Journal of Emerging Technologies and Industrial Applications
Vol. 5 No. 1 (2026) pp. 1-10
e-ISSN: 2948-507X

Journal homepage: https://jetia.mbot.org.my/index.php/jetia/index

Enhancing Firewall Security Through AI-Based Intrusion Detection System for Anomalous Behaviour

Asif Iqbal Hajamydeen[1], Nursyasya Zulaikha Mohammad[2]

[1]Artificial Intelligence and Cyber Security Centre, Management and Science University, University Drive, Off Persiaran Olahraga, Shah Alam, 40100, MALAYSIA

[2]Faculty of Information Sciences and Engineering, Management & Science University, University Drive, Off Persiaran Olahraga, Shah Alam, 40100, MALAYSIA

Email: asif@msu.edu.my, zsyasya93@gmail.com

Abstract: As attackers continue to develop more advanced attack methods, organizations are increasingly under threat from cyber security issues. While firewalls are effective in many instances as the initial line of defence, they may fail to protect against threats like APA (Advanced Persistent Attack), Zero Day Attacks, Ransomware, Insider Threats or AI-powered attacks. For these reasons, an organization needs to be more adaptable, intelligent and proactive in cybersecurity to ensure their digital assets and critical infrastructure are adequately protected. This investigation proposes an AI-based Intrusion Detection System (IDS) to operate in conjunction with current firewall infrastructure to improve detection. The Random Forest (RF) for supervised learning and the Isolation Forest (IF) for anomaly detection were combined into a hybrid machine learning approach. The approach was tested with the CICIDS2018 and UGR16 datasets, showing a better detection of known and unknown threats. AI Firewalls can be integrated with traditional firewalls to provide a comprehensive, real-time security solution, minimizing false alarms and increasing network security.

Received 10 February 2026; Accepted 01 May 2026; Available online 26 June 2026

Keywords:
Cybersecurity, Intrusion Detection System (IDS), Random Forest, Isolation Forest, Anomaly Detection, Machine Learning, Firewall Security

*Corresponding Author:

Asif Iqbal Hajamydeen,
Artificial Intelligence and Cyber Security Centre (AICS),
Management and Science University (MSU) Shah Alam, 40100, MALAYSIA
Email: asif@msu.edu.my

1 Introduction

With the growing reliance on digital infrastructure, Internet connected systems, cloud services and real-time data communication, cybersecurity has become an important concern for organizations [8,15]. Modern networks have a large amount of traffic that makes them target malware, denial of service attacks, phishing attacks, brute force attacks, port scanning, and unauthorized intrusions [8,15]. It is important that organizations are equipped with security mechanisms that can detect, prevent, and respond to suspicious activities in real-time, as cyberattacks are getting more sophisticated [21]. Today's network environment is more complex to secure, with traffic coming from a variety of sources such as user devices, servers, cloud platforms, remote access services, and web apps. This makes it harder to monitor manually and makes there more ways to attack. Attackers may be able to gain entry to a network without triggering traditional security controls by exploiting weak configurations, exposed services, stolen credentials, and vulnerable applications [8,15]. Thus, a robust defence mechanism should be able to monitor the network activity in real-time and detect suspicious changes before they become a serious incident [21].

Firewalls are still one of the most popular network security solutions as they permit us to define rules for filtering incoming and outgoing traffic according to IP addresses, port numbers and protocols [2]. However, when attackers hide malicious traffic in the form of legitimate traffic, or use common protocols, or exploit encrypted communications [18] then protection through a rule-based firewall is limited. This restriction becomes more severe in complex environments like cloud platforms, remote work systems, and large organizational networks where traffic behaviour is constantly shifting [18]. Firewall rules may be used to prevent traffic from known malicious sources or unused ports but may not be as effective if the attack traffic looks like normal traffic. For instance, malicious requests can be sent using regular protocols or over encrypted channels that are typically permitted within the organization's network. For this reason, the firewall might permit the connection because the traffic is not in violation of the firewall's rules. This is one reason why the security of firewalls must be enhanced with intelligence that can go beyond rule matching and analyse behaviour [2,18].

IDSs can be used to enhance the firewall's security by detecting suspicious and malicious traffic in the network [15]. Signature-based IDS can identify known attacks, but it is unable to identify new or modified attacks which do not have a signature in its database [8,15]. Anomaly-based IDS can recognize unknown threats when it recognizes the deviations from normal behaviour, but it can also produce false alarms when normal traffic deviates because of user actions, system loads, or network conditions [1,9]. The challenge is increased as security teams need to deal with the huge volume of alerts and at the same time find the most important threats. If an IDS generates too many false positives, administrators could spend time investigating normal activities that were reported as malicious. Concurrently, if the detection model is too strict, then real attacks will be missed. A balance is thus needed to ensure that the system can identify abnormal behaviour without compromising alert quality that is useful to the user [1,9].

This research suggests an Intrusion Detection System (IDS) using Artificial Intelligence (AI) along with firewall mechanisms to provide better protection from anomalous behaviour in networks. The system utilizes the supervised attack classification algorithm Random Forest and the unsupervised anomaly detection algorithm Isolation Forest. Random Forest is used to classify known attacks by labelled network traffic data, and Isolation Forest is used to detect unusual traffic patterns that can be considered as unknown or zero-day attacks [16,17]. It also provides dashboard-based monitoring, database-supported alert management, and firewall response actions to enable practical real-time security monitoring [21,22]. The proposed approach also embraces the concept of layered security. The firewall still carries out access control in this design, with the AI-based IDS adding additional traffic classification and anomaly detection capabilities. The dashboard and alert records provide clarity to administrators about the kind of threat encountered, its severity and what to do. This makes the system more useful for monitoring purposes as the detection result becomes visible to the administrator and is used to initiate response based on firewall rather than being isolated to the model results [21,22].

The growing complexity of network environments also makes this approach necessary. Today's networks do more than just support internal communication: they encompass cloud-based services, remote access, web apps, mobile devices and high volumes of encrypted traffic. These conditions increase the difficulty of static firewall rules determining a safe versus suspicious connection. Hence, a security mechanism which can analyse the patterns and recognize abnormal behaviour should be implemented to reinforce the firewall level and minimize reliance on manual rule updates [12,18]. In this research, abnormal behaviour is considered as one of the significant factors to signify possible intrusion. Signs of suspicious activity can be seen as unusual access, abnormal traffic, abnormal communication patterns, or behaviour that is not normal network usage. The changes may not be detected using traditional methods if the

activity does not have an attack signature. The combination of anomaly detection and classification should help detect both well-known attacks and suspicious yet unidentified behaviour that may represent new attacks.

It is noteworthy that the emphasis is on anomalous behaviour since not all intrusions start as an obvious attack. Certain attacks could begin with scanning, repeated attempts to connect, or with unusual traffic patterns and communication to unknown destinations. As a group, these activities can be signs of intrusion at a young age. The proposed system is designed to detect not only known signatures but also traffic behaviour to enhance the early detection of an attack so that it can do less damage. Administrator awareness is also a factor in security monitoring, which is considered in this research. A detection system should give administrators the information they need to determine if an event is normal, suspicious or malicious. In this regard, the proposed solution does not end with the prediction of the model. It also features alert severity, traffic information, and dashboard summaries to enable quick decision-making during monitoring activities based on the detection results.

2 Relevant Studies and Concepts

These core concepts include cybersecurity, firewalls, IDS, machine learning, anomaly detection, and hybrid detection models, which all aid in the development of an AI-based Intrusion Detection System integrated with firewall security. Cybersecurity ensures that digital systems, networks and data are safe from unauthorized access, misuse, disruption and damage [8]. With the growing reliance on interdependent systems, protection strategies need to be capable of mitigating both known and unknown threats [15]. The concepts are important because the proposed system will not only be a machine learning model, but also a security workflow that will link traffic analysis, decision making, alert generation, and response of the firewall. A firewall offers the most basic level of filtering, an IDS offers more in-depth monitoring, and machine learning offers more adaptive detection. These elements together can detect a broader spectrum of threats than a rule-based solution alone [12,15].

Firewalls play a crucial role in the defence of networks as they regulate traffic between trusted and untrusted networks according to access rules that are based on IP addresses, ports and protocols [2,18]. Advanced threats can masquerade as legitimate traffic and get through advanced filtering functions that are enhanced in next-generation firewalls [2]. Thus, it is necessary to provide firewall protection with the implementation of deeper traffic analysis and intelligent detection mechanisms. In the modern environment, the effectiveness of the firewall is also dependent on the maintenance of the rules. Static rules can become stale if network services change or attackers evolve their attacks. Manual rule management can be time consuming and can lead to configuration mistakes. For this reason, a firewall is more effective if it is backed up with detection technologies that can detect suspicious activity and feed into the rule adjustment or response actions. As a consequence, the firewall is more effective if it is supported by detection technologies that can detect suspicious activity and feed into rule adjustment or response actions [2,18].

An Intrusion Detection System (IDS) is a system that is used in conjunction with a firewall to identify suspicious activity in traffic patterns, system logs, and network behaviour [15]. The signature-based IDS can detect known attacks but cannot detect new or modified attack patterns [8]. Anomaly-based IDS is able to detect anomalies from normal activity, it is suitable for unknown attacks but may generate false positives if normal network activity changes [1,9]. Intrusion detection uses machine learning extensively as it has the ability to learn complex traffic patterns from large traffic volumes and enhance classification accuracy [12]. When labelled data is available, supervised learning can be used, and when the type of attacks is known, Random Forest can be used to classify them by combining multiple decision trees and to reduce overfitting [14,16].This makes it suitable for detecting attacks such as denial-of-service, brute force attempts, and scanning activities in structured datasets.

Random Forest is suitable for supervised intrusion classification because it uses multiple decision trees to make a final prediction, which helps improve stability compared with a single decision tree. This is useful for intrusion detection datasets that contain many traffic features and different attack categories. However, supervised learning still depends on labelled training data, which means it may be weaker when facing a completely new attack that has not been represented in the dataset [16].

Unsupervised learning is an important task as many new attacks do not have labelled examples in training [5, 6, 7]. Isolation Forest detects anomalies by isolating rare and unusual data points from normal data [17]. This makes it suitable for identifying abnormal traffic that may represent zero-day or previously unseen intrusions [9,17]. However, careful tuning is required because dynamic network behaviour may cause legitimate activity to be flagged as suspicious [9]. Isolation Forest complements supervised detection because it does not require labelled attack examples. Instead, it identifies unusual observations that differ from the majority of normal behaviour. This makes it useful for detecting suspicious traffic that may represent unknown threats. Nevertheless, anomaly detection needs careful threshold tuning because a legitimate change in traffic behaviour may also appear unusual to the model [1,9,17].

Hybrid intrusion detection systems combine the strengths of supervised and unsupervised learning. A supervised model can classify known attacks accurately,

while an unsupervised model can detect abnormal behaviour that is not present in labelled datasets [22]. Hybrid machine learning techniques also support real-time intrusion detection because different models can handle different types of traffic behaviour [21]. This supports the proposed system, which combines Random Forest, Isolation Forest, firewall integration, dashboard monitoring, and database-supported alert management.

A hybrid approach is therefore more suitable for this research because it allows known and unknown threats to be handled through different detection strategies. Known attacks can be classified through Random Forest, while abnormal or unseen patterns can be detected through Isolation Forest. This combination reduces the weakness of relying only on signatures or only on anomaly detection. It also provides a stronger basis for firewall integration because the system can generate responses based on both attack classification and anomaly scores [21,22]. Another key aspect of this research is the distinction between "detection" and "response". The major function of a firewall is to regulate access, and the major function of an IDS is to detect suspicious and/or malicious activity. If either component functions alone, there is no guarantee that a threat will be detected, and that something will be done about it. This can be bridged to some extent by the integration of IDS output and firewall response to provide a greater sense of “end-to-end” security in the same security workflow. In real time scenarios, response can be delayed, which may lead to an attack continuing to propagate through the network [21].

A false positive management is also a big issue in IDS research. The good thing about anomaly-based systems is that they can detect new activity that exceeds expectations, but they can also misidentify as suspicious what is actually legitimate activity if this activity shifts. This can cause 'alert fatigue', as the administrator may miss out on very serious alerts with the number of warnings they are getting. Thus, the process of pre-processing, feature selection, threshold adjustment and repeated testing are required to enhance the reliability and to minimize unnecessary alerts [1,9,11]. It is also evident in the literature that machine learning models need to be tested with the proper dataset and performance metrics. Labelled datasets can be used to teach a supervised classification model known attack patterns, and unlabelled or behaviour-based datasets can be used to detect anomalies. The metrics like accuracy, precision, recall and false positive rate help identify the capability of the IDS to identify threats without confusing administrators with false alarms. This is aligned with the known attacks’ classification using CICIDS2018 and anomaly based testing using UGR16 in this research [14,16].

Apart from model selection, the significance of dataset relevance is that an IDS trained with a few traffic patterns may not be as effective if it is presented with different traffic patterns. Benchmark datasets offer a controlled test environment for detection logic but may not encompass all production environments. For this reason, the proposed system performs dataset testing before the real application test to validate the system as initial validation. This helps support future testing in larger traffic sample and with a production type environment. A second problem in the current IDS literature is the trade-off between accuracy and usefulness of detection. High test accuracy does not mean a system is easy to use if it fails to provide administrators with the information needed to understand why a decision was made. Therefore, it is essential to have details of the alert, the severity of the alert and the visualization of the dashboard. This enables technical detection, as well as practical monitoring functions, which are essential in any real cybersecurity operations [20].

2.1 Comparison with Existing Systems

Intrusion detection systems and firewalls have several differences in terms of detecting the threat, data requirements, adaptability, and actions taken by the software after detection. Firewalls use rules to perform access control, yet they cannot effectively recognize attacks and their hidden features. IDS signature techniques including Snort and Suricata will only detect known attacks provided their signatures have been updated in time because attackers can change attack behaviour [15]. Yet another drawback of most existing systems is that their detection capabilities are not linked to actions, which means that a user may have to manually decide whether detected data is a threat and what needs to be done about it. To provide network security in real-time, detection must be connected to prioritizing alerts, logging, and blocking attacks via a firewall. That is why the designed system has additional components such as a dashboard and database [21].

Machine learning-based IDS enhances detection capability through data models that learn patterns in the traffic. Supervised learning models such as Random Forest are used in classifying traffic into normal and malicious categories based on labelled training data [16]. Unsupervised learning models such as Isolation Forest allow detection of unusual behaviour without the need of labelled data for attacks [9,17]. However, anomaly-based models can generate false alarms where legitimate traffic is classified as suspicious due to changes in behaviour [1,9]. The proposed system is unique compared to single systems since it integrates supervised traffic classification, unsupervised traffic anomalies, firewall actions, and dashboards in one sequence of events. Hybrid IDS designs are capable of enhancing network security since they combine different machine learning techniques [22]. Real-time intrusion detection helps in quick threat detection because the threats can be converted to alarms and firewall actions [21]. Moreover,

it enhances the visibility of administrators with an organized presentation of the outputs of the detection algorithm. Rather than just giving the raw value for the predictions of the algorithms, the dashboard provides priority alerts, attack distribution, protocol distribution, and firewall logs. This enables the administrator to have an idea on whether the traffic on the network consists mainly of normal traffic, anomalies, unknown anomalies, or attacks. Visibility is essential since the security of the network requires clear information, and not just the classification of the data.

Compared to other IDS software, the developed system focuses on the entire process of monitoring. While the IDS algorithms classify suspicious or malicious activities on the network, the firewall takes care of the mitigation of these attacks, and the dashboard allows these outputs to be visualized for the benefit of the administrator. This is necessary since even if the technical aspects are achieved, it might not be usable without proper visualization of the output [20,21]. This proposed process also helps decrease reliance on the use of signatures alone. Signature-based methods are important in dealing with known forms of attacks; however, they rely on whether the type of attack can be classified as known. The use of a machine learning method creates a capability of continued detection regardless of whether a specific signature exists. This creates additional protection for the security network [12,22].

3 Methodology

In the planning stage, the objectives of the study, scope of the system, algorithms, datasets, requirements for integrating with the firewall, dashboard functionality, and criteria for success were identified. The use of random forest algorithm was justified for supervised classification, as it works well with attacks which are known using labelled data [16]. Isolation forest algorithm was chosen for detecting anomalies since this approach detects rare or unusual traffic using unlabelled attacks [17]. CICIDS2018 dataset will be used in order to classify the known attacks and the UGR16 dataset will be used in order to detect the anomalies. The choice of datasets also justifies the objectives, as CICIDS2018 dataset has labelled traffic which helps in classifying the known attacks. On the other hand, the UGR16 dataset provides a way of detecting anomalies over the long period of time. The use of both the datasets makes it possible for evaluating the system in two aspects, namely, known attack classification and anomaly detection.

Among the identified risks during the risk analysis stage were data imbalance, overfitting, false positives, and problems with the integration of the IDS with the firewall. False positives represent a serious problem for IDSs since even normal traffic can sometimes be regarded as suspicious [1,9]. The following measures have been taken to address the identified risks prior to integration, including preprocessing, selecting features, adjusting models, and repeated testing [11,12]. The risk handling process was crucial since the effectiveness of an AI-based IDS is largely determined by the quality of input data and behaviour of the model. The presence of data imbalance may cause preference toward certain majority classes, whereas noise and irrelevant features may negatively affect detection performance. False positives may decrease the usability of the IDS since security administrators will constantly be flooded with alerts that are not relevant at all. The engineering process included the development of preprocessing of data, training of models, detection process, firewall behaviour, storage of data and visualization of results. Evaluation process included testing the detection rate, ability to detect anomalies, response speed and usability. Qualitative research based on semi-structured interviews was also conducted to determine user expectations, preferred types of alerts and necessity of clear, understandable security-related information [20].

The results obtained during interviewing influenced the design of the interface and alerts. Users expect a system that gives clear descriptions, is easy-to-use, and alerts are not highly technical. This is crucial as users need to receive information on what has happened, where the traffic comes from, and how serious the event is. In other words, the system should provide necessary monitoring information such as threat level, confidence of the result, protocols' distribution and logs from the firewall [20]. This also considers the way data travels throughout the process. Network traffic data needs to be captured, cleaned up, transformed, and put into a useful form so that it can be analysed with the help of the machine learning model. This process is needed to filter out unnecessary information that might affect the performance of the algorithm. If the data isn't properly prepared, the model will be analysing inconsistent information, leading to an increased number of false positives [11,12].

The testing process involves both aspects of evaluating the model performance and testing other components of the architecture for their ability to use that data for generating alerts. In this case, the classifier model was tested on the basis of its ability to classify traffic, while the anomaly detection model was tested for its ability to detect unusual traffic patterns. Testing the firewall component and the dashboard is essential since the solution being developed is not just an experiment with ML algorithms.

3.1 Proposed System Design

The proposed system is created as an AI-enabled intrusion detection system that is integrated with the firewall to provide network protection. The system comprises the following components: traffic acquisition, preprocessing, detection by means of machine learning models, firewall reaction, logging, storing information in databases, and dashboard reporting. The preprocessing

step is vital since the network traffic data can be associated with irrelevant information, which will negatively impact the functioning of the model [11].

The process starts with traffic record collection and preprocessing. In the preprocessing step, any additional noise that can impact the performance of the model is removed, and the traffic features are properly formatted. After the preprocessing step, the Random Forest model analyses whether traffic is similar to attacks, whereas the Isolation Forest model analyses if the traffic is behaving normally. The system decision is then logged and reported via the dashboard. The detection process includes the use of Random Forest and Isolation Forest for hybrid detection. The former is used for identifying known attacks from labelled network data, while the latter detects abnormalities in terms of identifying rare network events [16], [17]. Hybrid detection ensures that known attacks can be detected, along with suspicious activities that may not fall into any signature categories [22].

Firewall integration helps in acting against threats. If the traffic turns out to be safe, it is allowed to pass through but in case of suspicious or malicious activity, an alert is generated by the firewall and takes necessary measures like stopping suspicious IPs or ports. It is significant since timely action can save a great deal of trouble. This will maintain the firewall as the enforcing agent and make sure that the IDS is used as the intelligent analysis agent. It will not allow the firewall to block traffic at random times but will require the detection results and severity information before taking any action. It will minimize the chances of any incorrect blocking. The administrator will be able to see the details of the alert when required [21].

The UML use case diagram (**Figure 1**) consists of main actors and system functionalities. In this scenario, Administrator will control the security logs, firewall rules, IDS parameters, alerts, notifications, and update of the system. The user will denote access by a legitimate user and attacker will denote attacks or malicious traffic generated. Traffic classification is the main functionality of the system where it determines whether traffic needs to be allowed, alerted, or blocked. Alert details include timestamp, IP address, protocol, prediction, decision, and priority, which is stored in the MySQL database and dashboards.

The database component allows storing an alert history as each detected alert is stored along with several technical attributes such as date-time of alert generation, source and destination address of an alert, ports used, protocol employed, model decision, final verdict, and priority of a threat. Historical data will allow analysing previous cases of alerts and identifying potential suspicious trends among them. At the same time, this component can contribute for the future development of the tool since analysing previous alerts will help tune parameters and improve models

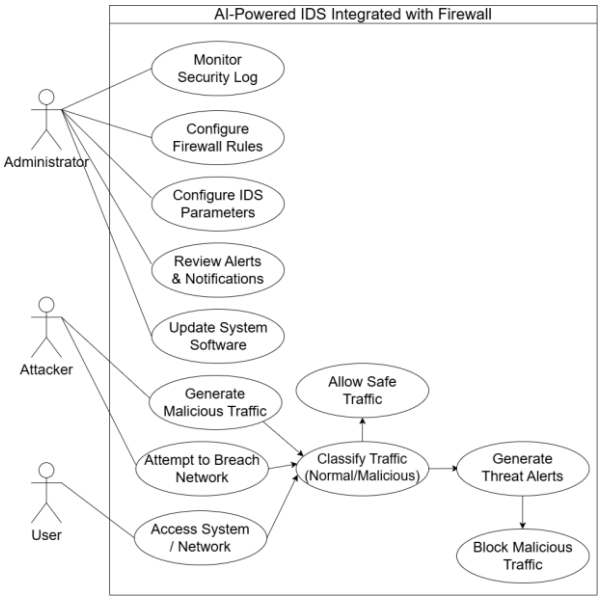

Fig. 1. UML case diagram for AI-Based Intrusion Detection System Integrated with Firewall

The third component is the dashboard. It aims at providing more convenience for monitoring purposes by summarizing the number of alerts, their severity level, distribution by attack's types, and protocols used. This approach will enable faster analysis since the user can instantly identify whether there are any usual activities on a network, potential suspicious cases, or confirmed attacks. At the same time, a simple interface is especially important for a user without sufficient expertise in cybersecurity [20].

4 Results and Discussion

From the results, it is clear that the proposed hybrid AI-based IDS enhances threat detection compared to traditional rule-based intrusion systems. Random Forest gave high performance in supervised classification as it was able to learn labelled attacks and classify them successfully. Supervised learning is appropriate where the attack patterns are present in the data [16]. The experiments conducted indicated that Random Forest was able to detect known attacks, including denial-of-service and brute force attacks from CICIDS2018, at 98%, 95%, and 97% accuracy, precision, and recall rates respectively. The high performance exhibited by Random Forest suggests that supervised learning is effective in cases where attack patterns are available in the training set. This helps to successfully identify common attacks, including denial-of-service attacks,

brute force attacks, and scan activities. Nevertheless, this is not sufficient because it is possible for attackers to use novel attack strategies to bypass supervised detection. This shows the necessity for anomaly detection [16], [22]. Isolation Forest brought additional benefits through anomaly detection and potentially zero-day behaviour within the UGR16 data set. Isolation Forest was created to detect and isolate rare events, so it is suitable for anomaly detection [17]. Nevertheless, anomaly detection could misclassify legitimate behaviour because of changes in normal behaviour based on different network loads, user activities, and even legitimate communication [1,9]. It means that anomaly detection can be efficient if done correctly. This example highlights the importance of proper implementation and tuning of an anomaly detection method within a monitoring tool. Traffic patterns in the network depend not only on regular behaviour but also on changes in users' actions, work hours, updates, and temporary increase in the number of requests. In other words, anomaly detection requires tuning of a used algorithm [1,9,12].

The combined usage of both Random Forest and Isolation Forest ensured that more attacks could be detected since each was dedicated to the purpose. Random Forest worked towards classifying attacks in an efficient way, whereas Isolation Forest helped detect attacks that were previously unidentified. The use of hybrid IDS through the use of machine learning techniques can enhance the level of security of networks [22]. This is beneficial in helping eliminate the shortcomings of using supervised or unsupervised approaches separately. The integration of the firewall ensured that the entire detection process became more effective since there would be an immediate response in case of any threats. The significance of real-time intrusion detection lies in the fact that it ensures quicker action, thus less damage [21]. In addition to this, the dashboard enabled better understanding of the system through showing the total number of alerts, priorities, attack protocols, attack distribution, and firewall logs in an organized way [20].

The dashboard further assisted the response phase by providing all relevant information about the detected threat in one view. Admins could see what type of threat was detected, the confidence level, the level of severity, distribution of attacks, distribution of protocols, and alert log entries. This is helpful since security staff have to know the situation behind any particular alert before responding to it blocking, modifying firewall settings, ignoring it, or investigating it. Thus, the system provides support for both automatic and human actions. Results further show that the proposed approach is better suited for an adaptive monitoring approach rather than static one. It is true that the firewall rule can filter out the traffic according to a set of predetermined conditions, but at the same time, it cannot detect suspicious behaviour, which was not anticipated when configuring the rule. In contrast, the use of AI allows adding the behavioural analysis component, which makes it possible to recognize any suspicious activity.

The false positives identified in the Isolation Forest model are a significant consideration in terms of the limitations of an anomaly detection algorithm. A model that is sensitive to any kind of anomaly will definitely generate more threat detection results, but it can equally generate many false alarms regarding changes in legitimate traffic. On the other hand, the problem with too tight a model is that it might miss subtle threats. It will thus be essential to tune the algorithm to strike a balance between sensitivity and effective alert quality [1,9]. It becomes clear from the results of the test that IDS effectiveness cannot be measured using just accuracy. While helpful, accuracy will only serve to obscure possible anomalies where the proportion of attacks is much lower than the number of normal traffic. Other indicators such as precision, recall, and false positives give a better idea of how well the model does in detecting the threat without generating many unnecessary alerts. These factors are critical in this case considering that the primary purpose of the system is to facilitate administrator responses [14].

In terms of practicality, the added component of the firewall response will add value by linking detection outcomes to mitigation actions. The detection process alone may notify administrators of any attacks but without mitigation, the risks will remain. With its ability to generate alerts, block IPs, close ports, and log events, the new system will be able to achieve that connection more effectively than ever before. The purpose of the research is not to come up with a machine learning classifier but enhance firewall security [21].

4.1 Pilot Study and Testing Findings

This phase confirmed the efficiency of the suggested model in the context of controlled experiments with simulated normal traffic and attacks. Structured testing is an integral part of a machine learning IDS since IDS performance should be analysed based on specific metrics and proper traffic settings [14]. The dataset CICIDS2018 was employed to evaluate known attack classification capabilities, while the dataset UGR16 helped assess anomaly detection efficiency. It should be noted that Random Forest proved to be highly efficient for detecting known attacks, and Isolation Forest provided additional results for novel attacks, although it needed fine-tuning to reduce false positives [9,16,17]. It can be stated that the testing phase helped confirm that the proposed model complied with basic criteria of real-time detection, high precision of machine learning models, and proper firewall integration. Classification based on Random Forest was effective for known attacks, while Isolation Forest detected unusual features do not present in labelled data. Nevertheless, it is necessary to mention that anomaly detection models need fine-tuning since normal traffic characteristics may change from day to day [1,9].

The result also proved that hybrid model is more flexible than a single one. The former enables reliable identification of known types of attacks through Random Forest and an extra cover provided by Isolation Forest for detecting suspicious but non-classified activity. Such flexibility is beneficial as network attacks may vary and include both known types of attacks as well as suspicious activity whose nature is still unknown to the model. Therefore, wider coverage is achieved; however, improvements can be made for reducing false alarms [21,22].

The design of the database ensured efficient testing since the data about alerts were stored in an ids_alerts table of a MySQL database. Alerts were characterized by timestamp, IP addresses, ports, protocol used, predictions obtained from Random and Isolation forests, decision regarding whether attack was detected, and priority level. This makes it easy to query information about the alerts, examine them, and visualize them using the dashboard. Additionally, alerts can lead to blocking IP addresses or closing ports [21]. Testing the system proved the necessity to link the information from the detector to the user interface. In case of displaying information in the form of raw results from the model, users will face problems trying to determine the severity of each incident. The inclusion of priority level, final decision, and traffic information is very helpful for understanding each event and allows faster investigations and the making of decisions regarding the necessity of response to the alert.

Despite the controlled nature of the study, its results proved valuable, providing evidence that the proposed system design can achieve the set goals. The controlled testing process made it possible to test models, response, data storing, and displaying information safely, without the risk of affecting any existing production network. At the same time, a broader range of tests would be required for the evaluation of actual performance.

4.2 System Interface and Database

There are four major screens included in the system interface. They include the dashboard interface (**Figure 2)**, the login page, create account page, and the firewall log dashboard screen (**Figure 3)**. While the login page will permit registered users to log into the system using their username or email address and passwords, the create account page allows new users to sign up for an account to use the system. This way, intrusion detection and monitoring operations will only be accessible by authorized users. The dashboard interface is used to monitor activities since it displays total alerts, priority levels, attacks and protocols distribution and firewall log records. With these features in mind, administrators will gain knowledge regarding network status, threats, and other essential aspects. Based on interview data gathered, the system should be easy to use and include specific alerting details in a language that is easily comprehensible by all types of users. Security information that is easily interpretable increases user trust since decisions are straightforward [20].

The design of the interface is crucial, not only in terms of the detection capability of an IDS but also in how effectively the results will be communicated. A complex interface may delay reaction and add to any confusion experienced in cases of security breaches. Through the use of graphical presentations, priority summary, and the use of log table, the IDS enables administrators to easily determine whether the state of the network is normal, questionable or undergoing an attack. The firewall log dashboard offers further insight into the detected events through timestamp, source IP, destination IP, protocol used, prediction results, priority and action done. Prioritization enables administrators to attend to cases with the greatest danger first. The implementation of a database allows real-time monitoring through data storage of IDS events.

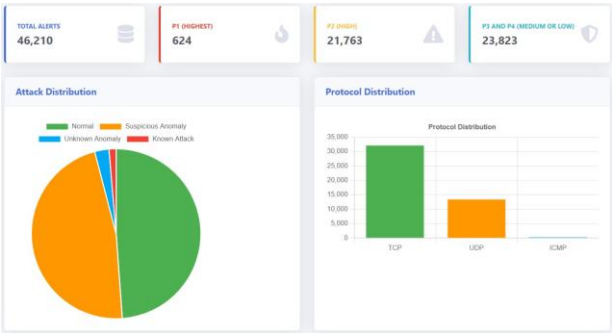

Fig. 2. Dashboard Interface

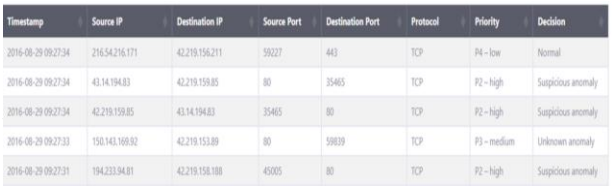

Fig. 3. Firewall Logs Dashboard

The database implementation makes it possible for real-time monitoring since the events reported by IDSs are stored in an organized manner. Information in each record consists of alert ID, time of occurrence, source IP, destination IP, source port, destination port, protocol type, predictions made using machine learning models, ultimate decision, and priority level. By indexing popular fields such as source IP, destination IP, and priority level, it is easier to concentrate on relevant information first. The use of databases is crucial as intrusion detection does not end after detecting the anomaly. Past records can help administrators see previous events, detect repetitive attacks, and monitor the behaviour of specific suspicious sources. Besides, the prioritization approach is another reason for using databases since the security team can concentrate on high-priority alerts. This contributes to

operational usefulness of the system. It means that there is an interaction between the two elements discussed. Interface makes it easy to quickly overview daily events, while databases provide organized data for future analysis. These elements complement each other because many security administrators need both instant notifications about incidents and a database of records for future examination and investigation.

5 Summary, Contributions and Future Work

This research reveals that implementing an IDS using AI with firewall security offers a better protection system in response to current cyber-attacks. Firewalls continue to be useful when it comes to access control; however, being based only on static rules restricts the efficiency of detecting any unknown or developing attacks [18]. The main advantage of IDS is enhanced visibility due to traffic analysis; however, signature-based IDS is capable of detecting only known attacks, and the detection process can generate false positives [1,15]. The primary value of this study consists in creating a novel IDS model which combines supervised and unsupervised machine learning along with firewall implementation. Random Forest algorithm allows for efficient detection of known attacks, and Isolation Forest enables the detection of anomalies to protect from unknown attacks [16,17]. Various approaches can be taken into consideration in hybrid IDS models [22]. Besides, real-time IDS is achievable through integrating IDS detection output with firewall actions such as alerts, blocking IPs, closing ports, and logging incidents [21].

This research is also valuable due to the fact that findings related to technical aspects can be applied to monitoring functions in practice. Apart from the generation of classification result, this application is also capable of saving an alert, setting its priority, showing on the dashboard and acting within a firewall based on that. It improves the system for security purposes as administrators will be able to see alerts, observe threats, and react according to their urgency. There have been several challenges identified during the development and testing process. One of the main problems with the Isolation Forest model was the appearance of false positives due to normal traffic behavior changes [1,9]. Another problem with machine learning algorithms is the imbalance of datasets, which may make the algorithm bias toward normal traffic more than attacks due to its higher occurrence rate. Preparation of the data is very important since data quality highly impacts cybersecurity machine learning [11].

Future improvements include optimizing the accuracy of detection, minimizing the number of false positives, and scaling up the model in order to enable practical application. For detecting more sophisticated attack patterns, future researchers can consider deep learning models including CNN, RNN, LSTM, and hybrid models of CNN-LSTM architecture [10, 20]. Furthermore, future research will also need to improve the ability of automatic blocking with necessary safety considerations, cloud-based monitoring for remote management, and explainable alerts so that administrators understand the reasoning behind their classification into three categories.

In addition to making the system easier to use, further development could also involve safer automation. Automation would speed up the process of response; however, it could also have an adverse effect since the detection may produce false results. A better approach may be to set different levels of response depending on the prioritization, which would mean that high-confidence malicious traffic should be automatically blocked, whereas lower-confidence cases should require manual review. Another potential extension of this research is through cloud-based monitoring, since many businesses have distributed networks based in various locations. Cloud-assisted monitoring would make it easier for users to review alerts, receive notifications, and monitor several locations via a centralized console. This would help make the research scalable and useful for business users who need flexible monitoring solutions for their network environments.

References

[1] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31. https://doi.org/10.1016/j.jnca.2015.11.016

[2] Ali, M., Younas, M., & Awan, I. (2018). Next Generation Firewalls: A Survey and Performance Evaluation. Computers & Security, 77, 110-127. https://doi.org/10.1016/j.cose.2018.03.004

[3] Hajamydeen, A. I., & Alhakimi, A. M. H. (2025). Utilizing Blockchain in Cybersecurity: An Emphasis on Privacy and Data Safety. In *Fostering Machine Learning and IoT for Blockchain Technology: Smart Cities Applications, Volume 1* (pp. 257-281). Singapore: Springer Nature Singapore.

[4] Hajamydeen, A. I., Hasni, M. D., & Abdullah, M. I. (2024). Integrating Wazuh for Efficient Real-Time Threat Monitoring and Vulnerability Assessment in a SOC Environment. In *Utilizing Renewable Energy, Technology, and Education for Industry 5.0* (pp. 292-320). IGI Global Scientific Publishing.

[5] Hajamydeen, A. I., & Udzir, N. I. (2019). A detailed description on unsupervised heterogeneous anomaly based intrusion detection framework. *Scalable Computing: Practice and Experience*, *20*(1), 113-160.

[6] Hajamydeen, A. I., & Udzir, N. I. (2016). A refined filter for UHAD to improve anomaly

detection. *Security and Communication Networks*, *9*(14), 2434-2447.

[7] Hajamydeen, A. I., Udzir, N. I., Mahmod, R., & Ghani, A. A. A. (2016). An unsupervised heterogeneous log-based framework for anomaly detection. *Turkish Journal of Electrical Engineering and Computer Sciences*, *24*(3), 1117-1134.

[8] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

[9] Chua, W. (2024). Web traffic anomaly detection using Isolation Forest. Information, 11(4), 83. https://www.mdpi.com/2227-9709/11/4/83

[10] Gueriani, A., Kheddar, H., & Mazari, A. C. (2024). Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems. arXiv preprint arXiv:2405.18624. https://arxiv.org/abs/2405.18624

[11] Hassan, M. A., & Bassiouni, M. (2021). Advancements in machine learning algorithms for cybersecurity: A survey. Computational Intelligence and Cybernetics, 19(2), 45-60. https://doi.org/10.1007/s42979-020-0085-x

[12] Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025). A comprehensive survey on intrusion detection systems with advances in machine learning and deep learning. Discover Artificial Intelligence, 5, 314. https://link.springer.com/article/10.1007/s44163-025-00578-1

[13] Kamal, Ayesha, Asif Iqbal Hajamydeen, and Adam Amril Jaharadak. "Log Necropsy: Web-Based Log Analysis Tool." In 2022 IEEE 10th Conference on Systems, Process & Control (ICSPC), pp. 176-179. IEEE, 2022

[14] Kaur, G., & Kaur, P. (2020). A survey on machine learning-based intrusion detection systems: Techniques, applications, and future directions. Journal of Cybersecurity, 12(3), 237-252. https://doi.org/10.1016/j.jcyb.2020.05.004

[15] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2(1), Article 20. https://doi.org/10.1186/s42400-019-0038-7

[16] Kumar, A. (2025). Impact of machine learning on intrusion detection in critical infrastructure environments. Information, 16(7), 515. https://www.mdpi.com/2078-2489/16/7/515

[17] Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. In Proceedings of the 2008 IEEE International Conference on Data Mining (pp. 413-422). IEEE. https://doi.org/10.1109/ICDM.2008.17

[18] Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2017). A survey of intrusion detection techniques in cloud computing. Journal of Network and Computer Applications, 36(1), 42-57. https://doi.org/10.1016/j.jnca.2012.05.003

[19] Pahl, C., & Loeffler, P. (2019). Software development methodologies: A systematic review. International Journal of Software Engineering and Knowledge Engineering, 29(5), 611-629. https://doi.org/10.1142/S0218194020500293

[20] Sinha, P., Sahu, D., Prakash, S., Yang, T., & Rathore, R. S. (2025). A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning. Scientific Reports, 15, Article 9684. https://doi.org/10.1038/s41598-025-94500-5

[21] Wu, Y., & Guo, X. (2020). Real-time network intrusion detection system using hybrid machine learning techniques. Journal of Computational Science, 43, 101080. https://doi.org/10.1016/j.jocs.2020.101080

[22] Zhang, Z., & Li, X. (2021). Hybrid intrusion detection systems for network security using machine learning algorithms. Journal of Network and Computer Applications, 175, 102905. https://doi.org/10.1016/j.jnca.2020.102905