Available *online* at : http://jnte.ft.unand.ac.id/

Jurnal Nasional Teknik Elektro

| ISSN (Print) 2302-2949 | ISSN (Online) 2407-7267 |

Intrusion Detection System Development on Internet of Things using Ensemble Learning

Nadia Ariana [1,2], Satria Mandala [1,2], Mohd Fadzil Hassan [3], Muhammad Qomaruddin [4], Bilal Ibrahim Bakri [5]

[1] *Department of Informatics, School of Computing, Telkom University, Bandung, 40257, Indonesia.*
[2] *Human Centric (HUMIC) Engineering, School of Computing, Telkom University, Bandung, 40257, Indonesia.*
[3] *Department of Computer and Information Sciences, Universiti Teknologi Petronas, Seri Iskandar, Perak, 32610, Malaysia.*
[4] *Faculty of Industrial Technology, Universitas Islam Sultan Agung, Semarang, 50112, Indonesia.*
[5] *Department of Business Information Technology, Business Informatics College, University of Information Technology and Communication, Baghdad, 10068, Iraq.*

ARTICLE INFORMATION

Received: June 22, 2023
Revised: August 4, 2023
Accepted: August 22, 2023
Available online: July 31, 2024

KEYWORDS

IDS, IOT, machine learning, security

CORRESPONDENCE

E-mail: satriamandala@telkomuniversity.ac.id

ABSTRACT

The utilization of intrusion detection systems (IDS) can significantly enhance the security of IT infrastructure. Machine learning (ML) methods have emerged as a promising approach to improving the capabilities of IDS. The primary objective of an IDS is to detect various types of malicious intrusions with a high detection rate while minimizing false alarms, surpassing the capabilities of a firewall. However, developing an IDS for IOT poses substantial challenges due to the massive volume of data that needs to be processed. To address this, an optimal approach is required to improve the accuracy of data containing numerous attacks. In this study, we propose a novel IDS model that employs the Random Forest, Decision Tree, and Logistic Regression algorithms using a specialized ML technique known as Ensemble Learning. For this research, we used the BoT-IoT datasets as inputs for the IDS model to distinguish between malicious and benign network traffic. To determine the best model, we compared the performance metrics of each algorithm across different parameter combinations. The research findings demonstrate exceptional performance, with metric scores exceeding 99.995% for all parameter combinations. Based on these conclusive results, we deduce that the proposed model achieves remarkable success and outperforms other traditional ML-based IDS models in terms of performance metrics. These outcomes highlight the potential of our novel IDS model to enhance the security posture of IoT-based systems significantly.

INTRODUCTION

New cybersecurity risks have emerged because of the organizations of deploying Internet of Things (IoT) devices in information technology environments [1], [2]. These emerging risks have the capacity to undermine fundamental principles such as operational ecosystem security, efficiency, mobility, and safety [3]. The advent of novel threat vectors not only impacts the technological aspects of our lives but also poses risks to our financial and physical well-being. The potential for attacks has raised concerns regarding online privacy, social networks, businesses, and critical infrastructure [4]. In a short period of time, it has the potential to cause harm to the hardware system as well [5]. This phenomenon is anticipated to extend globally, driven by the imperative need to implement security measures across a broader and more critical spectrum of fields than ever before. However, this is only the initial phase of an increasingly advanced era of digitalization.

The Internet of Things (IoT) comprises interconnected smart devices, enabling them to collect and exchange information seamlessly [6]. In most cases, IoT systems are composed of three primary components: IoT devices, network elements, and the acquisition of sensory data [7]. One fundamental attribute of IoT devices is they are continually active [8], [9]. Amidst such rapid advancements, the substantial volume of statistics presents new challenges for the development of information security [10]. This progress must align with the emergence of increasingly advanced threats, such as exploits and vulnerabilities within global data networks and numerous technical and security challenges [11]. Among those challenges, one notable concern is the occurrence of anomalous network dataflow, commonly referred to as network intrusion or breach.

Intrusion refers to the deliberate attempts to a sequence of unexpected activities, whether originating locally or globally, that undermine the confidentiality, integrity, or availability of a network [12]. There are various avenues through which these attacks can be carried out, including exploiting vulnerabilities in

https://doi.org/10.25077/jnte.v13n2.1113.2024

applications, protocols, and web applications. The presence of malicious applications on interconnected devices within an IoT network further compounds the problem. The larger the IoT network, the greater the potential for vulnerabilities, as attackers can target any device connected to the network to gain unauthorized access. The increase of use of IoT-based systems amplifies the risk of these attacks, potentially leading to profound societal impacts [13]. The application of an Intrusion Detection System (IDS) is one of several approaches to overcome this problem.

Considering the increasing demand and the necessity to address future complex threats, the implementation of Machine Learning (ML) techniques can serve as a solution to amplify an IDS. Numerous research studies have applied ML-based approaches for intrusion detection [14]. Authors in [15] conducted research that extensively explores the malicious use of machine learning which aiming to undermine user privacy, system stability, and service integrity, while also enhancing techniques related to intrusion and obfuscation. Nonetheless, network traffic has grown increasingly intricate and subject to dynamic changes, while cyber-attacks continue to evolve daily. It implies that new standardized patterns or unknown attacks have the potential to deviate from the patterns learned from the initial training data [16], leading to numerous errors during the actual process of the detection of the attack detection system. To address this challenge, it is imperative to develop a methodology which capable to identify the real-time errors when detecting cyber-attacks and dynamically adjust the attack detection system based on the prevailing attack conditions.

There were numerous research studies focused on the application of ML methods in IDS [17]. Authors in [11] proposes an intrusion decision system using the Random Forest Bagging, Gradient Boosting, and XGB classifier and it has an accuracy value of 94.3%, 92% and 94.3%. In 2022, an experiment with ensemble learning bagging on IOT conducted to detect a multi-classification and attained 96.2% on N-BaIoT data set [18]. These studies setting a new standard and paving the way for future researchers to strive into this field by developed remarkable results and scores. However, most of these research efforts primarily relied on the combination of traditional ML techniques and outdated datasets for training and validation purposes. To bridge this gap, this study suggests the implementation of more advanced ML methods, specifically Random Forest, Decision Tree, and Logistic Regression algorithm using Ensemble Learning Technique. These methods will be applied to a newly curated dataset comprising comprehensive descriptions of intrusions.

METHODS

Materials

Data

The conventional approach to train an IDS often involves manually generating a personalized or dedicated real network traffic dataset. While it is possible to create such datasets, most of the handcrafted network traffic samples are usually rather limited in coverage and raise concerns regarding their integrity. In this case, public datasets help address this problem. All the attack types in the dataset are shown in Figure 1.

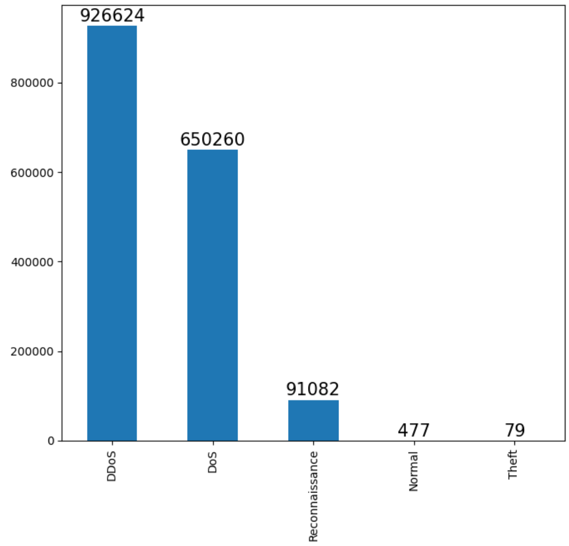

Figure 1. Attack Types

This experiment uses BoT-ToT dataset because it is one of the most recent public traffic datasets in the research field and represents a range of realistic network attacks [19], [20]. The dataset correlation is shown in Figure 2.

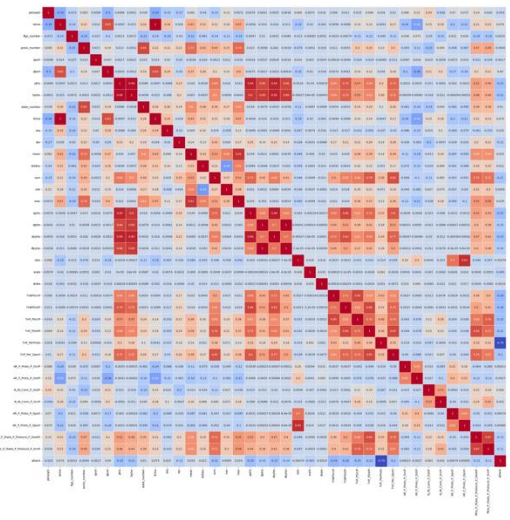

Figure 2. Dataset Correlation

Methods

The objective of this research is to detect attacks using ensemble technique, implement the models into the dataset, and compared three machine learning algorithms with Bagging Method. Firstly, we input the BoT-IoT dataset, and preprocessing is performed. Once the preprocessing stage is completed, the subsequent step is to construct the core of the IDS system. Initially, we build the models from the three algorithms preselect algorithms. When the DT, RF, and LR algorithms already modelled, we do the voting classifier to ensembled the three models. Figure 3 shows the flowchart of the research.

https://doi.org/10.25077/jnte.v13n2.1113.2024

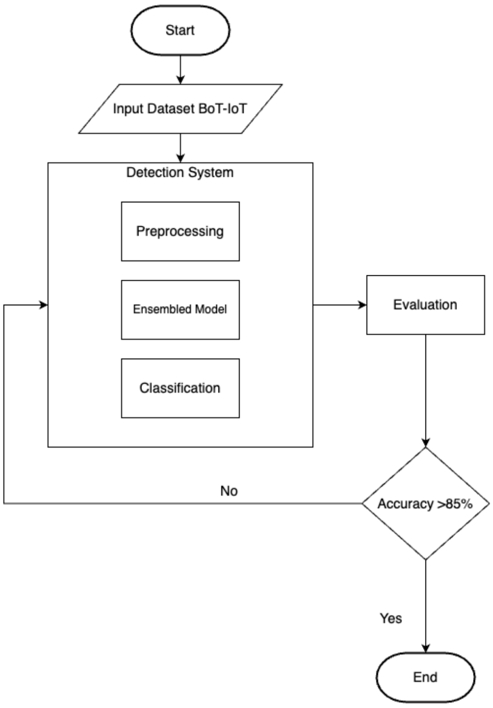

Figure 3. Flowchart of the research methodology

Preprocessing

Preprocessing serves as the foundational stage that affects the subsequent process of the research. The dataset was preprocessed to enhance the accuracy of the models. This dataset contains 926624 DDoS attacks, 650260 DoS attacks, 91082 Reconnaissance, 477 non-malicious attacks, and 79 theft attacks. In this study, the initial step involves data cleaning by eliminating irrelevant data, the aim is to prevent misunderstandings during the subsequent stage.

Ensemble Learning

There are various ensemble classifiers, including random subspace, bagging, and boosting [21]. In this experiment, we use bagging method (bootstrap aggregation), which are general ensemble methods. When addressing classification problems, bagging employs both the “voting” and regression averaging” approaches [11]. The ensemble method aims to choose the best final decision by using a majority vote on the output of the individual classifiers [22]. Figure 4 illustrates how the ensemble contributes to the research.

Various learning techniques are used by the ensemble classifier to achieve better performance than any single classifier. We designed an IDS that has been trained with RF, DT, and LR algorithm using Bagging Method. The bagging procedure is shown in Figure 5.

a. Random Forest

Random Forest (RF) is a decision tree ensemble method, generates multiple decision trees using different samples and makes classification decision based on the majority vote among them. The advantage of RF is it offers improved precision while prevent the risk of overfitting [23].

a. Decision Tree

DT is a supervised learning algorithm that employs a tree structure for classifying input vectors, where each node in the tree represents a comparison of attributes and field [24], [25]. The structure of this method comprises nodes, branches, and leaves, forming a tree-like arrangement. Based on the outcome of these comparisons (true or false), the traversal path is determined, either to the left or the right child of a specific node [24].

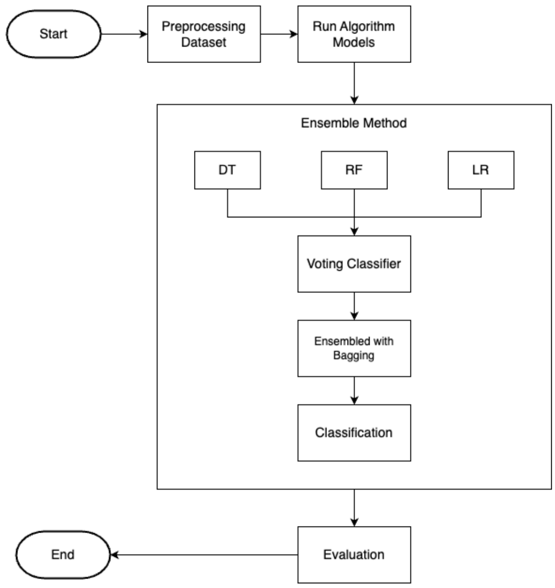

Figure 4. Ensemble work

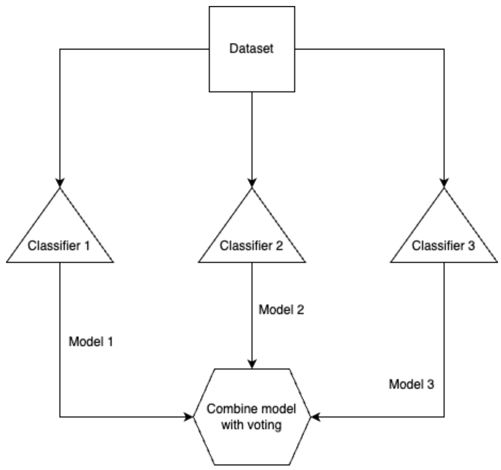

Figure 5. Bagging Process

b. Logistic Regression

Logistic Regression, a supervised classifier that employs a discriminative model during the training phase to make predictions based on the provided data [26], [27]. The logistic regression algorithm employed in this experiment is a classification technique. It is an efficient and computationally lightweight algorithm that performs an excellent scalability and performance even when handling extensive datasets. Logistic Regression is relatively less common employed in intrusion detection [28]. Nevertheless, a logistic regression-based intrusion detection model has been investigated in [29] through multi-class classification testing, this model demonstrated superior performance compared to other models.

Voting Technique

Voting refers to a machine learning model that aggregates predictions from multiple models to make a final decision [30]. In this study, voting was employed to enhance model performance.

Metrics

In this research, evaluation was employed to assess the system or algorithm's performance. The visualization of system performance was accomplished using a confusion matrix. In this research, we used accuracy as performance measure of the detection. Precision, recall, and f1 score as performance measure of the attacks.

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \tag{1}$$

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

Precision represents the proportion of accurate detections that are correctly classified [31] .

$$Recall = \frac{TP}{FN + TP} \tag{3}$$

Recall measures the proportion of the right detections to the total number of intrusion cases in the dataset [31], [32].

$$F1\ Score = \frac{2\ x\ Precision\ x\ Recall}{Precision + Recall} \tag{4}$$

The F1 score metric offers a balanced assessment of both precision and recall [31], [33]. True Positive (TP) becomes relevant when the model recognizes a malicious attack as malicious, while True Negative (TN) arises when the non-malicious packets are recognized as non-malicious. On the other hand, the predicted False Positive (FP) value arises when the traffic is non-malicious and recognized as malicious, while False Negative (FN) appears when a particular attack is malicious and recognized as non-malicious.

RESULTS AND DISCUSSION

We have collected conclusive analysis on the achievement of high performance in Intrusion Detection Systems (IDS) through parameter tweaking and the implementation of Ensemble Method and ML models, based on the experimental stages. In this section, the performance evaluation of the proposed model based on Ensemble Learning is presented. Furthermore, the performance of this method and the other models such as DT, RF, and LR presented on the following sub-headings.

Performance of Classification Model with Bagging Method

Once the data was preprocessed, we divided the dataset and constructed models using Bagging (Bootstrap Aggregating) technique. Authors in [34] conducted research on IDS using ensemble of DT algorithm and it has accuracy value of 97.73% with bagging method. The outcomes of this model are presented in Table 1. The accuracy result shows the application of ensemble method in machine learning significantly enhances the accuracy measurement of the attack detection.

Table 1. Result with Ensemble Bagging

Model	Method	Accuracy
DT RF LR	Ensembled with Bagging	99.995%

Performance of Model of Attacks with Bagging Method

Table 2. Result of the model attacks

Attack	Precision	Recall	F1 Score	Support
DDoS	1.00	1.00	1.00	184885
DoS	1.00	1.00	1.00	130585
Normal	1.00	1.00	1.00	80
Reconnaissance	1.00	1.00	1.00	18141
Theft	0.00	0.00	0.00	14

From Table 2, the performance metrics shows the proposed models have already achieved remarkable results, consistently obtaining scores of 1.00 across metrics. Nonetheless, the only notable distinction in this stage of the process is the small size of one of the attacks that tends to round down the result of the IDS model.

Discussion

The process of determining the optimal Intrusion Detection System (IDS) model is done by involving Ensemble Method. The experiment begins by preprocessing the dataset to make it more suitable for the utilization in the machine learning model. In this case, we train each model individually and combined them through an averaging process with Bagging (Bootstrap Aggregating). Figure 6 shows how bagging classifier works.

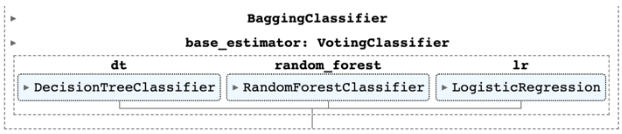

Figure 6. Bagging Classifier

Once the optimal model parameters have been obtained, it is necessary to evaluate the outcomes of this experiment to ensure that the IDS can effectively works [35]. Authors in [5] proposes an IDS for IOT, their work using advanced machine learning can detect intrusion for IOT networks but the TP rate of the U2R attacks is relatively small at 27%. In this study, a confusion matrix was employed to visualize the performance of the system. Each cell in the confusion matrix represents the count of predictions made by the model, indicating whether it accurately or inaccurate classified the classes [36]. The detailed description of the matrix is shown in Figure 7.

https://doi.org/10.25077/jnte.v13n2.1113.2024

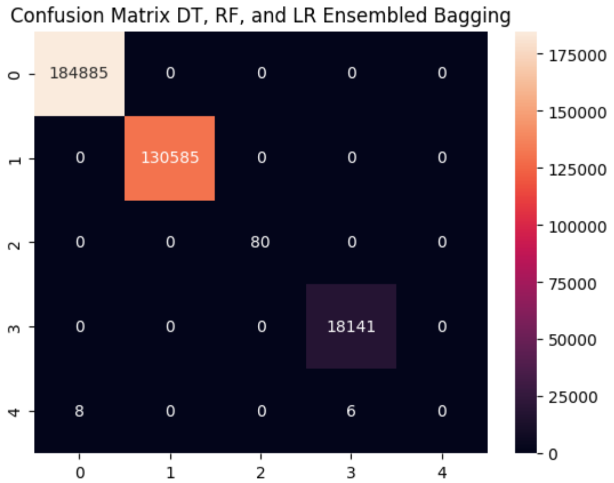

Figure 7. Confusion Matrix

Comparison with State-of the Art Related

The model proposed in this research has demonstrated a higher accuracy compared to [37], the current research that conducted an implementation with AdaBoost and reached 95.84% in accuracy. Table 3 shows the classification accuracy of our method and these methods in [37]–[43]. Our proposed ensemble model with DT, RF, and LR method demonstrates an exceptional performance compared to other methods in terms of attack detection accuracy by using the most recent datasets.

Table 3. Comparison with Related Studies

Work	Method	Dataset	Accuracy
Rachmadi et al. [37]	Ensemble with AdaBoost	MQTTset	95.84%
Meemongkolkiat et al. [38]	Bagging Classifier	CICIDS2017	99.96%
Kerim [39]	NB and RF with Ensemble	CICIDS2017	99.8%
Ghrib et al. [40]	Ensemble with XGBoost	NSL-KDD	98.72%
Seth et al. [41]	Voting Ensemble	CIC-IDS2018	95.49%
Mahfouz et al. [42]	Ensemble Model	HOIC Tool	98.99%
Lian et al. [43]	Adaboost	KDDCUP 99	98.89%
Our Method	Ensemble with Bagging	BoT-IoT	99.995%

CONCLUSIONS

Based on the experiment, the result indicates that the application of the Decision Tree (DT), Random Forest (RF), and Logistic Regression (LR) algorithm can serve as an excellent approach for constructing an Intrusion Detection System (IDS). This is achieved by employing the technique of ensemble learning into three machine learning algorithms. The research findings reveal that all the parameter combinations surpass 99.995%.

Ensemble learning plays a crucial role in enhancing the certainty of model decisions. As demonstrated, the performance of an ensemble model can be significantly impacted by the selection of the algorithms. Hence, it is crucial to develop an Intrusion System Detection (IDS) that is scalable, flexible, and reliable to fulfill the requirements of the Internet of Things (IoT). It is imperative to evaluate IDS models in terms of accuracy within a big data environment. By appropriately selecting the algorithm for building a system with ensemble method, the proposed classifier can achieve a higher performance compared to the other. These findings indicate that the right combined algorithm can substantially enhance classifier performance and has proven to accomplish higher accuracy compared to other machine learning models with ensemble learning. In the future, there is a potential to enhance a different Ensemble Learning model for IDS on IOT.

ACKNOWLEDGMENT

This research was supported by Research Center for Human Centric (HUMIC) Engineering and School of Computing, Telkom University, Bandung, Indonesia.

REFERENCES

[1] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset." 2018.

[2] K. Albulayhi, Q. Abu Al-Haija, S. A. Alsuhibany, A. A. Jillepalli, M. Ashrafuzzaman, and F. T. Sheldon, "IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method," *Applied Sciences*, vol. 12, no. 10, 2022, doi: 10.3390/app12105015.

[3] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards Developing Network forensic mechanism for Botnet Activities in the IoT based on Machine Learning Techniques," Jun. 2017.

[4] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, Nov. 2019, doi: 10.1016/J.FUTURE.2019.04.038.

[5] T. Saba, T. Sadad, A. Rehman, Z. Mehmood, and Q. Javaid, "Intrusion Detection System Through Advance Machine Learning for the Internet of Things Networks," *IT Prof*, vol. 23, no. 2, pp. 58–64, 2021, doi: 10.1109/MITP.2020.2992710.

[6] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks," *Electronics (Switzerland)*, vol. 8, no. 11, 2019, doi: 10.3390/electronics8111210.

[7] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, and H. Janicke, "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports," *IEEE Access*, vol. 8, pp. 209802–209834, 2020, doi: 10.1109/ACCESS.2020.3036728.

[8] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for

Internet of Things networks: A particle deep framework," *Future Generation Computer Systems*, vol. 110, pp. 91–106, 2020, doi: https://doi.org/10.1016/j.future.2020.03.042.

[9] N. Koroniotis and N. Moustafa, "Enhancing network forensics with particle swarm and deep learning: The particle deep framework," *CoRR*, vol. abs/2005.00722, 2020, [Online]. Available: https://arxiv.org/abs/2005.00722

[10] A. R. Zarzoor, N. A. S. Al-Jamali, and D. A. Abdul Qader, "Intrusion detection method for internet of things based on the spiking neural network and decision tree method," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 2278–2288, 2023, doi: 10.11591/ijece.v13i2.pp2278-2288.

[11] D. Rani, N. S. Gill, P. Gulia, and J. M. Chatterjee, "An Ensemble-Based Multiclass Classifier for Intrusion Detection Using Internet of Things," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/1668676.

[12] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A New Ensemble-Based Intrusion Detection System for Internet of Things," *Arab J Sci Eng*, vol. 47, no. 2, pp. 1805–1819, 2022, doi: 10.1007/s13369-021-06086-5.

[13] S. Alshathri, A. El-Sayed, W. El-Shafai, and E. El-Din Hemdan, "An Efficient Intrusion Detection Framework for Industrial Internet of Things Security," *Computer Systems Science and Engineering*, vol. 46, no. 1, pp. 819–834, 2023, doi: 10.32604/csse.2023.034095.

[14] A. Aljuhani, "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," *IEEE Access*, vol. 9, pp. 42236–42264, 2021, doi: 10.1109/ACCESS.2021.3062909.

[15] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly," *IEEE Access*, vol. 7, pp. 158126–158147, 2019, doi: 10.1109/ACCESS.2019.2948912.

[16] R. Abu Bakar, X. Huang, M. S. Javed, S. Hussain, and M. F. Majeed, "An Intelligent Agent-Based Detection System for DDoS Attacks Using Automatic Feature Extraction and Selection," *Sensors*, vol. 23, no. 6, 2023, doi: 10.3390/s23063333.

[17] R. Alanazi and A. Aljuhani, "Anomaly Detection for Industrial Internet of Things Cyberattacks," *Computer Systems Science and Engineering*, vol. 44, no. 3, pp. 2361–2378, 2023, doi: 10.32604/csse.2023.026712.

[18] Q. A. Al-Haija and M. Al-Dala'ien, "ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks," *Journal of Sensor and Actuator Networks*, vol. 11, no. 1, 2022, doi: 10.3390/jsan11010018.

[19] N. Koroniotis, "Designing an effective network forensic framework for the investigation of botnets in the Internet of Things," 2020.

[20] A. Koirala, R. Bista, and J. C. Ferreira, "Enhancing IoT Device Security through Network Attack Data Analysis Using Machine Learning Algorithms," *Future Internet*, vol. 15, no. 6, 2023, doi: 10.3390/fi15060210.

[21] N. Naz *et al.*, "Ensemble learning-based IDS for sensors telemetry data in IoT networks," *Mathematical Biosciences and Engineering*, vol. 19, no. 10, pp. 10550 – 10580, 2022, doi: 10.3934/mbe.2022493.

[22] Y. Alotaibi and M. Ilyas, "Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things’ Devices Security," *Sensors*, vol. 23, no. 12, 2023, doi: 10.3390/s23125568.

[23] J. B. Awotunde, F. E. Ayo, R. Panigrahi, A. Garg, A. K. Bhoi, and P. Barsocchi, "A Multi-level Random Forest Model-Based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks," *International Journal of Computational Intelligence Systems*, vol. 16, no. 1, 2023, doi: 10.1007/s44196-023-00205-w.

[24] N. Thockchom, M. M. Singh, and U. Nandi, "A novel ensemble learning-based model for network intrusion detection," *Complex and Intelligent Systems*, 2023, doi: 10.1007/s40747-023-01013-7.

[25] M. and O. S. and A. F. Alshamy Reem and Ghurab, "Intrusion Detection Model for Imbalanced Dataset Using SMOTE and Random Forest Algorithm," in *Advances in Cyber Security*, S. and A. M. Abdullah Nibras and Manickam, Ed., Singapore: Springer Singapore, 2021, pp. 361–378.

[26] E. Alshahrani, D. Alghazzawi, R. Alotaibi, and O. Rabie, "Adversarial attacks against supervised machine learning based network intrusion detection systems," *PLoS One*, vol. 17, no. 10 October, 2022, doi: 10.1371/journal.pone.0275971.

[27] M. Bhati Nitesh Singh and Khari, "An Ensemble Model for Network Intrusion Detection Using AdaBoost, Random Forest and Logistic Regression," in *Applications of Artificial Intelligence and Machine Learning*, H. M. and R. G. Unhelker Bhuvan and Pandey, Ed., Singapore: Springer Nature Singapore, 2022, pp. 777–789.

[28] A. Churcher *et al.*, "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors (Switzerland)*, vol. 21, no. 2, pp. 1–32, 2021, doi: 10.3390/s21020446.

[29] P. Ghosh and R. Mitra, "Proposed GA-BFSS and logistic regression based intrusion detection system," Jun. 2015, pp. 1–6. doi: 10.1109/C3IT.2015.7060117.

[30] A. Koirala, R. Bista, and J. C. Ferreira, "Enhancing IoT Device Security through Network Attack Data Analysis Using Machine Learning Algorithms," *Future Internet*, vol. 15, no. 6, 2023, doi: 10.3390/fi15060210.

[31] A. Al-Saleh, "A balanced communication-avoiding support vector machine decision tree method for smart intrusion detection systems," *Sci Rep*, vol. 13, no. 1, 2023, doi: 10.1038/s41598-023-36304-z.

[32] Y. Saheed, O. Abdulganiyu, and T. Ait Tchakoucht, "A Novel Hybrid Ensemble Learning for Anomaly Detection in Industrial Sensor Networks and SCADA Systems for Smart City Infrastructures," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, Jun. 2023, doi: 10.1016/j.jksuci.2023.03.010.

[33] B. I. Hairab, M. Said Elsayed, A. D. Jurcut, and M. A. Azer, "Anomaly Detection Based on CNN and Regularization Techniques Against Zero-Day Attacks in

IoT Networks," *IEEE Access*, vol. 10, pp. 98427–98440, 2022, doi: 10.1109/ACCESS.2022.3206367.

[34] O. D. and A. A. O. and M. J. O. Mebawondu Olamatanmi J. and Alowolodu, "Optimizing the Classification of Network Intrusion Detection Using Ensembles of Decision Trees Algorithm," in *Information and Communication Technology and Applications*, B. Misra Sanjay and Muhammad-Bello, Ed., Cham: Springer International Publishing, 2021, pp. 286–300.

[35] N. Abdullah, S. Manickam, and M. Anbar, *Advances in Cyber Security Third International Conference, ACeS 2021, Penang, Malaysia, August 24–25, 2021, Revised Selected Papers: Third International Conference, ACeS 2021, Penang, Malaysia, August 24–25, 2021, Revised Selected Papers*. 2021. doi: 10.1007/978-981-16-8059-5.

[36] D. Rani, N. S. Gill, P. Gulia, F. Arena, and G. Pau, "Design of an Intrusion Detection Model for IoT-Enabled Smart Home," *IEEE Access*, vol. 11, pp. 52509–52526, 2023, doi: 10.1109/ACCESS.2023.3276863.

[37] S. Rachmadi, S. Mandala, and D. Oktaria, "Detection of DoS Attack using AdaBoost Algorithm on IoT System," in *2021 International Conference on Data Science and Its Applications (ICoDSA)*, 2021, pp. 28–33. doi: 10.1109/ICoDSA53588.2021.9617545.

[38] N. Meemongkolkiat and V. Suttichaya, "Analysis on Network Traffic Features for Designing Machine Learning based IDS," in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/1993/1/012029.

[39] B. Kerim, "Securing IoT Network against DDoS Attacks using Multi-agent IDS," in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/1898/1/012033.

[40] T. Ghrib, M. Benmohammed, and P. S. Pandey, "Automated diagnosis of attacks in internet of things using machine learning and frequency distribution techniques," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 950–961, 2021, doi: 10.11591/eei.v10i2.2766.

[41] S. Seth, K. K. Chahal, and G. Singh, "A Novel Ensemble Framework for an Intelligent Intrusion Detection System," *IEEE Access*, vol. 9, pp. 138451–138467, 2021, doi: 10.1109/ACCESS.2021.3116219.

[42] A. Mahfouz, A. Abuhussein, D. Venugopal, and S. Shiva, "Ensemble classifiers for network intrusion detection using a novel network attack dataset," *Future Internet*, vol. 12, no. 11, pp. 1–19, 2020, doi: 10.3390/fi12110180.

[43] W. Lian, G. Nie, B. Jia, D. Shi, Q. Fan, and Y. Liang, "An intrusion detection method based on decision tree-recursive feature elimination in ensemble learning," *Math Probl Eng*, vol. 2020, 2020, doi: 10.1155/2020/2835023.

AUTHOR(S) BIOGRAPHY

Nadia Ariana
An undergraduate student in Informatics at the Faculty of Informatics, School of Computing, Telkom University, Bandung, Indonesia.

Satria Mandala
Satria Mandala is currently an Associate Professor in Human Centric (HUMIC) Engineering, School of Computing, Telkom University, Bandung, Indonesia. His research interests cover various areas, including Network Security, Wireless Sensor Network and Biomedical Informatics using Machine Learning. He received his PhD in Computer Science at the Universiti Teknologi Malaysia (UTM). He also has authored numbers of papers in preferred academic journals and a reviewer of scientific journals and conferences.

Mohd Fadzil Hassan
PhD in Informatics at University of Edinburgh, UK. Currently the Director of the Institute of Autonomous Systems Universiti Teknologi Petronas (UTP) Malaysia. The area of research interest concentrates on Artificial Intelligence, Multiagent Systems, and Service-Oriented Architecture (SOA).

Muhammad Qomaruddin
Muhammad Qomaruddin obtained his B.Sc. degree in Informatics Engineering from the Institut Sains Teknologi "AKPRIND", Yogyakarta, Indonesia. And obtained Master and PhD degrees in Computer Science from UTM Malaysia. Currently he is a senior lecturer at Universitas Islam Sultan Agung (UNISSULA), Semarang, Indonesia. The area of research interest concentrates on Education Technology, Human-computer interaction, Social Computing, Information System and social impact of technology.

Bilal Ibrahim Bakri
Bilal Ibrahim Bakri is MSc in communications and computers, assistant lecturer at Department of Business Information Technology, Business Informatics College, University of Information Technology and Communication, Iraq. His main research interest is related to communications and information technology.