Machine Learning and Deep Learning Approaches for CyberSecurity: A Review

ASMAA HALBOUNI1, (Graduate Student Member, IEEE), TEDDY SURYA GUNAWAN1, (Senior Member, IEEE), MOHAMED HADI HABAEBI1, (Senior Member, IEEE), MURAD HALBOUNI2, MIRA KARTIWI3, (Member, IEEE), AND ROBIAH AHMAD4, (Senior Member, IEEE)

1Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur 53100, Malaysia
2Department of Natural, Engineering and Technology Sciences, Arab American University, Jenin 240, Palestine
3Information Systems Department, International Islamic University Malaysia, Kuala Lumpur 53100, Malaysia
4Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur 54100, Malaysia

Corresponding author: Teddy Surya Gunawan (tsgunawan@iium.edu.my)

This work was supported by Universiti Teknologi Malaysia through Collaborative Research Grant CRG18.2.R.K130000.7356.4B416.

ABSTRACT The rapid evolution and growth of the internet through the last decades led to more concern about cyber-attacks that are continuously increasing and changing. As a result, an effective intrusion detection system was required to protect data, and the discovery of artificial intelligence’s sub-fields, machine learning, and deep learning, was one of the most successful ways to address this problem. This paper reviewed intrusion detection systems and discussed what types of learning algorithms machine learning and deep learning are using to protect data from malicious behavior. It discusses recent machine learning and deep learning work with various network implementations, applications, algorithms, learning approaches, and datasets to develop an operational intrusion detection system.

INDEX TERMS Cybersecurity, machine learning, deep learning, intrusion detection system.

I. INTRODUCTION

The internet is transforming people’s jobs, learning, and lifestyles, and today, allowing to the integration of social life and the internet, which increases security threats in various ways. What counts now is learning how to identify network threats and cyberattacks, particularly those previously seen. Cybersecurity is defined as the process of implementing cyber protective measures and policies to protect data, programs, servers, and network infrastructures from unauthorized access or modification. The internet connects the majority of our computer systems and network infrastructure. As a result, cybersecurity emerged as the backbone for practically all types of corporations, governments, and even people to secure data, grow their businesses, and maintain privacy.

People send and receive data across network infrastructure, such as a router, that can be hacked and manipulated by outsiders. The increased use of the internet has increased the amount and complexity of data, resulting in the emergence of big data. The constant rise of the internet and extensive data necessitated the creation of a reliable intrusion detection system. Network security is a subset of cybersecurity that safeguards systems connected to a network against malicious activity. The goal is to provide networked computers to ensure data security, integrity, and accessibility. Current cybersecurity research focuses on creating an effective intrusion detection system that can identify both known and new attacks and threats with high accuracy and a low false alarm rate [1].

As shown in Figure 1, the terms Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) are frequently used interchangeably to describe the same
principles in software development. These names all indicate the same thing: a machine programmed to learn and find the best solution to a problem. DL is a subfield of machine learning, whereas machine learning is a subfield of AI. As a result, ML and DL are employed to create an efficient and effective intrusion detection system. This paper provides an overview of machine learning and deep learning applications and approaches in intrusion detection systems by concentrating on network security technologies, methodologies, and implementation.

Alan Turing stated that general use computers could learn and qualify originality, which has paved the way to whether computers should look at data to develop rules rather than allow humans to do it. Machine learning algorithms are algorithms that can learn and adapt based on data. Machine learning algorithms are designed to generate output based on what is learned from data and examples. For example, such algorithms will allow a computer to choose and perform a particular task on novel traffic detection without explicit information [2].

Automatic analyses of attacks and security events, such as spam mail, user identification, social media analytics, and attack detection may be performed efficiently using machine learning [1]. As indicated in Figure 2, there are three main techniques to machine learning: supervised, unsupervised, semi-supervised, and reinforcement learning. Supervised learning is based on labeled data, unsupervised learning is based on unlabelled data, and semi-supervised learning is based on both.

The remainder of the paper is organized as follows: Section 2 discusses the intrusion detection system concept. Section 3 summarises the most frequently utilized datasets for the intrusion detection system. Section 4 discusses recent advances in machine learning and deep learning-based intrusion detection systems, while Section 5 concludes this paper.

II. INTRUSION DETECTION SYSTEMS

Intrusion Detection is the process of monitoring network traffic and events in computers in order to detect unexpected events, and it is called Intrusion Detection System (IDS) when a software application is used to do so [7]. IDS is a type of network security that can identify and sense risks before services are lost, illegal access is granted, or data is lost [6]. IDS can also provide a graphical user interface through which users can interact by having access to various features when doing the IDS testing and training process [4]. Figure 4 depicts the deployment of two IDS methods depending on activities: a Network-Based Intrusion Detection System (NIDS) and a Host-Based Intrusion Detection System (HIDS). NIDS, for example, examines packets gathered by network devices such as routers, while HIDS examines events on a host computer. Hybrid detection is a system that combines the best of both worlds [1], [8].

A. INTRUSION DETECTION SYSTEM APPROACH

Intrusion detection techniques are classified into Anomaly Detection Methods and Misuse Detection Methods [8], as shown in Table 1.
1) ANOMALY DETECTION
This model assumes that specific abnormal traffic has a low probability and can be distinguished from regular traffic with a high probability [9]. Unsupervised learning and statistical learning-based anomaly detection algorithms can detect unique and undiscovered assaults.

2) MISUSE DETECTION
This approach is a signature-based technique. While monitoring threats in an IDS, detection can occur based on known attack signatures [1]. This strategy is based on supervised learning and can detect illegal or suspicious behaviors that can be used to defend against similar assault behaviors.

TABLE 1. Differences between intrusion detection system approaches.

|                        | Anomaly Detection | Misuse Detection          |
|------------------------|-------------------|----------------------------|
| Detection of attacks   | Known and unknown attacks | Only known attacks |
| Detection performance  | High false alarm   | Low false alarm            |
| Attack background data | No, depend on      | Yes, depend on              |
|                        | knowledge for part | knowledge for all           |
|                        | of the feature     | detections                  |
|                        | design             |                            |
| Detection efficiency   | Depend on the      | High, inverse relation      |
|                        | complexity of the  | with a signature database   |
|                        | model              |                            |
| Update required        | No need for updates| Yes, requires updates       |

B. ATTACK CLASSIFICATION
As the network’s diversity increased, attacks and threats evolved, becoming more sophisticated and non-repetitive. As a result, numerous attack types have been identified, including DoS, Probe, U2R, Worm, Backdoor, R2L, and Trojan [9]. Denial of service (DoS) attacks are among the most common network resource attacks, as they render network services unavailable to all users. They employ a variety of different behaviors and methods to consume network resources. For Probe, the intruder marks open ports after scanning all devices connected to the network to exploit them and gain network access. Then there is Remote to User (R2U), in which an attacker sends packets to various devices across a network to gain access as a local user [10]. For this definition, a worm is defined as a malicious application capable of self-replication from one device to another [9]. Finally, User to Root (U2R) is used, in which the intruder attempts to access network resources to use them as a local user after numerous trials [11].

C. EVALUATION METRICS
Some indications are used to assess an intrusion detection system’s performance, either machine learning or deep learning-based. These indicators are based on the confusion matrix component that contains four metrics: True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN), and the assessment indicators are as follows [1]:

- **Accuracy** - The ratio of correct predictions to records; a higher accuracy indicates a more accurate prediction by the learning model.
- **Recall** - The model’s capacity to locate all positive records is the detection rate, as it quantifies the correctly predicted records.
- **Precision** - The capacity to avoid mislabeling negative records as positive; a high precision rate equates to a low rate of false positives.
- **F1-Score (F1)** - The sum of Precision and Recall; a higher F1 indicates a more effective learning model.
- **False Positive Rate (FPR)** - To compute the False Alarm Rate, divide the total number of normal records identified as attacks by the total number of normal records.

|                          | Predicted as Positive | Predicted as Negative |
|--------------------------|-----------------------|-----------------------|
| Labeled as Positive      | True Positive (TP)    | False Negative (FN)   |
| Labeled as Negative      | False Positive (FP)   | True Negative (TN)    |

For decades, scientists and researchers have been attempting to develop and build an intrusion detection system that is both effective and efficient. With the advent of artificial intelligence, all IDS models utilized machine learning methodologies and approaches. However, after years of research, deep learning began to perform better for IDS, as seen by assessment indicator outcomes. Section IV will explore machine learning and deep learning in IDS.

III. DATASETS
When it comes to intrusion detection systems, one should consider the dataset employed to ensure the system’s accuracy. Nowadays, applications and networks are growing exponentially, necessitating resilient network security. It can be accomplished by selecting the proper datasets for training and testing. Following that, a summary of the most often used dataset in intrusion detection systems will be discussed.
A. KDD CUP 1999
This dataset is the most widely used dataset for intrusion detection, based on the DARPA dataset. This dataset includes basic and high-level TCP connection information such as the connection window but no IP addresses. In addition, this dataset contains over 20 different types of attacks and a record for the test subset [10].

B. UNSW-IDS15
Founded in 2015 by Australian Centre for Cyber Security (ACCS). Samples in this dataset contain normal and malicious traffic [12], and it has been collected from three real-world websites; BID (Symantec Corporation), CVE (Common Vulnerabilities and Exposures), and MSD (Microsoft Security Bulletin) and then to generate the dataset, it emulated in a laboratory environment. This dataset has nine attack families, such as worms, DoS, and fuzzers [9].

C. CIC-IDS2017
The dataset was generated in 2017 by the Canadian Institute for Cybersecurity. This dataset contains normal and attack scenarios and includes an abstract behavior for 25 users based on SSH, HTTPS, HTTP, FTP, and email protocols [8], [13].

D. NSL-KDD
It is the improved KDD dataset, where a large amount of redundancy has been removed, and an advanced sub-dataset has been created [10]. This dataset utilizes the same KDD99 attributes and belongs to four attack categories: DoS, U2R, R2L, and Probe [8].

E. PU-IDS
A derivative dataset from NSL-KDD is generated to extract a statistic from an input data and then utilized to create new synthetic instances. The traffic generator of this dataset obtained the same format and attributes as the NSL-KDD dataset [8].

### Table 3. Attack types in UNSW-IDS15.

| Attack Class | No. of records | Description |
|--------------|----------------|-------------|
| Normal       | 93,000         | Natural traffic data |
| DoS          | 16,353         | Attack to make resources inaccessible for legitimate users |
| Analysis     | 2,677          | Port-based intrusion attacks, HTML penetrations, and spam |
| Fuzzers      | 24,246         | Scan-based intrusion attacks. Using software testing to discover flaws in the operating system or network. |
| Reconnaissance | 13,987   | Attack aims to collect information about flaws in system security |
| Backdoors    | 2,329          | Penetration remote attacks to access the computer by avoiding background security |
| Generic      | 58,871         | Penetration attack for block cipher attacks |

### Table 4. Attack types in CIC-IDS2017.

| Attack Class | No. of records | Description |
|--------------|----------------|-------------|
| Benign       | 2,358,036      | Natural traffic data |
| DDoS         | 41,835         | Multiple users operate simultaneously to attack one service |
| DoS Heartbleed | 11        | Unauthorized access gained by inserting malicious data into OpenSSL memory |
| DoS Hulk     | 231,073        | Unique and obfuscated traffic produced by Hulk tool to perform DoS |
| DoS slowloris | 5796          | Slow lorries tool implemented to perform DoS |
| PortScan     | 158,930        | Collecting data such as services and type of operating system through sending packets with different destination port |
| XSS          | 652            | Injects malicious data through web applications into normal websites |

### Table 5. Attack types in NSL-KDD.

| Attack Class | No. of records | Natural traffic data |
|--------------|----------------|---------------------|
| Normal       | 67,343         | Worm, Land, Smurf, Udpstorm, Teardrop, Pod, Mailbomb, Neptune, Process table, Apache2, Back |
| DoS          | 5,927          | Ipsweep, Nmap, Satan, Portsweep, Mscaen, Saint |
| Probe        | 11,656         | WarezClient, Worm, SnmpGetAttack, WarezMaster, Imap, SnmpGuess, Named, Multihop, Phf, Spy, Sendmail, Fig, Write, Xnoop, Xlock, Guess Password |
| R2L          | 995            | Buffer Overflow, SQLAttack, Rootkit, Perl, Xterm, LoadModule, Ps, Httpancel |
| U2R          | 2              | 200                 |

Table 6 shows a comparison of several deep learning methods, the year the dataset was created, whether it was publicly available, the number of characteristics that were utilized for analysis, and lastly, how much traffic the data handled.
TABLE 6. Comparison between datasets.

| Data Set       | Year | Availability | No. of features | Kind of traffic |
|----------------|------|--------------|----------------|----------------|
| KDD Cup99      | 1998 | Public       | 41             | Emulated       |
| NSL-KDD        | 1998 | Public       | 41             | Emulated       |
| ISOT           | 2010 | Public       | 49             | Emulated       |
| ISCX 2012      | 2012 | Public       | 8              | Emulated       |
| UNSW-NB15      | 2015 | Public       | 42             | Emulated       |
| KYOTO          | 2015 | Public       | 24             | Real traffic   |
| CIC-IDS2017    | 2017 | Public       | 84             | Emulated       |

IV. INTRUSION DETECTION SYSTEMS IN RECENT WORKS USING MACHINE LEARNING AND DEEP LEARNING

Methodologies and algorithms have undergone significant change and evolution to produce the most acceptable intrusion detection system in many applications that attempt to identify constantly changing threats and attacks. Initially, classification was based on machine learning, but as performance needed to be further improved, deep learning was utilized to produce higher accuracy and a lower false alarm rate.

The primary distinction between machine learning and deep learning is illustrated in Figure 5, and it is based on the method by which the system gets input. It depends on how the data is trained by machine learning, but it depends on the connections between artificial neural networks in deep learning to train data without requiring many human interactions. Additional differences between machine learning and deep learning are summarised here and in Table 7.

- **Data dependencies** – This metric indicates the volume of data. In traditional machine learning, based on rules, performance is improved when the data set is limited. In comparison, deep learning performs better with a vast number of data since a significant amount is required for accurate interpretation and understanding.
- **Feature processing** – This is a method of extracting features to generate patterns that contribute to the implementation of learning algorithms and reduce the complexity of the data. In other words, the feature process is used to do categorization and feature detection on raw data. While in machine learning, the expert must determine the necessary representations, in deep learning, the representations are identified automatically through the use of deep learning algorithms.
  - **Interpretability** – This is described as a model’s capacity to comprehend human language. An interpretable model can be understood without extra tools or procedures. On the other hand, it is difficult to specify how neurons should be modeled and how the layers should interact in deep learning, making it difficult to explain how the result was obtained.
  - **Problem-solving** – In conventional machine learning, the problem is divided into sub-problems, each of which is solved independently, and then the final answer is obtained. On the other hand, deep learning will resolve the issue completely [4].

The following subsections describe how researchers employed machine learning and deep learning to create an intrusion detection system.

A. MACHINE LEARNING IDS ALGORITHM

This subsection discusses recent research into IDS implementations that utilize a variety of machine learning algorithms. Machine learning algorithms, such as support vector machine (SVM) and random forest (RF), have been used to investigate the binary categorization of IDS using a supervised learning approach [14]. SVM outperformed RF throughout the training process, whereas RF outperformed SVM during the test procedure. Additionally, they concluded that a classifier’s performance would vary based on the dataset and attributes.

An IDS model based on a decision tree, naïve Bayes, and the random forest was proposed by [15] to classify Probe, R2L, and U2R on the NSL-KDD dataset. It is discovered that the highest accuracy was achieved in detecting DOS attacks using the RF algorithm. Additionally, when they compared their hybrid model with its 14 features to other hybrid models with varying features, the hybrid model had a greater accuracy for DOS, Probe, and U2R and a nearly identical accuracy for R2L.

In order to increase the performance of the attack detection model, an intrusion detection strategy utilizing SVM ensemble with the feature was presented in [16]. They examined validated training data and discovered that it might be used to improve the detection process resulting in the fast training time, high accuracy, and low false alarm rate. However, because this strategy trains classifiers independently of feature spaces and then combines judgments via an ensemble, some correlations across feature spaces will be missed during classifier learning, lowering the model’s accuracy.

Three datasets comprising high-level network features were explicitly created for non-payload-based network intrusion detection systems in [17] by enabling machine learning classifiers to use Advanced Security Network Metrics (ASNM) features. It was the first dataset to include
TABLE 7. Comparison between machine learning and deep learning.

|                               | Machine Learning                  | Deep Learning                     |
|-------------------------------|-----------------------------------|-----------------------------------|
| Input                         | Thousands of data                 | Millions of data (Big data)       |
| Output                        | Numerical values                  | Numerical values, text, sounds    |
| Hardware requirements         | Low-end machines like CPU         | Machines with GPU                 |
| How it works                  | Different algorithms are used to learn and predict future data from past data | Neural networks are used to pass the data through processing layers to interpret relations and features |
| Human Intervention            | Require human intervention a lot  | Does need much human intervention |
| How it’s managed              | Data analysts direct the algorithms to examine specific variables in the dataset | Once the process starts, the algorithms will be self-directed to analyze the dataset |
| Dataset size                  | Works well with the small-medium dataset | Works well with a big dataset |
| No. of layers                 | A shallow network that consists of input, output, and one hidden layer | A deep network that consists of input, output, and at least three hidden layers |
| Features                      | Manual identification of the features | Automatic identifications of the important features |
| Processing Time               | Few seconds or hours              | Few hours or weeks                |
| Training Time                 | Long time                        | Short time                        |
| Decision                      | The machine takes a decision based on the past data | With the help of an artificial neural network, machines take the decision |
| Hyperparameter tuning         | The capability of tuning is limited | It can be tuned in many ways |
| Implementations               | Prediction and simple applications | Complex applications              |
| Problem-solving               | Problem is divided into sub-problem | Solve the whole problem, end to end |
| Interpretability              | Easy to understand the result in some algorithms like DT, and some hard to understand like SVM | Difficult to understand |
| Power                         | Low processing power             | Requires high processing power    |
| Algorithms no.                | Many                             | Few                              |
| Accuracy                      | Less accuracy than DL            | Higher accuracy than ML           |

Adversarial obfuscation techniques and benign traffic samples that were applied to the malicious traffic execution of TCP network connections. While such classifiers can detect a sizable percentage of unknown threats, some unknown attacks may be undetectable, as illustrated in Figure 6.

The requirement for a horizontal platform for IoT applications/M2M resulted in creating the worldwide standard OneM2M [18], which aims to address the requirement for an M2M service layer that enables communication across heterogeneous apps and devices seen in Figure 7. Additionally, the authors investigated the second line of defense for oneM2M IoT networks that can identify and prevent threats and intrusions, dubbed Machine Learning-based Intrusion Detection and Prevention System, which can detect and prevent not only known but also unexpected attacks.

They developed their dataset from real-world IoT networks and implemented a detection model with three machine learning levels to identify and detect assaults and threats. They obtained 99.93% accuracy for the second detection level when using a decision tree-based machine learning algorithm and 99.34% accuracy when using an encoder-based machine learning strategy. However, this model obtained a high degree of accuracy and can detect and respond to risks associated with the oneM2M service layer.

**B. DEEP LEARNING IDS ALGORITHM**

This subsection discusses recent implementations of DL-IDS using a variety of deep learning methods. A model was introduced by [24] to collect and label real network traffic using their dataset in order to investigate mobile application identification and connect it to a cloud server.
TABLE 8. Machine learning algorithms for IDS.

| Author                        | Learning algorithm | Performance metric                                      | Dataset      | Attack targeted                        | Strengths                                                                 | Limitation                                                                 |
|-------------------------------|--------------------|---------------------------------------------------------|--------------|----------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Farnaaz & Jabbar, 2016 [19]   | RF                 | Accuracy, detection rate, false alarm rate, and Mathews | NSL-KDD      | DoS, Probe, R2L, and U2R,             | The model provides a low false alarm rate and high detection rate          | The increasing number of trees will slow the real-time prediction process  |
| Rao & Swathi, 2017 [20]       | KNN                | Accuracy, detection rate                               | NSL-KDD      | DoS, Probe, R2L, U2R, and normal      | The model was able to increase the accuracy and faster classification time | The authors did not consider the precision and recall rate.               |
| Khammassi & Krichen, 2017 [21]| Logistic Regression with Genetic Algorithm | Accuracy, detection rate, and false alarm rate         | UNSW-NB15    | DoS, U2R, R2L                         | The model provides high accuracy with only 20 features of UNSW-NB15 and 18 | Depending on KDD Cup99 may lead to misleading the evaluation as this     |
|                               |                    |                                                        | KDD Cup99    | features of KDD Cup99                 | features of KDD Cup99                                                     | dataset is outdated and contains redundant data                           |
| Verma & Ranga, 2018 [22]      | KNN and K-means    | Accuracy, detection rate, and false-positive rate      | CIDS-001     | Network traffic attacks                | The model provides the best performance of TP rate and low false alarm rate| The authors did not implement cross-validation to measure the robustness of |
| Hamed et al., 2018 [12]       | SVM with Recursive Feature Addition (RFA) | Accuracy, detection rate, and false alarm rate         | ISCX 2012    | Network traffic attacks                | Dealing with a large number of features and a small number of samples to  | The model ignores class distribution as it only works for binary          |
| Belouch et al., 2018 [23]     | SVM                | Accuracy, sensitivity, specificity, and execution time | UNSW-NB15    | Network traffic attacks                | avoid overfitting                                                         | classification.                                                           |

The classification was learned using deep learning methods such as AE, CNN, and RNN, with the greatest performance, obtained when utilizing CNN and LSTM, with an accuracy of 91.8% for 1D CNN classifiers and 90.1% for F-measure. However, their analysis was limited to a particular application, and because all features are equally essential, CNN and RNN lack a crucial evaluation function while still extracting features adequately.

An intelligent intrusion detection system was developed by [25] that combines deep learning algorithms with network virtualization to detect malicious behavior on IoT networks. Their technique enables efficient anomaly detection in IoT networks regarding scalability and interoperability by simulating and tracing five different attacks. Their model achieved a precision rate of 95% and a recall rate of 97% for various threat scenarios. However, as with many other IDS models, they emphasize detection rather than prevention techniques. Figure 8 illustrates the implementation of the deep learning model for IDS.

A deep learning classification model using NSL-KDD and KDD Cup99 was proposed in [26] to address increased human engagement and decreasing accuracy. The model was constructed using an unsupervised learning technique known as Non-symmetric Deep Autoencoder (NDAE). Their model required less training time than DBN and improved accuracy by 5% compared to pure Autoencoder, and is depicted in Figure 9. It consists of two NDAEs with three hidden layers each, and the two NDAEs are joined using an RF method. Their methodology, however, is ineffective in detecting complex attacks due to its high false alarm rate.

Convolutional neural networks with the NSL-KDD dataset were investigated in [28] and are depicted in Figure 10. In addition, the authors investigated a method for detecting threats in a vast real-time network by converting the raw

![FIGURE 8. Sample of IDS deep learning model.](image-url)
data to an image data format, which aids in resolving the unbalanced dataset issue by computing the cost function for each class from the training sample. As a result, they were able to reduce the number of computing parameters in their model, but their model’s accuracy was low compared to other machine learning and neural network models. Table 9 summarizes various deep learning algorithms for IDS.

In [27], a combination of CIC-IDS 2017, NSL-KDD, Kyoto, UNSW-NB15, and WSN-DS datasets was proposed to categorize and detect unplanned and unexpected cyberattacks using a deep neural network. The performance of this model was evaluated by comparing it to other machine learning classifiers, and their model outperformed the others. Similarly, in [2], the author suggested a deep neural network approach for classifying network data as harmful or benign. He supplemented his analysis with two more datasets: UNB-ISCX 2012 and CIC-IDS 2017. First, a feedforward Deep Neural Network was utilized for training the model, and then an Autoencoder was employed to categorize assaults and threats in the absence of tagged harmful data. Their model was 99.96% accurate for UNB-ISCX 2012 and 99.96% accurate for CIC-IDS 2017. Additionally, their research established the critical nature of the datasets needed to construct an IDS and the efficacy of Autoencoder for anomaly detection.

To enhance detection accuracy in IDS, the author incorporated big data, deep learning approaches, and natural language processing in [28]. They worked with KDD CUP99 and achieved an accuracy of 94.32% with their model. In addition, another deep neural network method was introduced in [29] to detect risks and attacks in the cloud environment. Their approach used Simulated Annealing and Improved Genetic Algorithms to create the hybrid optimization framework IGASAA using the datasets NSL-KDD2015, CIC-IDS2017, and CIDDS-001. Compared to the Simulated Annealing Algorithm (SAA), their model demonstrated a higher detection rate, increased accuracy, and a lower false alarm rate.

Web application security is highly reliant on detecting malicious HTTP traffic, which needs a significant investment in training data gathering and a large dataset. To detect malicious HTTP traffic, the authors in [29] introduced the DeepPTSD method based on a deep transfer semi-supervised learning methodology. The construction of their model is given in Figure 11. They used two raw public datasets from FSecurity and another from their lab via a honeypot server. When a little training dataset is available, their model exceeds other existing baselines, with a precision of 93.33% compared to 86.67% and 86.61% for CNN and RNN, respectively.

An intrusion detection model based on a convolutional neural network was presented in [30] to extract structural information. The authors performed multiclassification on NIDS using the NSL-KDD and KDD-CUP99 datasets. Their model’s accuracy increased compared to other classifiers, resulting in enhanced detection of unknown threats and a decrease in false alert rates. A feedforward deep neural network was proposed by [1] for an intrusion detection system to perform binary classification on the NSL-KDD dataset. Due to the dense structure of this model, it beat the usual machine-learning technique in terms of scalability with big datasets and time for training data. As a result, there was
TABLE 9. Deep learning algorithms for IDS.

| Author          | Learning algorithm | Performance metrics                                      | Dataset       | Attack targeted                        | Strengths                                                                                                                                  | Limitation                                                                 |
|-----------------|--------------------|----------------------------------------------------------|---------------|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Xiao et al., 2019 [33] | CNN                | Accuracy, detection rate, and false alarm rate           | KDD CUP99     | DoS, Probe, R2L, U2R, and normal       | The model provides a short classification time for real-time traffic and high accuracy                                                   | R2L and U2R have a low detection rate compared to other attacks              |
| Papamartzivas et al., 2019 [34] | Autoencoder       | Accuracy, precision, recall, F1-score                    | KDD CUP99, NSL-KDD | DoS, Probe, R2L, U2R, and normal       | The model provides autonomous misuse detection for large scale networks                                                               | Low detection accuracy for U2R and R2L attacks                                |
| Mayuranathan et al., 2019 [35] | RBM                | Accuracy, detection rate, precision, and recall          | KDD CUP99     | DoS and DDoS in the cloud environment   | By using feature selection, the model improved the performance of detecting attacks                                                     | High computational resources for IoT devices                                  |
| Jiang et al., 2020 [36]     | LSTM-RNN           | Accuracy, detection rate, and false alarm rate           | NSL-KDD       | Network traffic attacks                | The model outperformed the accuracy of other machine learning algorithms                                                              | The model does not detect new types of attacks                                |
| Tian et al., 2020 [37]       | DBN                | Accuracy, F1-score, precision, recall, and false-positive rate | NSL-KDD, UNSW-NB15 | Network traffic attacks                | The model is robust and provides a low false alarm rate                                                                              | The accuracy of the model may be affected due to the uncertainty of selecting parameters |
| Zhang et al., 2020 [38]       | CNN MLP C-LSTM    | Accuracy, F1-score, precision, and recall                | CSE-CIC-IDS2018 | NES Boundary HopSkipFlu                  | The model provides a high detection rate                                                                                              | The model was vulnerable against adversarial instances                         |

Deep learning algorithms were used in [32] to investigate the applicability of anomaly-based intrusion detection systems. Based on the NSL-KDD dataset, the authors studied a variety of machine learning and deep learning frameworks. According to the comparison, deep learning outperformed machine learning in the accuracy test. The best performance was first achieved by the RNN, then by the CNN, and finally by the Autoencoder. A comparison of deep learning methods based on intrusion detection systems is presented in Table 9, which compares the learning algorithm, performance metric, dataset, attack targeted, strengths, and limits of the algorithms.

C. HYBRID LEARNING IDS ALGORITHM

This section discusses works that combine machine learning and deep learning or use many algorithms of the same learning type. First, a deep learning-based intrusion detection system for an IoT network was developed in [39]. By providing a model based on Gated Recurrent Neural Networks (GRU and LSTM), their detection dataset was KDD99 cup.

They proposed adding deep learning classifiers to each TCP/IP architecture layer to increase its complexity. The model’s accuracy was 98.91%, and the false alarm rate was 0.76%. However, one may argue that the model’s robustness was low.

Hierarchical Intrusion Detection System (HAST-IDS) was developed in [40] to improve anomaly detection. As illustrated in Figure 13, they began by extracting spatial features using CNN and then temporal characteristics using LSTM. Finally, they evaluated the performance of their proposed model using the ISCX2012 and DARPA datasets. Although the hierarchical CNN-LSTM model beats pure CNN or LSTM models and gives higher accuracy for IDS, it is computationally expensive because of its complicated architecture.
TABLE 10. Hybrid learning algorithms for IDS.

| Author                | Learning algorithm                       | Performance metrics         | Dataset          | Attack targeted             | Strengths                                      | Limitation                                      |
|-----------------------|------------------------------------------|----------------------------|------------------|----------------------------|------------------------------------------------|------------------------------------------------|
| Yang et al., 2017 [48]| SVM and RBM                              | F1-score and precision      | Real online traffic | Network traffic attacks     | The model increased training speed and improved traffic detection | F1-score for some training sizes had a high false-negative rate |
| Yang et al., 2019 [49]| DBN with density peak clustering algorithm| Accuracy, recall, precision and F1-score | UNSW-NB15 NSL-KDD | Network traffic attacks     | The model outperformed other algorithms in accuracy and detection rate | The performance may be affected because the model was not able to learn low-level feature representations |
| Zhang et al., 2019 [50]| Genetic algorithm and DBN                 | Accuracy, detection rate, precision, recall and false alarm rate | NSL-KDD           | IoT network layer           | The model was able to select the optimal parameters to be trained | The model needs more time for training the dataset |
| Rajagopal et al., 2020 [51]| SVM, RF, L.R, and KNN                   | Accuracy, precision, recall, false alarm rate | UNSW-NB15 UGR'16 | Blacklist Spam Scan SSHscan UDPScan DOS DDOS | The combined algorithms increased the accuracy and detection rate | Evaluate a new dataset that contains recent attacks, and their work only focuses on the classifiers, not metadata |

D2H-IDS [41] is an intrusion detection system that was developed to ensure the security of connections between connected smart vehicles. This model is built on a framework for continuous automated secure service availability and utilizes a decision tree and deep belief network to classify attacks and reduce their dimensionality.

Security attacks in smart connected vehicles an intrusion detection system based on continuous automated secure service availability framework was proposed in [41]. The model classifies attacks and reduces their dimensionality using a decision tree and deep belief machine learning. A model for enhancing IDS performance was provided by [42] by integrating three classifiers with big data. The methods utilized were a combination of machine learning and deep learning techniques, including Random Forest (RF), Deep Neural Network (DNN), and Gradient Boosting Tree (GBT). The authors evaluated their strategy using the CIC-IDS2017 and UNSW-NB15 datasets. DNN has the highest accuracy at 99.19% based on UNSW-NB15 and 99.99% based on CIC-IDS2017. Although all three classifiers achieved good accuracy, training the model was difficult due to the features’ wide variety of numerical data.

In wireless sensor networks, IDS was performed using a combination of machine learning and deep learning [43]. The authors proposed the Restricted Boltzmann machine-based clustered RBC-IDS approach as a deep learning technique. They used the KDD Cup99 dataset and Network Simulator-3 to compare their model against adaptive machine learning-based IDS (NS-3). While RBC-IDS has high accuracy, the detection time was comparable to that of the adaptive machine learning model, resulting in overhead expenses. A hybrid network IDS was utilized in [6] using the UNSW-15 dataset that utilized the CNN-LSTM algorithm. When applied to real-world devices, they employed a transfer learning approach to optimize the IDS model’s efficiency. Their model was 98.43% accurate.

CBR-CNN (Channel Boosted and Residual Learning) was created in [44], employing deep Convolutional Neural Networks for intrusion detection using the NSL-KDD dataset. Training is carried out using an unsupervised learning approach, and normal traffic is modeled using stacked autoencoders (SAE). Their model had an accuracy of 89.41% for KDD-Test+ and 80.36% for KDD-Test-21, respectively. Table 10 analyses the learning method, performance metric, dataset, attack type, strengths, and limits of hybrid learning algorithms based on intrusion detection systems.

D. DISCUSSION AND OPEN CHALLENGES

Intrusion detection systems are now considered a necessary component of our daily lives. However, developing an intrusion detection system capable of detecting and...
responding to a wide range of attacks and threats is a difficult task. As a result, hundreds of studies in the field of intrusion detection systems have been carried out for various applications by academic researchers. Some academics believe that deep learning, through a neural network, will enable greater flexibility in IDS, allowing it to detect and classify harmful threats more effectively. This flexibility is because its algorithms have hidden layers with a high-dimensional feature representation of the data.

A comprehensive assessment of network-based intrusion detection systems was offered in [10], in which they stressed the need for labeling data when doing evaluation and training on anomaly-based intrusion detection systems. Moreover, in [45], the author investigated the possibility of improving model optimization, and they concluded that the supervised learning approach is more successful than the unsupervised learning approach. After all, it can achieve higher performance in terms of the algorithms used because it uses labeled data to train the models. NADS implementation with various applications, data centers, fog, cloud computing, and the Internet of Things (IoT) was a priority [13].

The authors asserted that datasets not based on reality might result in mistaken studies in their conclusions. Employing ESR-NID computation approaches, they provided in [45] a model for searching for a solution to automatically generate rulesets for network intrusion detection by using computation techniques (Evolving Statistical Rulesets for Network Intrusion Detection). The model outperforms other existing models and is capable of dealing with a variety of various types of attacks.

To summarize, some researchers were concentrating on whatever algorithm would provide the best performance, such as [14], [15], [21]–[23], [33], [39]. A comparison between different types of algorithms used for IDS is presented in Table 11, in terms of the learning approach, advantages, and disadvantages.

As a means of increasing accuracy and improving model implementation, some researchers investigated combining algorithms in order to achieve higher accuracy or a lower false alarm rate, as in [40], [41], while others combined methods in machine learning and deep learning, as in [43], [44], [46]. Some researchers experimented to see which dataset could provide a more stable model,
as in [15], [21], [25], [35], [38], [43], while others created their dataset to use in IDS development, as in [17], [24], [47]. Each dataset contains a different range of threats and attacks, so some researchers experimented to see which dataset could provide a more stable model.

The intrusion detection system field has many challenges, represented by:

1) UNAVAILABILITY OF UP-TO-DATE DATASET
A highly effective IDS must be trained and tested against a dataset of new and old threats and attacks. When more patterns and types of attacks are discovered in a dataset, the model becomes more resistant to various attack types. Thus, one of the challenges for IDS is to maintain an up-to-date dataset with sufficient records to cover the majority of attack types.

2) HYPERPARAMETER TUNING
The deep structure of an IDS model requires that the hyper-parameters be specified. The activation function and optimization method, the number of nodes per layer, and the total number of layers in a network are all hyperparameters. Hyperparameters affect training and model building, with the ability to increase or decrease the IDS model’s accuracy and detection rate. Hyperparameters can be tuned manually, which will take a significant amount of time, or automated to improve the performance of the IDS model.

3) IMBALANCED DATASET
Existing datasets contain varying numbers of records for various types of attacks. These differences will affect the accuracy and detection rate of various types of attacks. A low-record attack will have a lower detection rate than a high-record attack. This issue can be resolved by either balancing the dataset or by increasing the number of minority attack records.

4) PERFORMANCE IN REAL-WORLD
When researchers attempt to develop an intrusion detection system, they train and test the model in laboratories, with the majority of the data coming from public sources. Thus, an IDS model faces a challenge when it is implemented in a real-world environment, as the model developed in the lab should be validated in a real-world environment to ensure its efficiency.

V. CONCLUSION
One of the essential subjects in the cybersecurity area was intrusion detection systems. Many researchers are developing a system that will secure data against malicious conduct. However, research into other applications of learning algorithms, such as establishing a new dataset or merging algorithms, is currently ongoing. As a result, we explain the concept of an intrusion detection system, types of attacks, and how to determine whether or not we have an effective system in this work.

Selecting a good dataset to train and test an intrusion detection system is a crucial parameter, and it was clear that datasets have an impact on research in this sector, as some deem it out of date or contains redundant information. As a result, the most frequent datasets used to detect threats over the last decade are compared in the research.

The final step in this project was to look into what other people did to save their data. Recent research has revealed that there are numerous data protection implementations. They employed machine learning for several purposes at first, and many studies were conducted to determine which algorithm would provide higher accuracy or which datasets would produce a lower false alarm rate. Finally, they arrived at deep learning after extensive investigation and testing. Many studies and experiments have shown that deep learning is superior to machine learning because it can handle more complicated problems with greater accuracy and lower false alarm rates. Previous work has been used in a variety of applications. They employed various datasets, architectures, learning methodologies, and learning algorithms to secure data from attacks and dangers each time.

REFERENCES
[1] D. I. Edeh, “Network intrusion detection system using deep learning technique,” M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, 2021.
[2] G. C. Fernandez, “Deep learning approaches for network intrusion detection,” M.S. thesis, Dept. Comput. Sci., Univ. Texas at San Antonio, San Antonio, TX, USA, 2019.
[3] H. Benmeziane, “Comparison of deep learning frameworks and compilers,” M.S. thesis Comput. Sci., Inst. Nat. Formation Informatique, École nationale Supérieure d’Informatique, Oued Smar, Algeria, 2020.
[4] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, and M. Gao, “Machine learning and deep learning methods for cybersecurity,” IEEE Access, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.
[5] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
[6] H. Dhillon, “Building effective network security frameworks using deep transfer learning techniques,” M.S. thesis, Dept. Comput. Sci., Western Univ., London, ON, Canada, 2021.
[7] M. Labonne, “Anomaly-based network intrusion detection using machine learning,” Ph.D. dissertation, Inst. Polytechnique de Paris, Palaiseau, France, 2020.
[8] A. Kim, M. Park, and D. H. Lee, “AI-IDS: Application of deep learning to real-time web intrusion detection,” IEEE Access, vol. 8, pp. 70245–70261, 2020.
[9] P. Wu, “Deep learning for network intrusion detection: Attack recognition with computational intelligence,” M.S. thesis, School Comput. Sci. Eng., Univ. New South Wales, Sydney NSW, Australia, 2020.
[10] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, “A survey of network-based intrusion detection data sets,” Comput. Secur., vol. 86, pp. 147–167, Sep. 2019.
[11] M. Alkasasseh and M. Almsheidin, “Machine learning methods for network intrusion detection,” 2018, arXiv:1809.02610.
[12] T. Hamed, R. Dara, and S. C. Kremer, “Network intrusion detection system based on recursive feature addition and bigram technique,” Comput. Secur., vol. 73, pp. 137–155, Mar. 2018.
[13] N. Moustafa, J. Hu, and J. Slay, “A holistic review of network anomaly detection systems: A comprehensive survey,” J. Netw. Comput. Appl., vol. 128, pp. 33–55, Feb. 2019.
[14] L. Amroth and J. Fiddler Dennis, “Supervised learning techniques: A comparison of the random forest and the support vector machine,” Uppsala Univ., Uppsala, Sweden, 2016.
[15] D. H. Lakshminarayana, “Intrusion detection using machine learning algorithms,” M.S. thesis, Dept. Comput. Sci., East Carolina Univ., Greenville, NC, USA, 2019.
[16] J. Gu, L. Wang, H. Wang, and S. Wang, “A novel approach to intrusion detection using SVM ensemble with feature augmentation,” Comput. Secur., vol. 86, pp. 53–62, Sep. 2019.

[17] I. Homoliak, K. Malinka, and P. Hanacek, “ASNM datasets: A collection of network attacks for testing of adversarial classifiers and intrusion detectors,” IEEE Access, vol. 8, pp. 112427–112453, 2020, doi: 10.1109/ACCESS.2020.3001768.

[18] A. Shenfiel, D. Day, and A. Ayesh, “Intelligent intrusion detection systems using artificial neural networks,” IET Exp., vol. 4, no. 2, pp. 95–99, Jun. 2018.

[19] N. Farmaaz and M. A. Jabbar, “Random forest modeling for network intrusion detection system,” Proc. Comput. Sci., vol. 89, pp. 213–217, May 2016.

[20] B. B. Rao and K. Swathi, “Fast KNNS classifiers for network intrusion detection system,” Indian J. Sci. Technol., vol. 10, no. 14, pp. 1–10, Apr. 2017.

[21] C. Khammassi and S. Krichen, “A GA-LR wrapper approach for feature selection in network intrusion detection,” Comput. Secur., vol. 70, pp. 255–277, Sep. 2017.

[22] A. Verma and V. Ranga, “Statistical analysis of CIDDS-001 dataset for network intrusion detection systems using distance-based machine learning,” Proc. Comput. Sci., vol. 125, pp. 709–716, Jan. 2018.

[23] M. Belouch, S. El Hadaj, and M. Idhammad, “Performance evaluation of intrusion detection based on machine learning using apache spark,” Proc. Comput. Sci., vol. 127, pp. 1–6, Jan. 2018.

[24] X. Wang, S. Chen, and J. Su, “Real world traffic collection and deep learning for mobile app identification,” Wireless Commun. Mobile Comput., vol. 2020, pp. 1–14, Feb. 2020, doi: 10.1155/2020/4707909.

[25] G. Thamilarasu and S. Chawla, “Towards deep-learning-driven intrusion detection for the Internet of Things,” Sensors, vol. 19, no. 9, p. 1977, Apr. 2019, doi: 10.3390/s19091977.

[26] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A deep learning approach to network intrusion detection,” IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018.

[27] R. Vinayakumar, M. Alazab, K. Soman, P. Poomanchandran, A. Al-Nemrat, and S. Venkatraman, “Deep learning approach for intelligent intrusion detection system,” IEEE Access, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[28] Y. Dong, R. Wang, and J. He, “Real-time network intrusion detection system based on deep learning,” in Proc. IEEE 10th Int. Conf. Softw. Eng. Service Sci. (ICSESS), Oct. 2019, pp. 1–4.

[29] T. Chen, Y. Chen, M. Lv, G. He, T. Zhu, T. Wang, and Z. Wang, “A payload based malicious HTTP traffic detection method using transfer semi-supervised learning,” Appl. Sci., vol. 11, no. 6, p. 7188, 2021, doi: 10.3390/app11067188.

[30] G. Liu and J. Zhang, “CNID: Research of network intrusion detection based on convolutional neural network,” Discrete Dyn. Nature Soc., vol. 2020, pp. 1–11, May 2020.

[31] C. Yin, Y. Zhu, J. Fei, and X. He, “A deep learning approach for intrusion detection using recurrent neural networks,” IEEE Access, vol. 5, pp. 21954–21961, 2017.

[32] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, and J. Han, “Enhanced network anomaly detection based on deep neural networks,” IEEE Access, vol. 6, pp. 48231–48426, 2018, doi: 10.1109/ACCESS.2018.2860306.

[33] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, “An intrusion detection model based on feature reduction and convolutional neural networks,” IEEE Access, vol. 7, pp. 42210–42219, 2019.

[34] D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, “Introducing deep learning self-adaptive misuse network intrusion detection systems,” IEEE Access, vol. 7, pp. 13546–13560, 2019.

[35] M. Mayuranathan, M. Murugan, and V. Dhanakoti, “Best features based intrusion detection system by RBM model for detecting DDOS in cloud environment,” J. Ambient Intell. Hum. Comput., vol. 12, no. 3, pp. 3609–3619, 2019.

[36] F. Jiang, Y. Fu, B. B. Gupta, Y. Liang, S. Rho, F. Lou, F. Meng, and Z. Tian, “Deep learning based multi-channel intelligent attack detection for data security,” IEEE Trans. Sustain. Comput., vol. 5, no. 2, pp. 204–212, Apr. 2020.

[37] Q. Tian, D. Han, K.-C. Li, X. Liu, L. Duan, and A. Castiglione, “An intrusion detection approach based on improved deep belief network,” Appl. Intell., vol. 50, pp. 3162–3178, May 2020.

[38] C. Zhang, X. Costa-Pérez, and F. Patras, “Tiki-taka: Attacking and defending deep learning-based intrusion detection systems,” in Proc. ACM SIGSAC Conf. Cloud Comput. Secur. Workshop, 2020, pp. 27–39.

[39] M. K. Putchala, “Deep learning approach for intrusion detection system (IDS) in the Internet of Things (IoT) network using gated recurrent neural networks (GRU),” M.S. thesis, Dept. Comput. Sci. Eng., Wright State Univ., Dayton, OH, USA, 2017.

[40] W. Wang, Y. Sheng, J. Wang, X. Zeng, and X. Ye, “HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection,” IEEE Access, vol. 6, pp. 1792–1806, 2018.

[41] M. Aloqaily, S. Otoun, J. A. Rialdawi, and Y. Jaraaweh, “An intrusion detection system for connected vehicles in smart cities,” Ad Hoc Netw., vol. 90, Jul. 2019, Art. no. 101842, doi: 10.1016/j.adhoc.2019.02.001.

[42] O. Faker and E. Dogdu, “Intrusion detection using big data and deep learning techniques,” presented at the ACM Southeast Conf., 2019.

[43] S. Otoun, B. Kantarci, and H. T. Moeufah, “On the feasibility of deep learning in sensor network intrusion detection,” IEEE Netw. Lett., vol. 1, no. 2, pp. 68–71, Jun. 2019, doi: 10.1109/LNET.2019.2901792.

[44] N. Chouhan, A. Khan, and H.-U.-R. Khan, “Network anomaly detection using channel boosted and residual learning based deep convolutional neural network,” Appl. Soft Comput., vol. 83, Oct. 2019, Art. no. 105612, doi: 10.1016/j.asoc.2019.105612.

[45] S. Rastegari, “Intelligent network intrusion detection using an evolutionary computation approach,” Ph.D. dissertation, School Comput. Secur., Edith Cowan Univ., Joondalup WA, Australia, 2015.

[46] J. Yang, J. Deng, S. Li, and Y. Hao, “Improved traffic detection with support vector machine based on restricted Boltzmann machine,” Soft Comput., vol. 21, no. 11, pp. 3101–3112, 2017.

[47] N. Chabouni, “Intrusion detection and prevention for IoT systems using machine learning,” Ph.D. dissertation, School Math. Comput. Sci., Université de Bordeaux, Bordeaux, France, 2020.

ASMAA HALBOUNI (Graduate Student Member, IEEE) received the bachelor’s degree in telecommunication engineering from An-Najah National University, Palestine. She is currently pursuing the M.S. degree in computer and information engineering with International Islamic University Malaysia, Malaysia. Her research interests include intrusion detection, network security, and deep learning.

TEDDY SURYA GUNAWAN (Senior Member, IEEE) received the B.Eng. degree (cum laude) in electrical engineering from the Institut Teknologi Bandung (ITB), Indonesia, in 1998, the M.Eng. degree from the School of Computer Engineering, Nanyang Technological University, Singapore, in 2001, and the Ph.D. degree from the School of Electrical Engineering and Telecommunications, The University of New South Wales, Australia, in 2007.

He was the Head of the Department of Electrical and Computer Engineering, from 2015 to 2016, and the Head of Programme Accreditation and Quality Assurance with the Faculty of Engineering, International Islamic University Malaysia, from 2017 to 2018. He has been a Charter Professor at UET, U.K., since 2016, an Insinyur Professional Utaama at PII, Indonesia, since 2021, and a Registered ASEAN Engineer, since 2018. He has been a Professor, since 2019, and has been an ASEAN Chartered Professional Engineer, since 2020. His research interests include speech and audio processing, biomedical signal processing and instrumentation, image and video processing, and parallel computing. He was awarded the Best Researcher Award at IJUM, in 2018. He was the Chairperson of IEEE Instrumentation and Measurement Society—Malaysia Section, in 2013, 2014, 2021, and 2022.
MOHAMED HADI HABAEBI (Senior Member, IEEE) is currently a Professor with the Department of Electrical and Computer Engineering, International Islamic University Malaysia (IIUM). His research interests include the IoT, mobile app development, networking, blockchain, AI applications in image processing, cyber-physical security, wireless communications, small antennas, and channel propagation modeling.

MURAD HALBOUNI received the bachelor’s degree in telecommunication engineering from Palestine Technical University, Kadoorie, Palestine. He is currently pursuing the M.S. degree in cyber crime with Arab American University, Palestine. His research interests include cybercrime and digital evidence analysis, metro networks, network security, and machine learning. He also works at Paltel, a Palestinian communication business, as a Network Engineer.

MIRA KARTIWI (Member, IEEE) is currently a Professor with the Department of Information Systems, Kulliyyah of Information and Communication Technology, and currently the Deputy Director of E-Learning with the Centre for Professional Development, International Islamic University Malaysia (IIUM). She was one of the recipients of the Australia Postgraduate Award (APA), in 2004. For her achievement in research, she was awarded the Higher Degree Research Award for Excellence, in 2007. She has also been appointed as an Editorial Board Member in local and international journals to acknowledge her expertise. She is also an experienced consultant specializing in the health, financial, and manufacturing sectors. Her research interests include health informatics, e-commerce, data mining, information systems strategy, business process improvement, product development, marketing, delivery strategy, workshop facilitation, training, and communications.

ROBIAH AHMAD (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Evansville, Evansville, IN, USA, the M.Sc. degree in information technology for manufacturer from the Warwick Manufacturing Group, University of Warwick, U.K., and the Ph.D. degree in mechanical engineering from University Teknologi Malaysia, Malaysia. She is currently an Associate Professor with the Razak Faculty of Technology and Informatics, UTM, Kuala Lumpur, Malaysia. She has more than 20 years experience as a Research Scientist. She has published more than 100 peer-reviewed international journal articles/proceedings in areas of instrumentation and control, system modeling and identification, and evolutionary computation. She currently holds a position as an executive committee for Humanitarian Activities for IEEE Malaysia Section and the Past Chair for IEEE Instrumentation and Measurement Society Malaysia Chapter.

* * *