports indicate that botnet attacks are a significant source of assault in IoT devices. Strategies for early detection are critical. Because new types of botnet attacks emerge every day, using a deep learning or machine learning technique to detect the botnet is critical. Deep learning and machine learning methods are critical for detecting zero-day botnet assaults. There are two methods for detecting IoT botnets. There are two types of hosts: host-based and network-based. Host-based detection on devices can be implemented by analyzing system logs and monitoring system calls. Implementing host-based security solutions on IoT devices is difficult due to their small size and limited resources.

Network-based detection can be implemented by analyzing network flow statistics, which include details such as source and destination IP addresses, port numbers, protocols used, session duration, amount of data exchanged, number of packets sent, number of bytes sent, connection type, and so on. Because bots' initial sessions are brief while attempting to establish a connection, network flow-based botnet detection can be effective. The sessions will be lengthy after the link is established.

By examining channel characteristics in a computer networked system using distinct machine learning models, this study examines how to discern component failures (which affect typical network behavior) from network assaults.

The following are the primary contributions of this study, as adopted from [10, 11]:

1. This study presents an overall machine learning (ML) framework that makes use of data collected from computer networked Internet of Things (IoT) devices;
2. To evaluate the proposed framework for a number of different classification methods, the study employs both a simulation framework and a real-time testbed;
3. To assess the performance of the ML classifiers used in this study, four conventional performance evaluation criteria are used.
4. This study provides cutting-edge contemporary performance evaluation criteria for assessing the performance of machine learning algorithms.

The remainder of the article is organized as follows. Section 2 undertook a thorough examination of recent works in the literature arena. The methods used is described in Section 3. Section 4 explains the outcome and results of the proposed detection method, and Section 5 concludes and provides further study.

2. Related Works

A lot of researchers have conducted experiments to evaluate the resilience of CPS systems in IoT devices using ML models. To begin with, Khan et al. [12] proposed an innovative and safe architecture with a standardized process hierarchy/lifecycle for dispersed small and medium sized enterprises (SMEs) based on collaborative blockchain, internet of things (IoT), and artificial intelligence (AI) with machine learning (ML) techniques. They designed "BSMEs," a blockchain with an IoT enabled permissionless network topology that gives solutions to cross chain platforms. The B-SMEs handle the registration of participating SMEs, day-to-day information administration and exchange between nodes, and analysis of partnership exchange related transaction data before they are recorded on the blockchain immutable storage. In the IoT, Al-Wesabi et al. [13] developed a Pelican Optimization Algorithm with Federated Learning Driven Attack Detection and Classification (POAFL-DDC). For IoT threat detection, the POAFL-DDC approach used decentralized on-device data. Another study by [14] proposed a technique for identifying network anomalies in IoT devices in order to improve device security. The IoT Botnet dataset

was used in the study, and K-fold cross-validation tests were used to validate the values of assessment metrics.

Last but not least, Alghamdi and Bellaiche [15] provided a multi-pronged classification strategy for a deep ensemble-based intrusion detection system (IDS) employing Lambda architecture. To distinguish between malicious and benign traffic, binary classification used Long Short Term Memory (LSTM), whereas multi-class classification employs an ensemble of LSTM, Convolutional Neural Network, and Artificial Neural Network classifiers to detect the kind of attack.

3. Materials and Methods

This section presents the experimental procedure and the dataset utilized to train the machine learning classifiers. Additionally, this section presents the various evaluation metrics that were employed to evaluate the machine learning models.

3.1. Data Collection

It is difficult to find an adequately tagged dataset for botnet identification. This study is based on a publicly available dataset from the FigShare data repository, which may be downloaded at https://doi.org/10.6084/m9.figshare.21769658.v1 (accessed on July 1, 2023). The dataset has already been labeled and is being analyzed for botnet identification. The data provided are used as a standard in the present study.

3.2. Data Preprocessing

The dataset was preprocessed in order to transform raw data into useful information for machine learning algorithms to grasp [16]. It is claimed that the data is generally incomplete and rife with inaccuracies [17]. Handling null or missing values, label encoding, and feature selection are all processes in the preprocessing stage.

3.3. The Data Division

The data was separated into training (70 %) and testing (30 %) sets. These are hyperparameters whose values govern the learning process and determine the model parameters that a learning algorithm learns [18]. The testing dataset aids in evaluating the models' performance.

3.4. The Machine Learning Classifiers

This study makes use of three conventional machine learning classifiers: RF, SVM, and NB. To create predictions or classifications, RF employs an ensemble of many decision trees. The random forest technique produces a more accurate result by mixing the outputs of various trees [19]. The SVM algorithm's purpose is to find the optimum line or decision boundary for categorizing n-dimensional space so that we may simply place fresh data points in the proper category in the future. A hyperplane is the optimal choice boundary [20]. Additionally, NB is a probabilistic classifier, which means it predicts based on an object's likelihood [21]. The developed algorithms can determine whether a network is real or botnet traffic to assist enterprises, government, and organizations in making educated judgments.

3.5. Performance Evaluation Measures

In the current study, the root mean squared error (RMSE), mean absolute error (MAE), mean absolute percentage error (MAPE), and coefficient of determination (R^2) were employed to assess the performance of the machine learning models. The greater the R^2, as it approaches 1, the better the accuracies and the lower the error scores, and hence the better the model performance. Equations 1, 2, 3, and 4 denote the RMSE, MAE, MAPE, and R^2, respectively.

$$RMSE = \sqrt{\sum_{i=1}^{n} \frac{\left(y_{observed} - \hat{y}_{predicted}\right)^2}{n}}, \quad (1)$$

$$MAE = \frac{1}{n} \sum_{i=1}^{n} \left| y_{observed} - \hat{y}_{predicted} \right|, \quad (2)$$

$$MMAPE = \frac{100\,\%}{n} \sum_{k=1}^{n} \left| \frac{y_{observed} - \hat{y}_{predicted}}{y_{observed}} \right|, \quad (3)$$

$$R^2 = \left(\frac{\sum_{i=1}^{n} (y_{observed} - y_{average})(\hat{y}_{predicted} - \hat{y}_{average})}{\sqrt{\sum_{i=1}^{n} (y_{observed} - y_{average})^2 \sum_{i=1}^{n} (\hat{y}_{predicted} - \hat{y}_{average})^2}} \right)^2, \quad (4)$$

where $y_{observed}$ represents the observed values, $\hat{y}_{predicted}$ is the predicted values, n is the number of samples, $y_{average}$ and $\hat{y}_{average}$ represent the average observed and predicted values, respectively.

3.6. The Proposed Architecture

The planned architecture for the study is depicted in Fig. 1. To train the dataset, the proposed machine learning models, which included the random forest (RF), support vector machine (SVM), and naive bayes models, were employed. The results reflect either genuine or botnet traffic. This results in a system driven by artificial intelligence (AI) that can detect it in real-time behavioral analysis, block it, and put an end to any botnet activity.

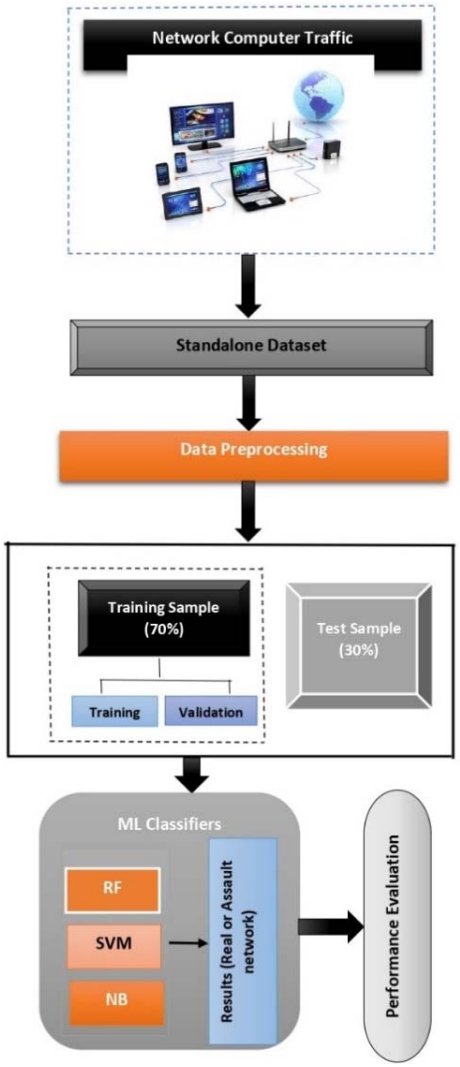

Fig. 1. The proposed architecture of the study.

4. Experimental Results and Discussion

This section presents the results gained from the ML algorithms employed for the present study.

4.1. Experimental Setup and Requirements

The proposed methodology was implemented using the Google Colab platform with Python software on a personal computer. Python is a high-level, general-purpose programming language that is free source. Because of its code readability philosophy, efficient code, easy communication features, and ease of learning, it has been the favored programming language for the majority of data scientists. Python has a vibrant scientific library as well as a number of wonderful environments, including Spyder and Jupyter Notebook. Python Matplotlib is a robust 2D graphic package that helps machine learning researchers plot graphs. We chose Python languages for our machine learning experiment because of these benefits. Furthermore, Scikit-Learn, a public and open-source ML library for Python. It is a rapid and simple data mining and analysis tool. Scikit-learn includes supervised and unsupervised learning algorithm implementations. In addition to classification, regression, and clustering techniques, this package offers features for model selection, dimensionality reduction, and data pre-processing. SciPy, which stands for Scientific Python, is a technical computation package that is built on NumPy. Because it is an open-source library, we can freely utilize it. SciPy includes modules for optimization, linear algebra, integration, interpolation, and special functions. Matplotlib, a Python charting package, and NumPy, its numerical math extension. It provides an object-oriented API for embedding charts in programs that use general-purpose GUI toolkits.

The computer contains 32 Gb of RAM and two multicore CPUs, each with 12 cores and 2.3 gigaflops of processing power. The botnet dataset samples were trained and tested in three ways. To begin, the complete sample is divided into 70 % training and 30 % testing instances.

Finally, 10-fold cross-validation was utilized to assess the performance of the proposed model. The classification R^2, RMSE, MAE, and MAPE are used to assess performance. Finally, the proposed model is compared to current state-of-the-art IoT-based botnet detection techniques.

4.2. Performance of the ML Algorithms

Digitization has altered the way we live and conduct our daily routines. Pervasive computing in IoT health devices has changed the medical treatment landscape. The availability of the internet on little devices is establishing a regime. These tiny gadgets are limited in resources and lack adequate security procedures. The attacker faces these vulnerable devices in order to steal sensitive data. To protect these devices, security administrators deploy various procedures such as access control mechanisms, password protection, and firewalls that use cryptographic techniques to secure the network and data. These strategies, however, are insufficient. Monitoring the network for malicious activity using machine learning and deep learning algorithms is a viable approach.

The performance of various single machine learning models in the proposed architecture is shown in Table 1. Model performance differed little between the employed algorithms. According to the data, the RF had the highest performing metrics in terms of R^2 (0.9965) and the lowest error scores in all other metrics, including RMSE (0.0015), MAE (0.0522), and (0.0872).

According to Table 1, the NB obtained the second-best performing ML model. The NB had an R^2 of 0.9261, whereas the SVM had an R^2 of 0.9125. In terms of other performance categories, the NB also had the second-best error scores in terms of RMSE (0.0032), MAE (0.0625), and MAPE (0.0877).

Although all of the models earned substantial scores in all of the performance measures, the SVM performed the worst in terms of the error scores, however, with substantial accuracy. According to this study, the RF is the best ML algorithm for recognizing legitimate or malicious communication in a linked computer network.

Table 1. ML models performance and evaluation.

Model	Metrics	Results
RF	R2	0.9965
	RMSE	0.0015
	MAE	0.0522
	MAPE	0.0872
SVM	R2	0.9125
	RMSE	0.0045
	MAE	0.0721
	MAPE	0.0880
NB	R2	0.9261
	RMSE	0.0032
	MAE	0.0625
	MAPE	0.0877

The coefficient of determination (R^2) of the models used is shown in Fig. 2. This provides a clear visualization of the models' performance. It should be noted that when the coefficient of determinant (R^2) approaches 1, the models perform better. In regression analysis, the accuracy representation is the coefficient of determinant. Random forest is the top performing model, followed by naive bayes classifiers.

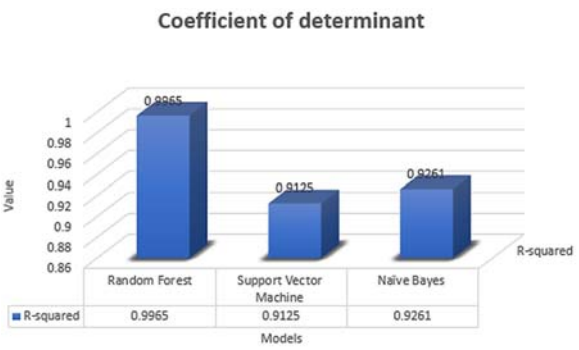

Fig. 2. R-squared representation of the ML models.

Furthermore, Fig. 3 depicts the error score performance of the models, namely, random forest, support vector machine, and nave bayes classifiers. Among the other machine learning models, the random forest achieved the best error ratings.

4.3. Comparison with State-of-the-art

Additionally, the study's findings were compared to the state-of-the-art to assess the robustness of the models used. The RF used in the study outperformed a comparable study by Vimont et al. [22], while the NB outperformed Disha and Waheed [23] in accomplishing the same goal as this study. With considerable error scores, the proposed model beat the aforementioned studies. This study contributes a fresh method to the body of literature in the domain area. Furthermore, the study found that it is required to regularly check the functioning of connected computer networks in order to facilitate and improve communication. Computer networks are critical to modern society because they enable the transmission and sharing of information between individuals, groups, and objects. The suggested model is more adaptable and efficient than previous models due to its consistent performance across the coefficient of determination and error rate. The selection of characteristics is another factor that distinguishes the proposed model from previous detection methods. The suggested model performs better with training sets, whereas other approaches under consideration required a large number of variables for botnet detection. Furthermore, the integration of both models strengthens the detection process for both binary and multiclass attack detection scenarios.

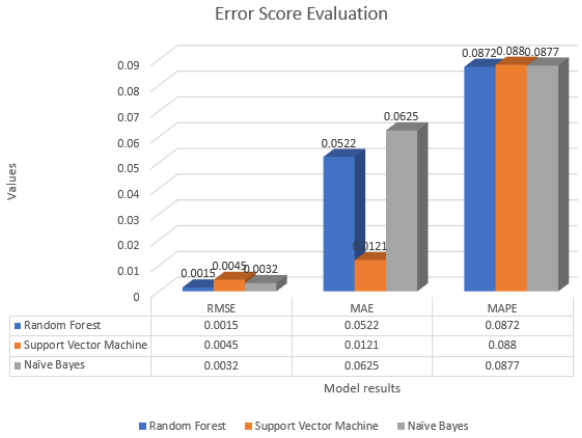

Fig. 3. Error scores of the ML classifiers.

4.4. Analysis of the 10-fold Validation

The data was randomly divided into ten blocks for 10-fold cross-validation, with one block used to train the model and the other nine blocks sent for testing. Finally, the model's performance is determined by averaging the test results from all nine blocks of samples. The k-fold cross-validation method has been proposed as a viable method for analyzing the performance of botnet detection models. Based on the results of the data distribution training outcome of the models, the 10-fold cross-validation that was used had a substantial impact on the performance of the models, thus the 70 %-30 % training and testing split. Again, the model detects all network threats, including DoS and DDoS attempts. The exact inference and results

are also revealed by the depiction of the R2 values in Fig. 2 and the error scores in Fig. 3. Though the suggested model detects several botnet attacks smoothly, with the exception of a few minor class attacks, the model's overall performance must be compared to contemporary state-of-the-art intrusion detection models, which inevitably reveals its true detection capabilities.

5. Conclusion and Future Works

Computer networks have had a huge impact on society by providing global connectivity and information exchange. The utilization of Internet of Things devices has greatly changed communication, and hence digital communication. This study demonstrated that machine learning techniques are effective in detecting actual or malicious traffic in a connected computer network. The models used in this study produced considerable results, and their influence on providing a benchmark analysis for decision making is enormous. The system achieved a performance rate of over 90 % in terms of the coefficient of determinant rates in all three machine learning models, proving it to be a better detector than other peers' botnet detection. Despite the observed performance, the proposed model has several drawbacks. One of the flaws is the lack of a feedback strategy, which might help the system to become more dynamic.

A feedback technique may enable the model to separate the compromised instances or hosts from the network, resulting in a more reliable network communication process. The system fails to detect minority class attack instances such as Heartbleed, Infiltration, and Web-SQL Injection throughout the 10-fold cross validation test and 70 %-30 % train and testing instances split test, posing a challenge to the suggested botnet identification methodologies. It was related to the minority class instances' low engagement in the training program.

The authors want to use deep learning techniques such as convolutional neural networks (CNN) and hybrid models such as random forest-convolutional neural network (RF-CNN) in the future.

Acknowledgements

The authors would like to express their appreciation to Adwoa Afriyie for her advice and help during the study. Our heartfelt thanks also go to Eric Afrifa and Malcolm Afrifa for their encouragement.

References

[1]. J. Vrchota, P. Reho, M. Ma, Critical Success Factors of the Project Management in Relation to Industry 4. 0 for Sustainability of Projects, *Sustainability*, Vol. 13, Issue 1, 2021, 281.

[2]. D. Chatziparaschis, M. G. Lagoudakis, Aerial and Ground Robot Collaboration for Autonomous Mapping in Search and Rescue Missions, *Drones*, Vol. 4, Issue 4, 2020, 79..

[3]. J. Almalki, *et al.*, Enabling Blockchain with IoMT Devices for Healthcare, *Inf.*, Vol. 13, Issue 10, 2022, 448.

[4]. D. Shiny Irene, S. I. Priyadharshini, R. Tamizh Kuzhali, P. Nancy, An IoT based smart menstrual cup using optimized adaptive CNN model for effective menstrual hygiene management, *Artif. Intell. Rev.*, Vol. 56, Issue 7, 2022, pp. 6705-6722.

[5]. C. Diallo, Opportunities and Challenges of IoT Security Using Distributed Ledger Technology, *Sensors & Transducers*, Vol. 256, Issue 2, 2022, pp. 27-35.

[6]. S. Afrifa, V. Varadarajan, P. Appiahene, T. Zhang, Using Machine Learning to Classify Network Abnormalities into Legitimate or Assault in IoT-based Cyber Physical System, in *Proceedings of the 9th International Conference on Sensors and Electronic Instrumentation Advances (SEIA'2023), 20-22 September 2023, Funchal (Madeira Island), Portugal*, 2023, pp. 20-22.

[7]. L. F. Ilca, O. P. Lucian, T. C. Balan, Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response, *Sensors*, Vol. 23, Issue 15, 2023, 6757.

[8]. M. M. Akhtar, D. R. Rizvi, IoT-Chain: Security of things for Pervasive, Sustainable and Efficient Computing using Blockchain, *EAI Endorsed Trans. Energy Web*, Vol. 7, Issue 30, 2020, e7.

[9]. X. D. Hoang, X. H. Vu, An improved model for detecting DGA botnets using random forest algorithm, *Inf. Secur. J.*, Vol. 31, Issue 4, 2022, pp. 441-450.

[10]. S. Afrifa, V. Varadarajan, Cyberbullying Detection on Twitter Using Natural Language Processing and Machine Learning Techniques, *Int. J. Innov. Technol. Interdiscip. Sci.*, Vol. 5, Issue 4, 2022, pp. 1069-1080.

[11]. S. Afrifa, V. Varadarajan, P. Appiahene, T. Zhang, E. A. Domfeh, Ensemble Machine Learning Techniques for Accurate and Efficient Detection of Botnet Attacks in Connected Computers, *MDPI Eng*, 2023, pp. 650-664.

[12]. A. A. Khan, A. A. Laghari, P. Li, M. A. Dootio, S. Karim, The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises, *Sci. Rep.*, Vol. 13, Issue 1, 2023, 1656.

[13]. F. N. Al-Wesabi, *et al.*, Pelican Optimization Algorithm with Federated Learning Driven Attack Detection model in Internet of Things environment, *Futur. Gener. Comput. Syst.*, Vol. 148, 2023, pp. 118-127.

[14]. M. Al Rawajbeh, *et al.*, A new model for security analysis of network anomalies for IoT devices, *Int. J. Data Netw. Sci.*, Vol. 7, Issue 3, 2023, pp. 1241-1248.

[15]. R. Alghamdi, M. Bellaiche, An ensemble deep learning based IDS for IoT using Lambda architecture, *Cybersecurity*, Vol. 6, 2023, 5.

[16]. S. Afrifa, T. Zhang, P. Appiahene, V. Vijayakumar, Mathematical and Machine Learning Models for Groundwater Level Changes: A Systematic Review and Bibliographic Analysis, *Futur. Internet*, Vol. 4, Issue 9, 2022, 259.

[17]. P. Appiahene, V. Varadarajan, T. Zhang, S. Afrifa, Experiences of sexual minorities on social media: A study of sentiment analysis and machine learning

approaches, *J. Auton. Intell.*, Vol. 6, Issue 2, 2023, pp. 1-15.
[18]. W. K. Adu, P. Appiahene, S. Afrifa, VAR, ARIMAX and ARIMA models for nowcasting unemployment rate in Ghana using Google trends, *J. Electr. Syst. Inf. Technol.*, Vol. 10, 2023, 12.
[19]. S. Afrifa, T. Zhang, X. Zhao, P. Appiahene, M. S. Yaw, Climate change impact assessment on groundwater level changes: A study of hybrid model techniques, *IET Signal Process.*, Vol. 17, 2023, e12227.
[20]. P. Appiahene, E. J. Arthur, S. Korankye, S. Afrifa, J. W. Asare, E. T. Donkoh, Detection of anemia using conjunctiva images: A smartphone application approach, *Med. Nov. Technol. Devices*, Vol. 18, 2023, 100237.
[21]. P. Appiahene, J. W. Asare, E. T. Donkoh, G. Dimauro, R. Maglietta, Detection of iron deficiency anemia by medical images: a comparative study of machine learning algorithms, *BioData Min.*, Vol. 16, Issue 1, 2023, 2.
[22]. A. Vimont, H. Leleu, I. Durand-Zaleski, Machine learning versus regression modelling in predicting individual healthcare costs from a representative sample of the nationwide claims database in France, *Eur. J. Heal. Econ.*, Vol. 23, Issue 2, 2022, pp. 211-223.
[23]. R. A. Disha, S. Waheed, Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique, *Cybersecurity*, Vol. 5, 2022, 1.