Journal of Intelligent Systems and Internet of Things
Vol. 14, No. 01, PP. 278-292, 2025
DOI: https://doi.org/10.54216/JISIoT.140122

Adaptive FPGA-Based Intrusion Detection System for Real-Time Internet of Things Security

Israa Ali Al-Neami[1,*], Zaynab Saeed Hameed[1], Zahraa Abbas Al-zubaydi[1]

[1]Department of Computer Engineering, University of Technology, Baghdad, Iraq
Emails: Israa.A.AlShaikhli@uotechnology.edu.iq; zaynab.s.hameed@uotechnology.edu.iq; Zahraa.A.Alzubydi@uotechnology.edu.iq

Abstract

The rapidly evolving landscape of cyber threats demands robust and adaptive Intrusion Detection Systems (IDS) capable of real-time operation. This paper presents a novel approach to augmenting Field-Programmable Gate Arrays (FPGA) for the development of a high-performance IDS designed to enhance communication security by rapidly and accurately identifying threats. The proposed system integrates advanced techniques, including Meta Ensemble Learning (MEL), Extreme Gradient Boosting (XGBoost), and a Hybrid Deep Learning (HDL) model that combines Long Short-Term Memory (LSTM) networks for temporal analysis and Convolutional Neural Networks (CNN) for feature extraction. This synergistic approach significantly reduces detection latency and improves the accuracy of threat identification. The effectiveness of the FPGA-based IDS is evaluated using four widely recognized datasets—NSL-KDD, IoTID20, CICIDS2017, and UNSW NB15—all of which focus on communication attacks, making them ideal for testing IDS performance in diverse IoT environments. The results demonstrate that the proposed IDS not only achieves a high detection rate with a low false positive rate but also operates efficiently in real-time settings, underscoring its viability as a critical security solution in data communication networks. Moreover, the system's exceptional performance in securing IoT devices, which are frequently targeted due to their ubiquity and vulnerabilities, highlights its potential as a reliable and scalable security measure. The FPGA-based IDS offers a significant contribution to the field by providing a rapid, accurate, and real-time security solution that addresses the pressing need for effective threat detection and prevention in modern communication networks.

Received: February 25, 2024 Revised: May 07, 2024 Accepted: July 28, 2024

Keywords: Machine Learning; Network; Security; Data communication; Intrusion detection

1. Introduction

Large organizations and businesses rely on data communication in this era, and without IDSs or intrusion detection systems, protecting these networked systems from malicious activities is impossible [1]. Today, cybersecurity issues are evolving and escalating, making it more difficult to prevent external interlopers from interfering with a company's information communication. While more traditional measures such as firewalls and antivirus are still useful, they are not sufficient to address the more intricate forms of cyber threats. Developers developed IDS to constantly monitor network activity, detect security threats, and promptly respond [2]. IDS can be classified in regards to the configuration and operation as well as the method of network Intrusion Detection Systems (NIDS) operate across all communication sections, analyzing packet data to identify any anomalies, while Human Intrusion Detection Systems (HIDS) operate by analyzing system logging data and the application data of individual devices [3,4]. There are two primary detection methods: two types of intrusion detection systems (IDSs). We classify IDSs into two types: signature-based and anomaly-based. While signature-based detection detects known threats, the anomaly-based approach focuses on the development of behaviour information. As shown in Figure 1 [4], signature-based IDS are effective against known threats but struggle with zero-day attacks and novel intrusion techniques. In contrast, anomaly-based IDS can detect previously unknown threats but often result in more false

positives [5]. Advancements in machine learning and artificial intelligence have significantly enhanced IDS capabilities. Machine learning algorithms, particularly deep learning models, can analyze vast amounts of network data, identifying complex patterns indicative of malicious activity [6]. Deep neural networks, such as convolutional neural networks (CNNs) and long-short-term memory (LSTM) networks, have the potential to improve the accuracy and speed of attack detection. These models can autonomously learn and adapt to emerging threats, enhancing network security's robustness and scalability. Recent research indicates that combining various machine-learning approaches can optimize IDS performance [7,8]. New methods are always being developed, such as transformer-based transfer learning for uneven network traffic and machine learning-based feature selection for intrusion detection. These enhancements address the evolving and increasingly sophisticated nature of online threats. This paper contributes to this ongoing effort by presenting an FPGA-based IDS designed for real-time network protection. By leveraging the Meta Ensemble Learning model, Extreme Gradient Boosting, and a hybrid deep learning model combining CNNs and LSTM networks, we aim to provide a comprehensive solution for intrusion detection. This approach is particularly effective in securing IoT devices, which are vulnerable due to their widespread deployment and limited computational resources. We have tested our approach on various communication environments, including UNSW NB15, CICIDS2017, IoTID20, and NSL-KDD, ensuring a thorough evaluation. Particularly, the applicability of this model to IoT security is highlighted because IoT is considered a very vulnerable domain for cyber threats. IoT is relatively more exposed to vulnerabilities compared to computerized conventional establishments, which afford distinctive protection. Through this IDS that will use an FPGA, the system can efficiently detect threats appropriate for IoT networks to improve the security of connected IoT devices and guarantee the sanctity of their communications [9,10]. This study advances the development of more effective and adaptable IDS in the face of ever-evolving cyber threats.

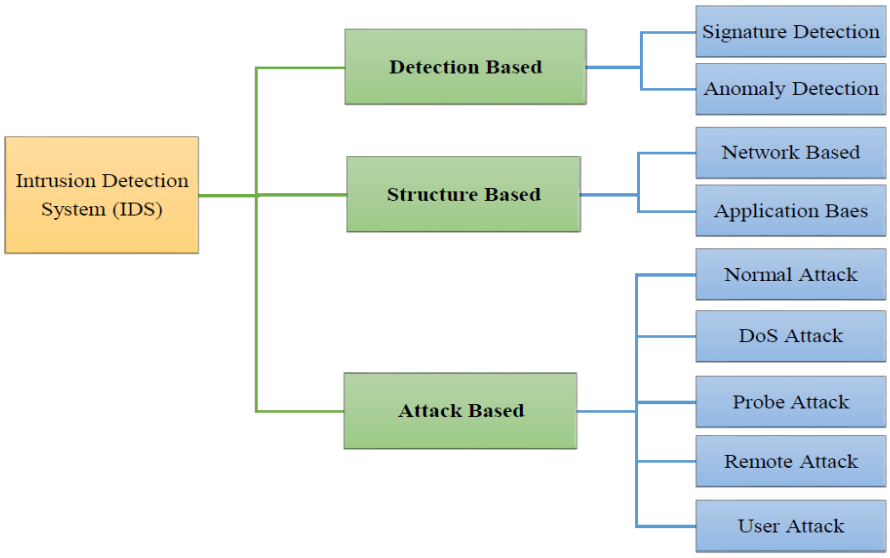

Figure 1. Intrusion detection system classification [4]

2. Literature Review

IDS are used to prevent undesirable persons and objects from entering the communication and intercepting or disrupting the network's functions. As technology has progressed and threats become more intricate, IDS have integrated artificial intelligence and more recently, machine learning and deep learning into the IDS platform to improve the IDS analysis capabilities of threats. The development of the accurate and efficient IDS models has emerged as the area of significant concern in the most recent times due to the increased complexity of the threats in the cyber security domain. In [11] proposed the Multi Support Vector Machine (M-SVM), which is approved feature selection based network intrusion detection system with machine learning method. Regarding the second research question, the study aimed at enhancing the accuracy and performance of IDS by developing an integrated model that incorporates feature selection with support vector machines. The main goal of this method is to decrease the dimensionality of the option set, thereby improving the IDS efficiency in terms of the detection time and the percentage of accurate interpretations. The researchers showed the superiority of M-SVM over a conventional model of SVM in terms of both speed and performance when applied on large and compound databases.

Discussed use of machine learning techniques for efficient intrusion detection system in wireless sensor networks (WSNs). This was the area that they have aimed at to target and improve the IDS which they established for the WSNs and which is characterized with such constraints as for example limited computational power and energy.

Intrusion is detected in the proposed system since the system relies on machine learning algorithms to analyse the pattern of communication traffic to isolate invaders. In their study, they noted that the methods they used to improve the security of WSNs were efficient and did not have adverse effects on the performance of nodes under test [12].

In [13] 'fast intrusion detection system through swift wrapper feature selection and speedy ensemble classifier. ' The IDS of this research was categorized under low-interaction IDS for it aims at identifying intrusions within a short time more effectively by selecting powerful features to boost the performance of the ensemble learning. The features of the swift wrapper method involved the reduction of computation by feature selection while the ensemble classifier improved the detection accurate by using several learning models. A new approach is proposed in the form of a composite deep learning model. This study was focused on the existing security threats of IoT networks and in this research we intended to design an efficient IDS by using the features of deep learning. In the present work, a unique hybrid approach, namely CNN-LSTM is utilized to learn spatio-temporal features of the network traffic. This makes the approach effectively used in the detection of intricate intrusion patterns that are characteristic of IoT devices as depicted by figure 2 [14]. Deep learning based network intrusion detection system called Dugat-LSTM in [15,16] which uses a chaotic optimization. This study aimed at improving IDS in terms of the ability to detect anomalies using LSTM networks and optimizing the weights of the neural networks using a chaotic optimization algorithm. This approach was applied to enhance the LSTM model performance in detecting intrusions based on a set of hyperparameters. The random training approach used in the paper guarantees the correct training of the model, given the highly dynamic and random nature of network traffic data where the model is supposed to discover simple yet easily-overlooked patterns that signify malicious activity. Conducted experiments using untargeted white-box adversarial attack and heuristic-based defense on real-time DL-based NID systems. In this research work, the objective was to identify some of the weaknesses that are prevalent in deep learning-based IDS, while concurrently designing some measures that can effectively counter these threats. Through undertaking this research, the researchers developed a heuristic defense strategy that not only provides a balancing defense to the IDS but also increases its reliability in practical contexts [17].

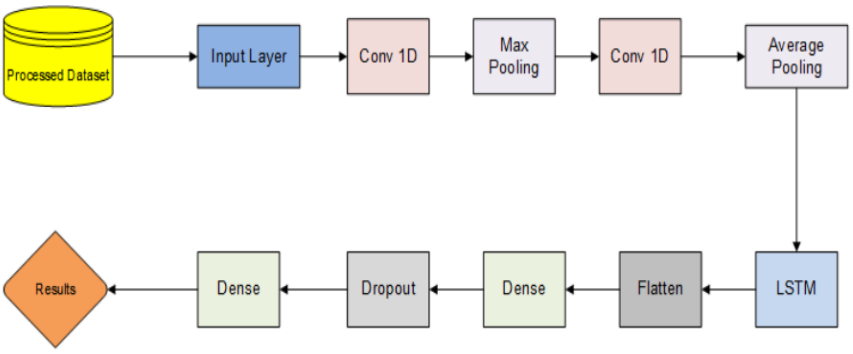

Figure 2. Hybrid Deep Learning Algorithm for Intrusion Detection [14].

A new IDS model for the smart agriculture context and its specific characteristics in terms of cybersecurity. The authors present a downsized kernel method designed to improve the IDS's performance although reducing amount time required for the computation without the detriment of results quality. In order to deal with tremendous increase in data complexity, heterogeneity, and real time threat identification considerations in smart agriculture environments (SMAC), the system is designed [18]. Enhanced Distributed Intrusion Detection System (E-DIDS) This system helps in evaluation of the attacks that the Unmanned Aerial Vehicle (UAVs) are undergoing and also is a perfect means of check and balance to make sure that security measures are in proper place. Given the structure of UAV networks single site solutions are not practical in detecting threats to the network hence the E-DIDS model is a distributed system using multiple E-DIDS agents to efficiently identify threats. This is believed to assist in providing adequate and effective safety measures for UAV operations given the new generation problems facing unmanned aerial vehicles where those performing cyber-crimes are using advanced tools [19]. Novel, fast and efficient intrusion detection system (IDS) for Vehicular Ad-Hoc Networks (VANETs) based on federated learning. This approach takes advantage of the FL approach of training a model locally on multiple vehicles' data without necessitating the storage of data centrally to boost the IDS's capacity to identify intrusions on the targeted system. The given system can be useful in offering a measurable and effective security model to VANETs to protect data privacy and decrease call overhead [20]. Mining of attacks on WSNs for enhanced security through an intrusion detection system based on machine learning with Stochastic Gradient Descent (SGD). This proposed system is tailored into conquering those factors and challenges that are specific to WSNs as illustrate in figure 3 such as; minimal computational power and energy conservation [16].

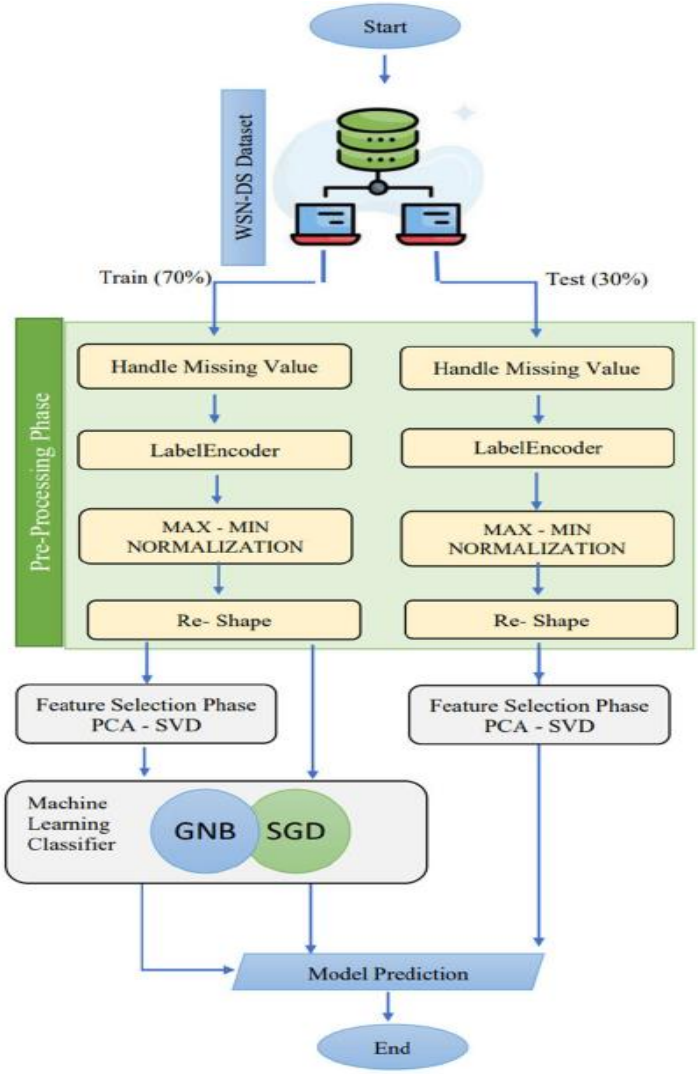

Figure 3. SGD Intrusions Detection for Wireless Sensor Network Attack Detection System [16]

In [21] put forward Similarity-Based Intrusion Detection for Controller Area Network (CAN) using Improved Levenshtein Distance and N-gram Analysis (SIDiLDNG) which is a new method for CAN using Similarity Based Intrusion Detection based on Improved Levenshtein Distance and N-gram analysis. The CAN traffic is supposed to be monitored for signs of an anomalous state within the system by comparing the new messages to what the system already knows and is expecting. The advanced option like Levenshtein Distance and N-gram Analysis will help the system to decide about the presence of intrusion in a better way by identifying small nuances. The examples of IDS in [22] demonstrating a network intrusion detection system (IDS) that employs deep learning. This work aims at analysing how various forms of deep learning models, with regard to CNNs and Recurrent Neural Network (RNNs), will help in making the process of identifying these attacks more efficient and accurate. Basically, the deep learning models are trained the network traffic data to show them what kind of behavioral patterns can be attributed to being bad. Propose an Immune System-based Intrusion Detection System (IS-IDS) that would identify attacks in a network using methods analogous to the human immune system. There is immune memory, self/non-self-discrimination, and finding outliers that can be applied to locate and eliminate online threats and risks. This method attempts to evolve a security system that will have the capacity to learn what it needs and act accordingly in search of both known and new security threats [23]. For IoMT, what kind of system should develop, intruder detection system also known as Intrusion Detection System (IDS). The proposed IDS aims at considering the actual network data they specify, and use machine learning to identify anomalous behaviors or features which could signify the existence of a threat. The method aims to operate under the peculiar circumstances of IoMT under which it is crucial to safeguard data and identify issues upon their occurrence. In this paper, the authors proceed with the rational of why the community should work towards standardizing a dataset of feature set for IDS [24]. To address this, the present study will identify a set of IDS features in an exhaustive and comprehensive manner and show that it is feasible to achieve an optimal level of meaningful comparison across different data sets and studies.

The purpose of this standardization is to increase the dependability of both the construct and the practice of IDS studies [25]. Described a network intrusion detection system (IDS) based on the supervised learning technique as described in [26]. When it comes to the implementation of an IDS that very effective then the study considered various categories of supervised learning model such as decision tree, support Vector machine and k-nearest neighbors. Ethernet traffic flow information that has been labeled in some way is then employed to show the models how they are supposed to differentiate the normal and malicious activities. Hybrid Convolutional Recurrent Neural Network Intrusion Detection System (HCRNNIDS) is suggested as a mixed network intrusion detection system that contains CNN and RNN in network structure. Since CNNs excel at spatial feature extraction and RNNs are preserve temporal sequence, the hybrid model integrates both CNNs and RNNs. This makes it easier for the IDS to find complex patterns of attack in network traffic Menlo Security refers to a network security control system that has been specifically designed to meet the demands of modern networks [27]. Create an IDS for mobile Internet of Things (IoT) using machine learning. The proposed system adopts the ML techniques where in the network data, we are able to see things that seem funny to mean an intrusion. The intrusion detection system (IDS) proposed here is designed to operate under the limited computational capacity and low-energy requirement found in mobile IoT [28]. It will be advisable to implement two-tier IDS that uses both auto-encoders and Long Short-Term Memory (LSTM) networks. In the first of the steps, the auto-encoders are applied for the unsupervised feature learning, and more specifically dimensionalities are reduced. In the second step, the data is processed using LSTM networks for temporal sequence analysis, and identification of intruder. It's important because the goal of this method is to make it easier for the IDS to establish more difficult and sophisticated patterns of intrusion in the network traffic [29].

Hybrid IDS model based on Deep Learning: DCNNBiLSTM IDS: An IDS model that adopts deep learning and integrates DCNN and BiLSTM. It is seen, DCNN excels in feature learning in space domain, while BiLSTM is effective to temporal sequential analysis. Altogether, the designed mixed model is improved for detecting spare intrusion patterns in the network traffic than the separate one [30]. Employ multi-layer perceptron (MLP) used well in intruder detection to design a real-time IDS. The suggested system capitalizes on the fact that DNN can review and learn from a very large number of network traffic data and identify patterns that are likely to be indicative of malicious activities. This is because, the IDS is supposed to operate in real time hence it can be able to detect as well as mitigate possible threats [31].

3. Methodology

The proposed FPGA-based Intrusion Detection System (IDS) has been architected in such a way that it is capable of high speed processing with the low latency and the ability to detect threats in real time. The system includes several component groups and every component group carries out a definite function in the IDS pipeline. Design, implementation, and evaluation of an adaptive FPGA-based Intrusion Detection System (IDS) that integrates three advanced models: Here are some of the models that are used which include the Meta Ensemble Learning model, Extreme Gradient Boosting (XGBoost), and the Hybrid Deep Learning (HDL) model. This makes the system to run on real time, hence making it to have stronger network security as compared to the use of other technologies such as CPUs and which have high latencies when used in the operations of FPGAs. The proposed IDS is evaluated using four well-known datasets: of several network traffic datasets, including UNSW NB15, CIC overall IDS2017, IoTID20, and NSL KDD benchmark, to evaluate the system's detection performance and its ability to generalize the attack types across multiple datasets.

A. FPGA Implementation Framework

The architecture of the proposed IDS on the FPGA consists of the following components:

- Data Preprocessing Module: Basic for cleaning, performances data normalization and features extracting from the incoming network traffic data.
- Feature Extraction and Selection Module: In using CNNs for spatial feature extraction, feature selection methods are used to down sample the data thus minimizing compute complexity.
- Model Inference Engine: Use of Meta Ensemble Learning model, XGBoost and the HDL model for implementing the intrusion detection mechanism.
- Decision and Response Module: Each term is used to analyze the outputs of the model and to assess whether an intrusion has happened, and the proper response should be given.

B. FPGA Design and Development

The design and development process involves the following steps:

FPGA Board Selection: The PYNQ-Z1 FPGA board is chosen for its balance between performance and ease of use.

Hardware Description Language (HDL) Coding: Schematic parts of the FPGA are defined using VHDL or Verilog to allow for hardware abstractions.

Integration with Python Jupyter Notebook Interface: The IDS interacts with the FPGA board using the Python programming interface to allow for control and decision making.

a. Data Preprocessing

Data Collection: The datasets used under the UNSW NB15, CICIDS2017, IoTID20, and NSL-KDD are considered to collect Network traffic data.

Data Cleaning and Normalization: Noise is reduced through data cleansing process while normalization is also done to remove differences.

Feature Extraction: CNNs are used to train layer model to extract important features from data automatically.

Feature Selection: To name a few examples, one may use Information Gain, Pearson Correlation, and F-test to select a small set of features to work with instead of using the entire data set.

b. Model Development

Meta Ensemble Learning Model: Integrates concurrent ML models to help enhance the detection outcomes. Other concepts that are used include bagging and boosting.

Extreme Gradient Boosting (XGBoost): This feature improves the boosting gradient framework for speed and performance to boost the detection feature.

Hybrid Deep Learning Model (HDL): CNN : to analyze the space, LSTM to analyze the time, It is relatively easy to implement to capture a rich and complete set of intrusion patterns in the network traffic.

c. FPGA-Based Implementation

Hardware Acceleration: FPGA is used in this case to enhance the processing of data by programming it in a way that makes it speed up its functioning and allow for real-time analysis together with the intrusion identification.

Parallel Processing: Exploring the strengths of an FPGA to allow parallel processing of data in cases where multiple streams of data are being processed. Optimization: Continuous optimization of HDL code and FPGA configuration to achieve high performance and low latency.

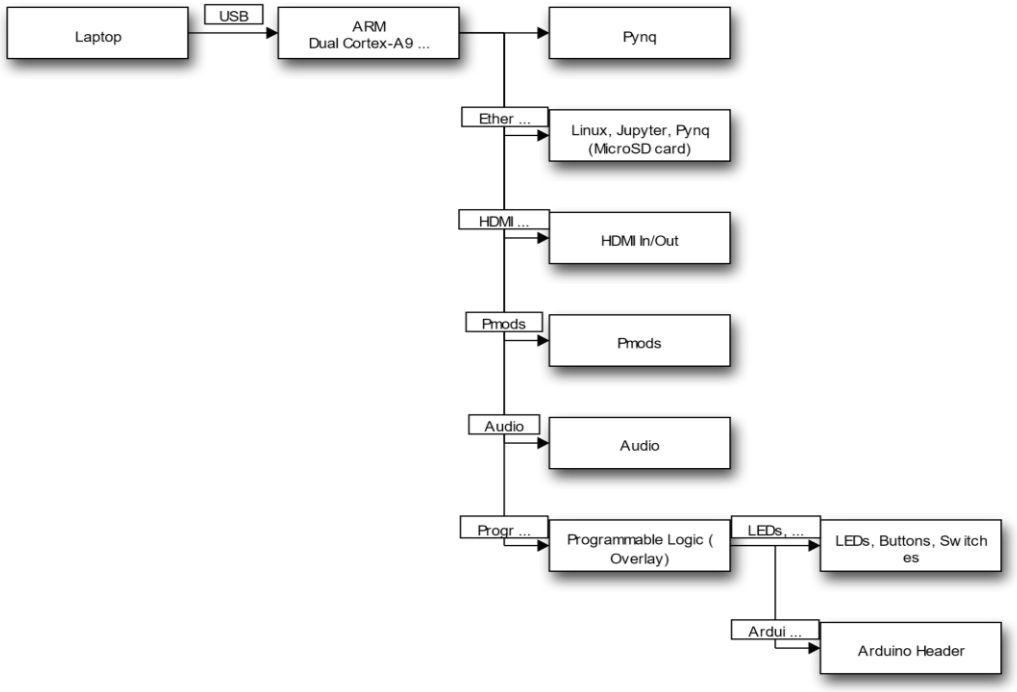

Figure 4. proposed PYNQ

Figure 5 presents the framework of the Adaptive FPGA-Based IDS prepared for real time network security. This is a kind of design that aims at utilizing two or more FPGA devices as well as utilizing high end machine learning models in performing its function in order to provide high performance and low latency in the detection of intrusion. The key components and their interactions are described as follows: The key components and their interactions are described as follows:

FPGA-Based IDS: The part of the system on which all the data processing is based, developed on the use of FPGA, creates the possibility of effective processing and fast work. The implementation of this concept enables it to perform elaborate algorithms in machine learning necessary for identifying intrusion within the shortest time possible.

Data Ingestion and Preprocessing: Traditionally, this module is in constant reception of the network traffic information from several sources. The results of the experiment can be refined by an arranged set of matrices, where the raw data themselves are preprocessed to clean noise and generalize information. This way, it is possible to avoid working with the ‘’dirty’’ data, that can seriously affect the quality of the feature extraction and following analysis.

Feature Extraction using CNNs: During this phase, Convolutional Neural Networks (CNNs) are used for feature extraction from the network traffic data that were preprocessed in the previous stage. CNNs have shown highest suitability in extracting more features including complicated structures and patterns that could be a lead to security threats.

Feature Selection: The features that have been obtained from the previous step are then subjected to feature selection methods in an attempt to recognize the most relevant features. This step involves qualitatively converting the components of the dataset or decreasing the number of analysis variables, which results in reduced computational intensity and increased effectiveness of the machine learning algorithms. Such approach helps to avoid many unnecessary complexities and allow the system to be more precise and effective as it deals with the shells of events.

Meta Ensemble Learning Model (MEL): This model averages the result of several machine learning models used in the learning process to enhance detection rate. By using bagging and boosting techniques, the methods combine the strength of multiple models that aims to create a highly accurate and reliable meta-model for intrusion identification.

XGBoost: XGBoost stands for Extreme Gradient Boosting is a more efficient gradient boosting technique that is used to build a model that consists of ensemble of decision trees. XGBoost has the notable advantage of speed, which makes this machine learning algorithm optimal for use in real-time identification of intrusions. It improves the discriminative ability of the system checking the traffic data in the network over the intricate and concealed patterns.

Hybrid Deep Learning (HDL) Model: The construction of the HDL model combines CNNs for spatial representation analysis with LSTM networks for the temporal analysis. Network traffic information is collected by this approach based on both space and time, making the detection of patterns of network data and finds more subtle attempts at intrusion.

Anomaly Detection and Response: A general introduction of the Meta Ensemble Learning model, XGBoost, and the HDL model’s outputs are used to find anomalies and possible intrusions. This module provides the final verdict on the basis of the combined results to confirm that an intrusion has taken place or not has taken place. Intrusion responses are active whenever an intrusion alert is issued in order to counter the intrusion threat and safeguard the network.

The figure 5 symbolizes the data and the exchanges between the above mentioned components , which underline the coherent structure of the DL models integration and the use of FPGA structure as a platform to develop a desirable IDS, which is more powerful, efficient and in real-time.

This is particularly the case when applying the model to IoT security as IoT devices are frequently attacked due to their popularity and diverse security standards. Thus, the employment of the FPGA-based IDS shows that the threat detection is rather fast and accurate, proving that it may be a solid approach to securing IoT devices and preserving the IoT transmissions’ confidentiality.

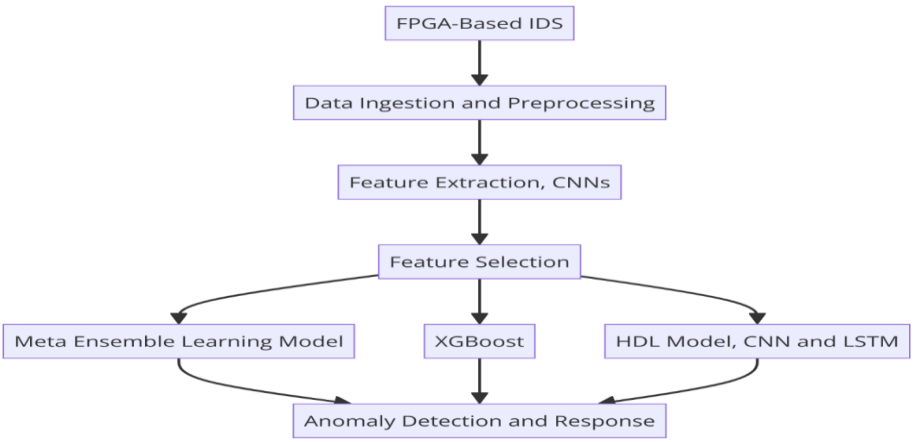

Figure 5. Proposed model procedure.

4. Result And Analysis

The performance and efficacy of the Adaptive FPGA-Based Intrusion Detection System (IDS) are evaluated using four well-known datasets: For the evaluation, we implemented and tested on datasets like UNSW NB15, CIC_IDS2017, IoTID20, and NSL-KDD. These datasets are employed frequently in the context of cybersecurity investigations, and they offer an exhaustive database for evaluating the performance of IDS in identifying different categories of network threats. The new UNSW NB15 dataset was developed by the ACCS to address the shortcomings evident within currently available datasets used for intrusion detection. It has a complete list of network traffic features derived from the combination of genuinely present realistic normal modern activities' profil and on the other hand the contemporary attacks' spoof. Packet capture was performed with the use of IXIA PerfectStorm in a controlled network in order to monitor the traffic generated by the applications. The dataset includes 49 features, including packet-level, flow-level, and hybrid features, as well as nine types of attacks: Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms, Fuzzers, Analysis. Approximately 2. 5 million records which, without a doubt, can be considered a large database for training and checking IDS models. CICIDS2017 is a dataset created by the Canadian Institute for Cybersecurity to mimic the modern real world network traffic and attack. This is a good set of features that is characterized by a broad coverage of the network traffic and the availability of the attack labels. As previously explained, both normal and attack traffic were taken over a real network and for a week this aggregate traffic was recorded as shown below.The dataset includes 80 network traffic features, such as source and destination IP addresses, protocols, and various statistical features of the traffic. Includes a wide range of attacks, such as Brute Force, Heartbleed, Botnet, DoS, DDoS, Web Attacks, Infiltration, and various types of malware. Over 3 million records, providing a rich dataset for evaluating IDS models. The IoTID20 dataset is specifically designed to represent Internet of Things (IoT) network traffic. It includes a comprehensive set of IoT device communications and various types of cyber-attacks targeting IoT environments. Communication traffic data was captured from a testbed of IoT devices, including smart home devices and sensors. The dataset includes 83 features, covering packet-level and flow-level characteristics of IoT network traffic. The dataset includes various IoT-specific attacks, such as Mirai, Bashlite, and IoT-DoS, reflecting real-world attack scenarios against IoT devices. Approximately 1 million records, providing a focused dataset for IoT intrusion detection. The NSL-KDD dataset is an improved version of the KDD Cup 1999 dataset, which was originally created for the International Knowledge Discovery and Data Mining Tools Competition. NSL-KDD addresses some of the inherent issues in the KDD99 dataset, such as redundancy and difficulty in learning. The dataset was derived from DARPA 1998 IDS evaluation dataset, which simulated a military network environment over nine weeks. It includes 41 features, categorized into basic features, content features, and traffic features. The dataset encompasses four major categories of attacks: Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), and Probing. Figure 6 presents the size of the data in splitting data into training and testing (70% training, 30% testing). The datasets are used with different numbers of records, and input features, the four dataset are used are inbalanced after using the SMOTE approach to oversample the minority classes (to achieve a balanced distribution), to make the balanced data as shown in Figure 7. The proposed models Meta Ensemble Learning model, Extreme Gradient Boosting (XGBoost), and a novel Hybrid Deep Learning (HDL) model are applied for all mentioned datasets in binary classification and the result shown in figures 8-11. The performance of different proposed models applied to the IoTID20 dataset for category classifications is discussed and evaluated. Figure 12 displays the precision scores for each model on other classes in the IoTID20 dataset. Figure 13 presents the recall scores for each model on other classes in the IoTID20 dataset. Figure 14 shows the accuracy of the proposed models.

Table 1: Number of normal and attack records in training and testing sets.

No.	Dataset	Type	Split data		Total Classes
			Training 70%	Testing 30%	
1	KDD99	Normal	68,094	29,184	97,278
		Attack	277,720	119,023	396,743
	Total: 494,021				
2	UNSW-NB15	Normal	65,100	27,900	93,000
		Attack	115,271	49,402	164,673
	Total: 257,673				
3	CIC-IDS2017	Normal	289,438	124,045	413,483
		Attack	440,351	188,723	629,074
	Total: 1,042,557				
4	NSL-KDD	Normal	67,343	9,711	77,054
		Attack	59,407	12,833	72,240
	Total:149,294				
	Total:		1,382,724	560,821	1,943,545

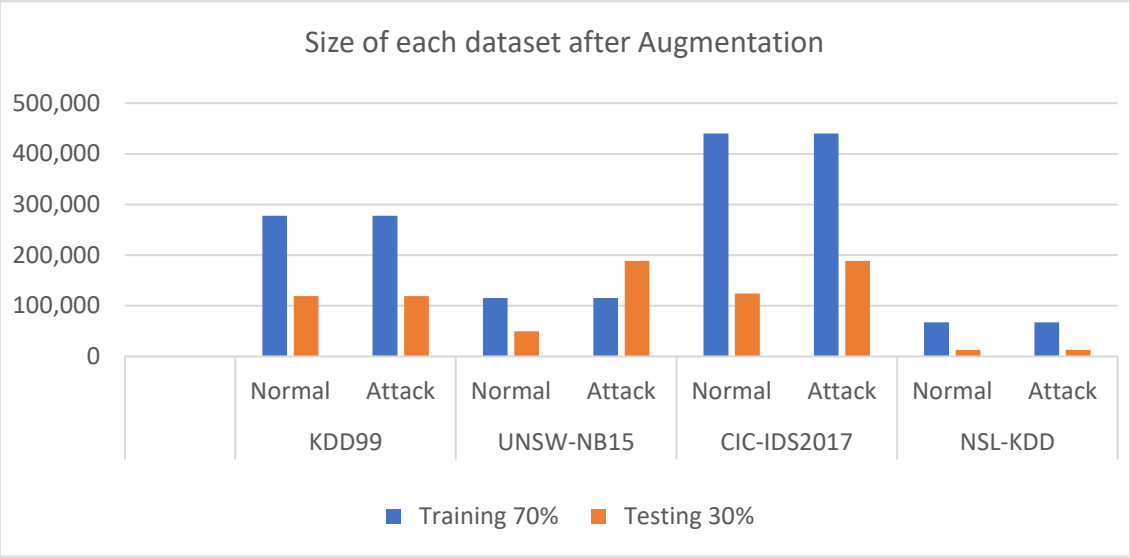

Figure 7. Size of the data after Augmentation

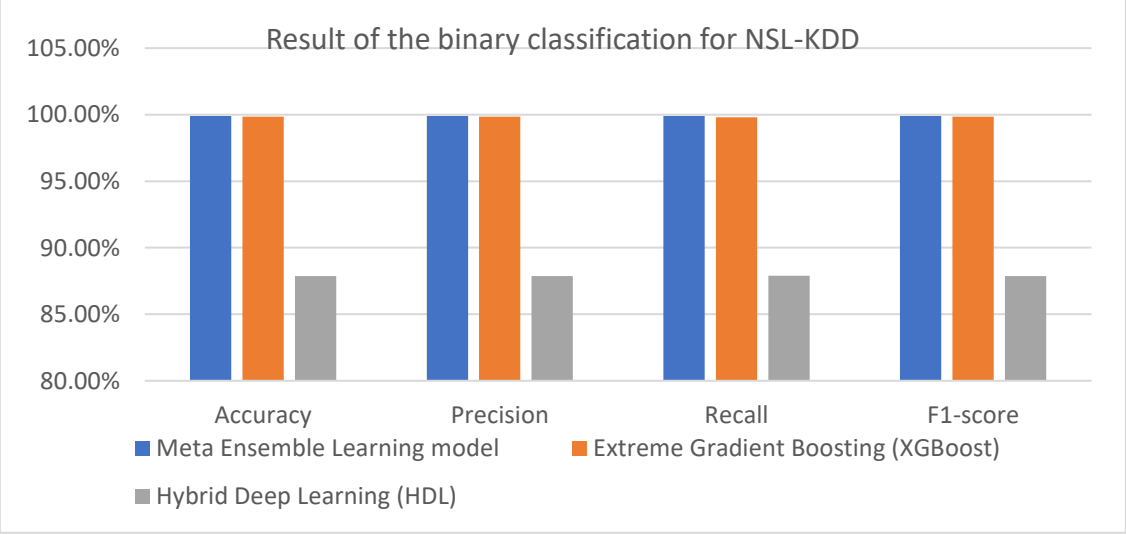

Figure 8. Result of the binary classification for proposed models in NSL-KDD dataset.

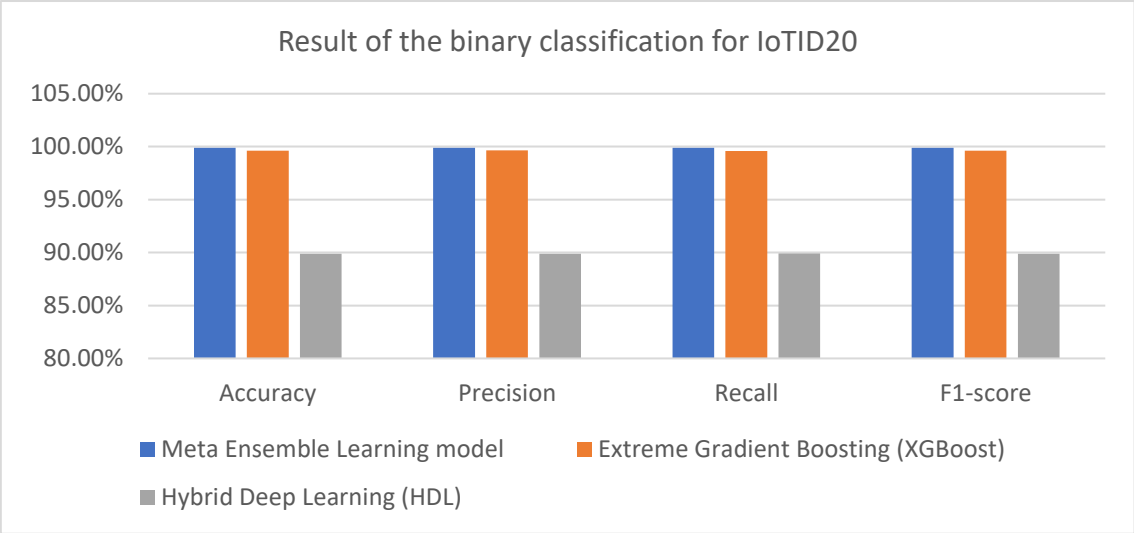

Figure 9. Result of the binary classification for proposed models in IoTID20 dataset

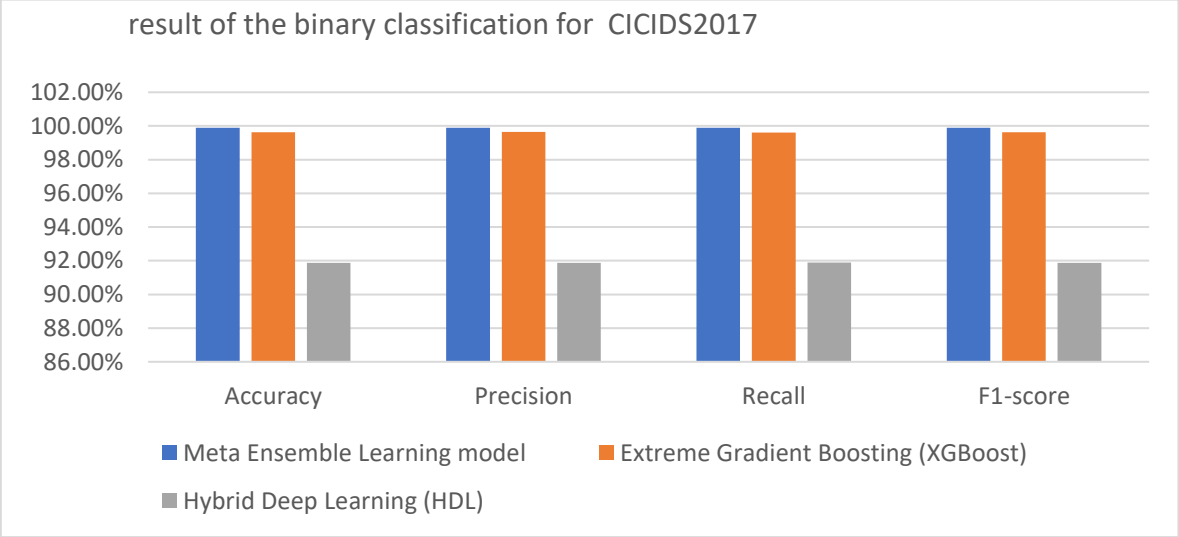

Figure 10. Result of the binary classification for proposed models in CICDS2017 dataset

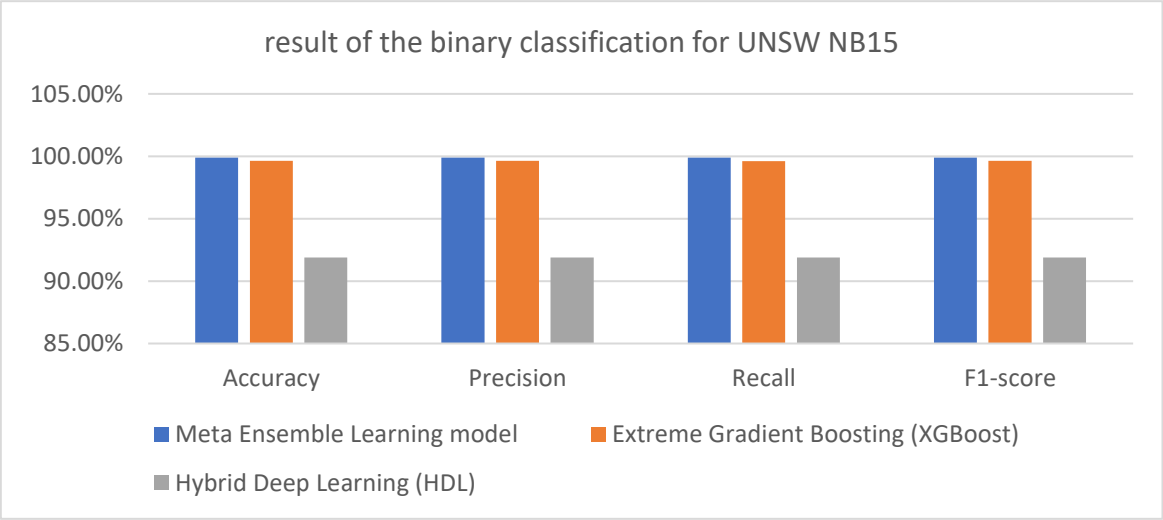

Figure 11. Result of the binary classification for proposed models in UNSW NB15 dataset.

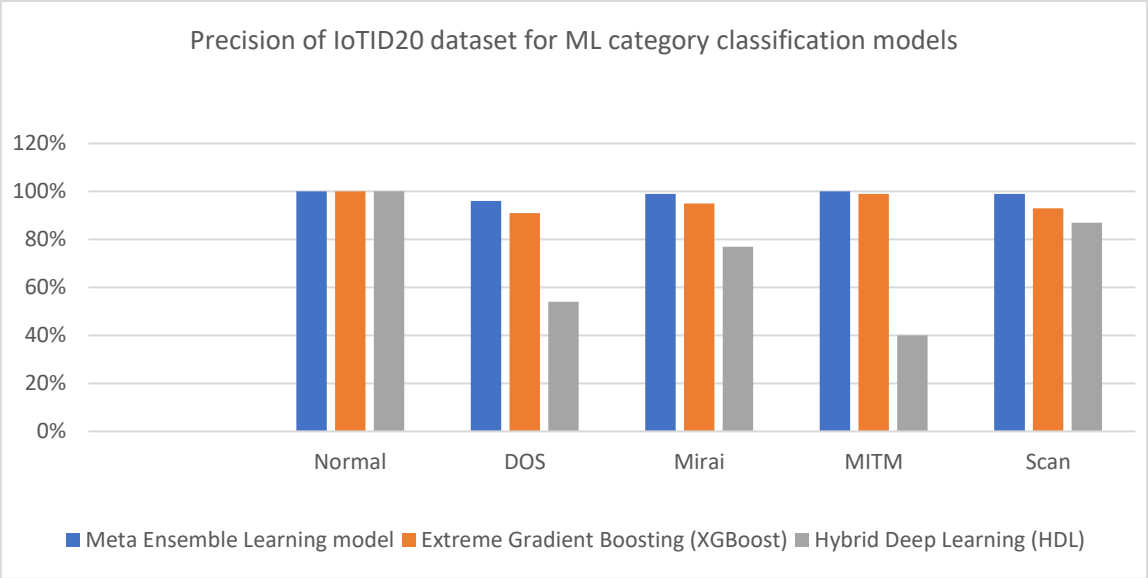

Figure 12. Precision of IoTID20 dataset for ML category classification models.

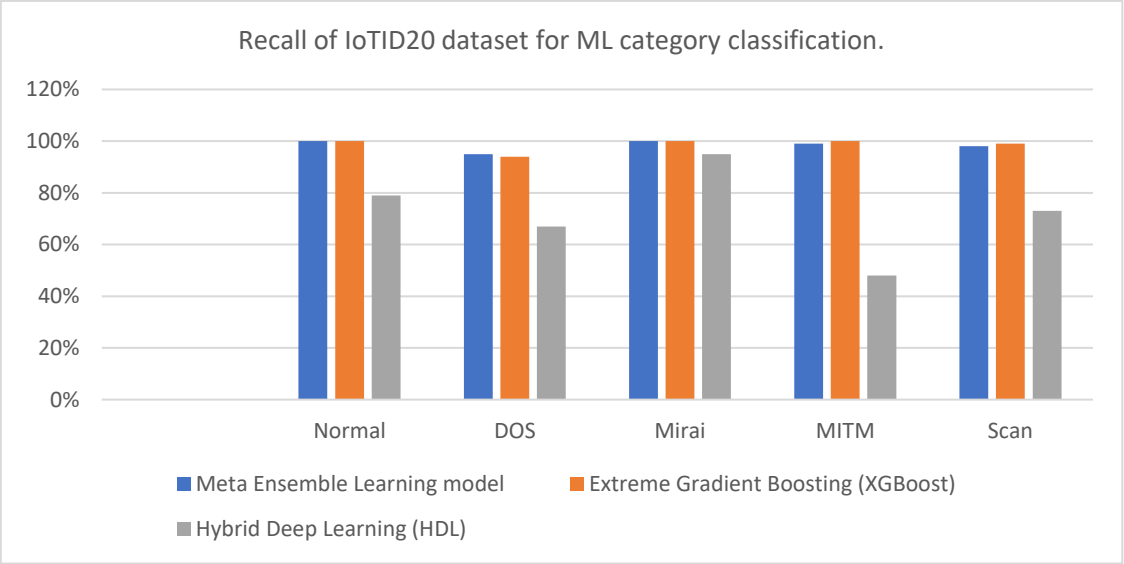

Figure 13. Recall of IoTID20 dataset for ML category classification.

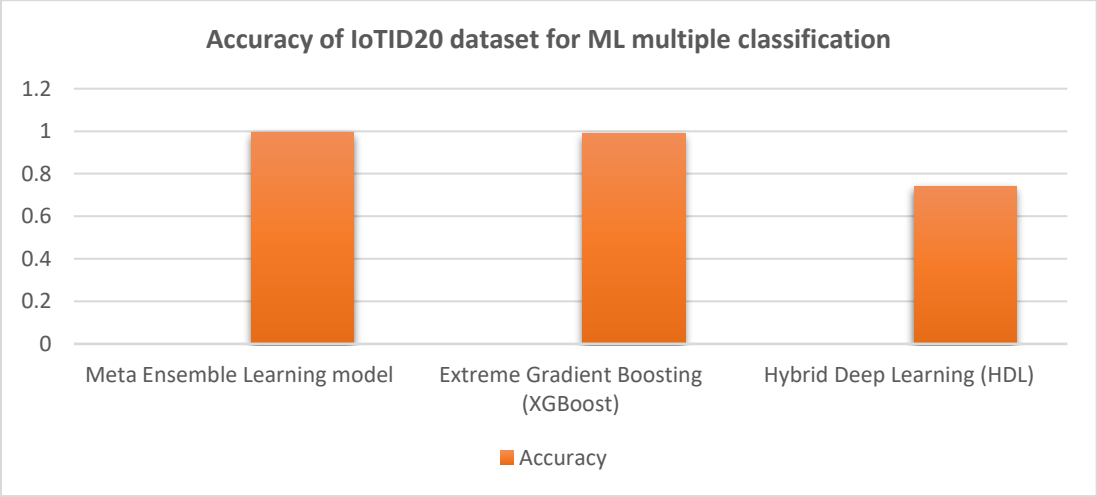

Figure 14. Accuracy of IoTID20 dataset for ML multiple classification.

The performance of proposed models applied to the IoTID20 dataset for subcategory classifications. The results for each model tests have been conducted with various ML classification models with IoTID20 dataset. The results of such investigation are shown in figures 15-17.

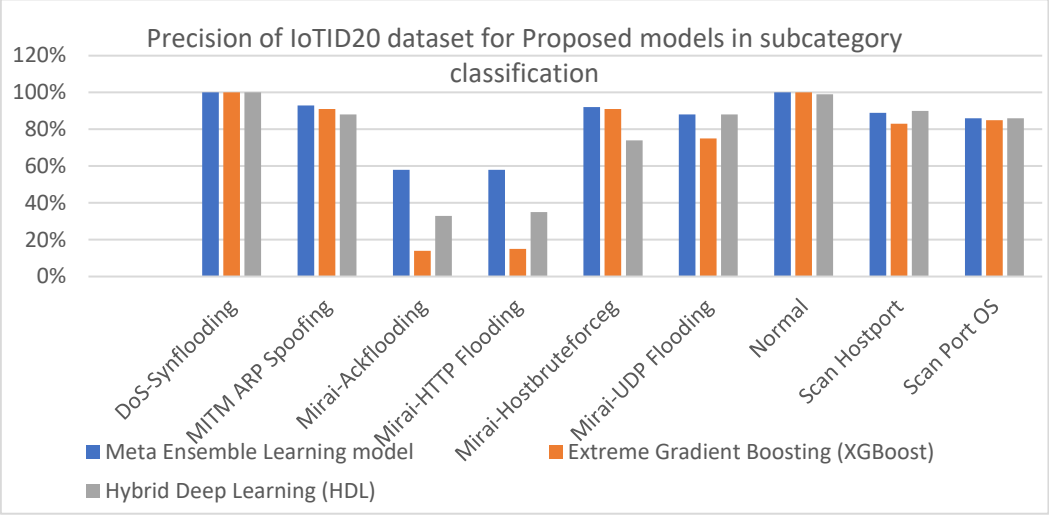

Figure 15. Precision of IoTID20 dataset for proposed models in subcategory classification.

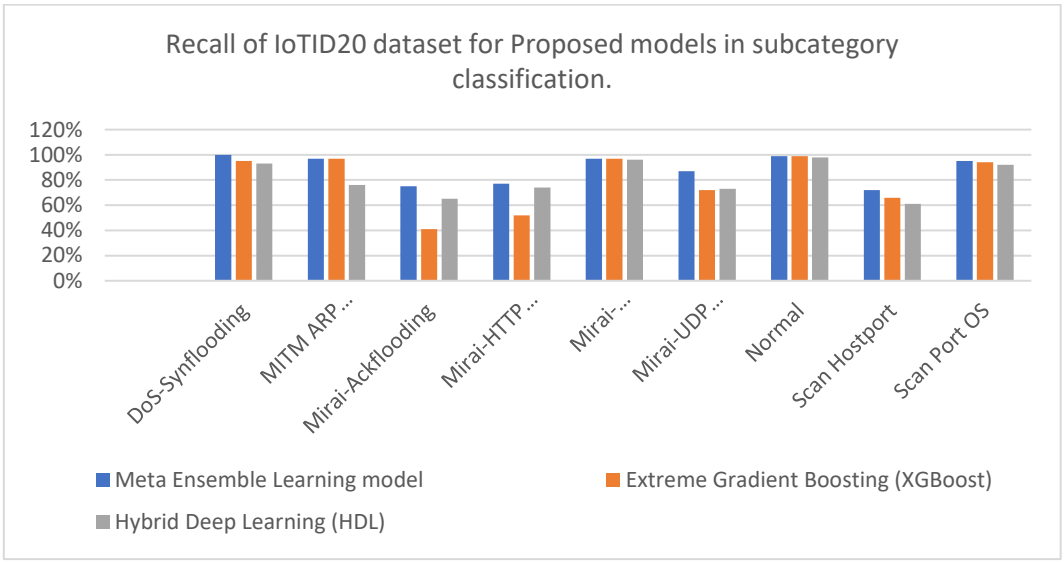

Figure 16. Recall of IoTID20 dataset for proposed models in subcategory classification.

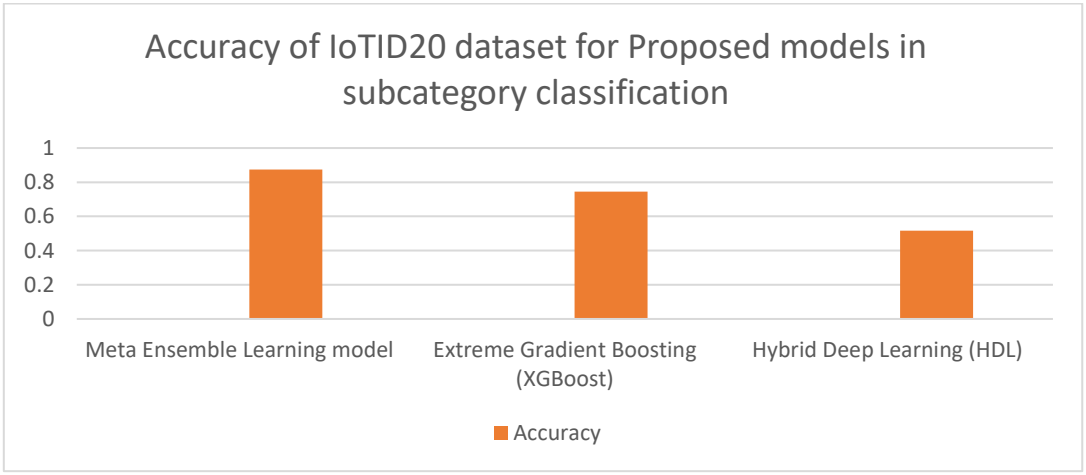

Figure 17. Accuracy of IoTID20 dataset for proposed models in subcategory classification.

A comprehensive analysis of proposed model's performance in comparison to previous studies. Evaluate the accuracy of the proposed MEL (Meta Ensemble Learning) model against various state-of-the-art methods employed by researchers in the field. Table 2 summarizes the accuracy comparison with previous studies.

Table 2: Accuracy result of the proposed model with related work.

Author	**Method**	**Binary**	**Multiple**	**Sub**
Ikhalati, et al. [32]	CNN-LSTM	98.80%	.....	.....
Bajpai, et al. [33]	Xgboost	98.64%	83.71%	62.30%
Yadav, et al. [34]	PCA and LSTM	99.51%	.....	.....
Safi, et al. [35]	DCNN	99.84%	98.12%	77.59%
Hussein, et al. [36]	RF	100.00%	96.50%	83.70%
Bhavsar, et al. [37]	PCC-CNN	99.00%	99.01%	…..
Alothbily, et al. [38]	Bagging	99.00%	99.00%	…..
Sarwar, et al. [39]	IDSBSPO	99.84%	78.46%	.....
Alothbily, et al. [40]	Ensemble	99.98%	.....	.....
Ullah, et al. [41]	LSTMDL	99.99%	.....	.....
Proposed	FPGA-based model	99.99%	99.19%	87.48%

5. Conclusion

The research presented in this paper introduces an adaptive FPGA-based Intrusion Detection System (IDS) designed to enhance real-time network security. The system is consequently able to register enhancement in the detection of network intrusions on account of the high performance and low latency properties inherent in FPGAs as well as the enhanced machine learning models. The case study of Meta Ensemble Learning model along with the Extreme Gradient Boosting (XGBoost) algorithm and the Hybrid Deep Learning (HDL) model that consist of both Convolutional Neural Network (CNN) and Long Short Term Memory (LSTM) also show the versatility of the technique. The effectiveness of the proposed system is evaluated using four widely recognized datasets: UNSW NB15, CICIDS2017, IoTID20, NSL-KDD, and final dataset. The results from the evaluations show that the adaptive FPGA- based IDS satisfies the real-time processing of the high-quality data and, with high detection rates alongside low false positive rates. Notably, discussing the IoT security, the model relevance is seen as IoT devices are more and more becoming favorites of hackers due to their massive use and poor protection. These features show the possibilities of using the FPGA-based IDS in the protection of IoT networks and devices, as well as the need for implementing IDS as an essential measure towards ensuring the security of IoT business communications. Therefore, based on the research conducted in this work, the adaptive FPGA based IDS can fill the gap of the existing IDS solutions to meet today's need ad hoc and robust threat detection solutions to enhance network security systems. Of the two solutions that can be applied to enhancing the cybersecurity of networks, the combination of top-tier ML with FPGA may be considered as a scale able and efficient one, capable of performing in real time, therefore, becoming an essential piece in the puzzle of protection against constantly emerging threats.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Mikhail DY, Hawezi RS, Kareem SW. An Ensemble Transfer Learning Model for Detecting Stego Images. Appl Sci 2023;13:7021. https://doi.org/10.3390/app13127021.

[2] Nandanwar H, Katarya R. Deep learning enabled intrusion detection system for Industrial IOT environment. Expert Syst Appl 2024;249:123808. https://doi.org/10.1016/j.eswa.2024.123808.

[3] Khalid Yousif M, Dallalbashi ZE, Kareem SW. Information security for big data using the NTRUEncrypt method. Meas Sensors 2023;27:100738. https://doi.org/10.1016/j.measen.2023.100738.

[4] Salih AA, Abdulazeez AM. Evaluation of classification algorithms for intrusion detection system: A review. J Soft Comput Data Min 2021;2:31–40.

[5] Awla HQ, Rahman Mirza A, Kareem SW. An Automated CAPTCHA for Website Protection Based on User Behavioral Model. 2022 8th Int Eng Conf Sustain Technol Dev 2022. https://doi.org/10.1109/iec54822.2022.9807472.

[6] Sai Chaitanya Kumar G, Kiran Kumar R, Parish Venkata Kumar K, Raghavendra Sai N, Brahmaiah M. Deep residual convolutional neural Network: An efficient technique for intrusion detection system. Expert Syst Appl 2024;238:121912. https://doi.org/10.1016/j.eswa.2023.121912.
[7] A New Efficient Method for Information Security in Hadoop. Qalaai Zanist Sci J 2022;7. https://doi.org/10.25212/lfu.qzj.7.2.42.
[8] Almukhtar F, Mahmoodd N, Kareem S. Search engine optimization: a review. Appl Comput Sci 2021;17.
[9] Yousif RZ, Kareem SW, Abdalwahid SM. Enhancing Approach for Information Security in Hadoop. Polytech J 2020;10:81–7. https://doi.org/10.25156/ptj.v10n1y2020.pp81-87.
[10] Ullah F, Ullah S, Srivastava G, Lin JC-W. IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic. Digit Commun Networks 2024;10:190–204. https://doi.org/10.1016/j.dcan.2023.03.008.
[11] Turukmane A V, Devendiran R. M-MultiSVM: An efficient feature selection assisted network intrusion detection system using machine learning. Comput & Secur 2024;137:103587. https://doi.org/10.1016/j.cose.2023.103587.
[12] Sadia H, Farhan S, Haq YU, Sana R, Mahmood T, Bahaj SAO, et al. Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach. IEEE Access 2024;12:52565–82. https://doi.org/10.1109/access.2024.3380014.
[13] Zorarpaci E. A fast intrusion detection system based on swift wrapper feature selection and speedy ensemble classifier. Eng Appl Artif Intell 2024;133:108162. https://doi.org/10.1016/j.engappai.2024.108162.
[14] Yaras S, Dener M. IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm. Electronics 2024;13:1053. https://doi.org/10.3390/electronics13061053.
[15] Devendiran R, Turukmane A V. Dugat-LSTM: Deep learning based network intrusion detection system using chaotic optimization strategy. Expert Syst Appl 2024;245:123027. https://doi.org/10.1016/j.eswa.2023.123027.
[16] Saleh HM, Marouane H, Fakhfakh A. Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning. IEEE Access 2024;12:3825–36. https://doi.org/10.1109/access.2023.3349248.
[17] Roshan K, Zafar A, Ul Haque SB. Untargeted white-box adversarial attack with heuristic defence methods in real-time deep learning based network intrusion detection system. Comput Commun 2024;218:97–113. https://doi.org/10.1016/j.comcom.2023.09.030.
[18] Zidi K, Ben Abdellafou K, Aljuhani A, Taouali O, Harkat MF. Novel intrusion detection system based on a downsized kernel method for cybersecurity in smart agriculture. Eng Appl Artif Intell 2024;133:108579. https://doi.org/10.1016/j.engappai.2024.108579.
[19] Tlili F, Ayed S, Chaari Fourati L. Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS). Comput & Secur 2024;142:103878. https://doi.org/10.1016/j.cose.2024.103878.
[20] Chen X, Qiu W, Chen L, Ma Y, Ma J. Fast and practical intrusion detection system based on federated learning for VANET. Comput & Secur 2024;142:103881. https://doi.org/10.1016/j.cose.2024.103881.
[21] Song J, Qin G, Liang Y, Yan J, Sun M. SIDiLDNG: A similarity-based intrusion detection system using improved Levenshtein Distance and N-gram for CAN. Comput Secur 2024;142:103847.
[22] Ashiku L, Dagli C. Network intrusion detection system using deep learning. Procedia Comput Sci 2021;185:239–47.
[23] Dutt I, Borah S, Maitra IK. Immune system based intrusion detection system (IS-IDS): A proposed model. IEEE Access 2020;8:34929–41.
[24] Thamilarasu G, Odesile A, Hoang A. An intrusion detection system for internet of medical things. IEEE Access 2020;8:181560–76.
[25] Sarhan M, Layeghy S, Portmann M. Towards a standard feature set for network intrusion detection system datasets. Mob Networks Appl 2022:1–14.
[26] Mebawondu JO, Alowolodu OD, Mebawondu JO, Adetunmbi AO. Network intrusion detection system using supervised learning paradigm. Sci African 2020;9:e00497.
[27] Khan MA. HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. Processes 2021;9:834.
[28] Amouri A, Alaparthy VT, Morgera SD. A machine learning based intrusion detection system for mobile Internet of Things. Sensors 2020;20:461.
[29] Mushtaq E, Zameer A, Umer M, Abbasi AA. A two-stage intrusion detection system with auto-encoder and LSTMs. Appl Soft Comput 2022;121:108768.
[30] Hnamte V, Hussain J. DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection

system. Telemat Informatics Reports 2023;10:100053.
[31] Thirimanne SP, Jayawardana L, Yasakethu L, Liyanaarachchi P, Hewage C. Deep neural network based real-time intrusion detection system. SN Comput Sci 2022;3:145.
[32] Ullah S, Ahmad J, Khan MA, Alkhammash EH, Hadjouni M, Ghadi YY, et al. A new intrusion detection system for the internet of things via deep convolutional neural network and feature engineering. Sensors 2022;22:3607.
[33] Martikkala A, David J, Lobov A, Lanz M, Ituarte IF. Trends for low-cost and open-source IoT solutions development for industry 4.0. Procedia Manuf 2021;55:298–305.
[34] Nižetić S, Šolić P, Gonzalez-De DL-I, Patrono L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. J Clean Prod 2020;274:122877.
[35] Rymarczyk J. Technologies, opportunities and challenges of the industrial revolution 4.0: theoretical considerations. Entrep Bus Econ Rev 2020;8:185–98.
[36] Pal S, Jadidi Z. Analysis of security issues and countermeasures for the industrial internet of things. Appl Sci 2021;11:9393.
[37] Aziz Al Kabir M, Elmedany W, Sharif MS. Securing IOT devices against emerging security threats: Challenges and mitigation techniques. J Cyber Secur Technol 2023;7:199–223.
[38] Ahmetoglu H, Das R. A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. Internet of Things 2022;20:100615.
[39] Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors 2023;23:4117.
[40] Alladi T, Chamola V, Zeadally S. Industrial control systems: Cyberattack trends and countermeasures. Comput Commun 2020;155:1–8.
[41] Injadat M, Moubayed A, Nassif AB, Shami A. Machine learning towards intelligent systems: applications, challenges, and opportunities. Artif Intell Rev 2021;54:3299–348.