

Secure Signal And Image Processing Architectures Based On Machine Learning For Next-Generation Cyber Defense

Dr Priyanka Mishra^{1*}, Dr. Rabins Porwal², Dr Rajamohan Parthasarathy³, Surender Singh⁴, Dr. Aasheesh Raizada⁵, P. Kavitha⁶

^{1*}Professor, Faculty of Computer Engineering(FCE), Poornima University, Jaipur ORCID ID - 0000-0002-3365-1235 Email id- prynkmshr@gmail.com

²Professor Department of Computer Application School of Engineering & Technology (UIET) Chhatrapati Shahu Ji Maharaj University (CSJMU), Kanpur, Uttar Pradesh, India. Email: rabins@csjmu.ac.in ORCID: 0000-0003-4646-4962

³Professor, Department of Computer Applications, Aditya University, Surampalem, Kakinada (District), Andhra Pradesh, India. Pincode: 533437, Email: rajamohanp@adityauniversity.in, ORCID ID:0000-0002-1571-6250

⁴Assistant Professor, Bhai Gurdas Institute of Engineering and Technology Computer Science and Engineering
Email ID: surinder1835@gmail.com

⁵ Associate Professor, CDOE, Mangalayatan University, Aligarh 202146 (U.P.) India Email: aasheesh.raizada@mangalayatan.edu.in

⁶Assistant Professor, Department of Mathematics, Amrita School of Physical Sciences, Coimbatore, Amrita Vishwa Vidyapeetham - 641112 - India. ORCID ID - 0009-0001-9238-2688 Email id - p_kavitha@cb.amrita.edu

Abstract

The blistering development of cyber threats due to more advanced and covert attack techniques has revealed the major shortcoming of the traditional intrusion detection mechanisms based on the fixed rules or one-dimensional analysis. Conventional methods tend to fail in the process of balancing detection and reduction of false-positive in dynamic networks. Inspired by these issues, this paper suggests a safe signal and image processing architecture, which relies on machine learning, next-generation cyber defense. The suggested framework uses a dual-branch architecture where the network traffic is processed as multivariate signals and image representation obtained after signal-to-image conversion. One branch of signal processing uses statistical feature learning and another branch of image processing uses convolutional neural networks to learn both spatial and nonlinear traffic patterns. Integration of complementary representations is then done at the feature-level to produce final intrusion classification. The framework is tested on the benchmark dataset of UNSW-NB15 in a supervised learning environment, and the performance is measured with the help of conventional measures such as accuracy, precision, recall, F1-score, and ROC-AUC. The experimental findings show that the suggested fusion architecture has better robustness, better discriminative ability and lower false-positive rates than single-modality models. These results emphasize the efficiency and useful applicability of secure signal image learning architectures in implementation in next generation cyber defense systems.

Keywords: Signal Processing; Image Processing; Machine Learning; Cyber Defense; Intrusion Detection.

1. Introduction

The recent cyber infrastructures have been changing at a rapid pace due to the increased use of cloud computing, Internet of Things (IoT), industrial control systems, and software-defined networks. On the one hand, these technologies have made it possible to achieve a level of scalability and efficiency never before seen before, but on the other hand, they have greatly increased the cyber-attack surface. Modern cyber threats are more advanced, dynamic and covert and use protocol vulnerabilities, traffic anomalies, and system-level vulnerabilities to circumvent traditional security controls. The attacks that are network based like denial-of-service, reconnaissance, exploitation and malware propagation have

been more sophisticated and difficult to detect by the traditional rule based intrusion detection systems. According to the recent research, the dynamic character of the next-generation cyber threats cannot be addressed by the available static and signature-based security solutions, which results in more false alarms and undetected intrusions [1], [2]. Signal processing has become a fundamental element of a cyber protection system in reaction to this dynamic threat environment. Network traffic may be intuitively represented as multivariate signals, in which statistical, temporal, and behavioral characteristics represent the dynamics of communication flows. The signal-based analysis allows the derivation of discriminatory patterns regarding the volume of traffic, the timing of packets, protocol and flow behavior. They have been extensively employed in anomaly detection and intrusion detection since they are easy to interpret and do not have a high computational cost. Nonetheless, signal-only techniques are commonly weak when it comes to modeling nonlinear interactions and high-dimensional dependencies that exist in contemporary attacks, especially when attackers intentionally act like regular traffic users [3].

In line with the progress in signal processing, image processing methods have started receiving increasing focus in cyber security studies. It is possible to apply powerful computer vision models to identify spatial and structural patterns that are not easily apparent in standard feature vectors by converting the features of network traffic into image-like representations. The analysis based on the images enables the convolutional neural networks to discover hierarchical representations and utilize the local correlations among features. Recent publications have shown that traffic data can be mapped to grayscale images or feature matrices to enhance attack detection performance, particularly in the case of advanced and obfuscated threats, by a significant margin [4]. Although such encouraging outcomes are possible, image-based techniques on their own can bring with them increased false-positive rates and computational complexity, when used in real-time security settings.

The introduction of machine learning and deep learning has radically changed the structure of cyber defense. Intrusion detection tasks have been widely addressed using data-driven models like logistic regression, support vector machines, convolutional neural networks, and deep neural networks. These models allow automatic feature learning, flexibility to changing threats, and better detection accuracy than the traditional techniques. Security systems using machine-learning have shown better performance in various network settings, such as cloud systems, enterprise networks, and cyber-physical systems [5], [6]. Nonetheless, most of the solutions available use a single modality of representation either statistical signals or image-based features, thus constraining their strength and generalization ability.

The research gap here is critical in that it has not been integrated in a single secure cyber defense architecture of signal-level and image-level representations. The majority of the existing research works concentrate on either signal-based machine learning or image-based deep learning separately. Signal-based approaches are more concerned with precision and interpretability, but tend to have lower recall in the case of complicated attack patterns. On the other hand, image-based techniques have better recall and can have increased false positives and are not explainable. Not many studies are able to investigate in a systematic manner how these complementary representations can be integrated to create a balanced and secure intrusion detection system. In addition, the absence of strategies of architectural fusion that can collectively utilize the statistical and spatial properties of network traffic is one of the major constraints of the existing research [7].

The rationale behind the choice of a joint signal-to-image learning model is the necessity to overcome the limitations of one-modality security systems. With the combination of

signal processing and image processing in one architecture, the global statistical behavior of network traffic and the localized spatial pattern of the network traffic can be captured. Signal representations are stable, have low false-positive, and are interpretable whereas image representations can be used to reveal complex nonlinear relationships with deep models. A fusion-based architecture can thus be able to improve detection strength, decrease susceptibility to evasion assaults, and the general discriminative power. This is in line with the increased focus on hybrid and multi-modal learning approaches in the next-generation cyber defense systems [8].

Besides performance, security and reliability are the most important in the real world deployment scenarios. The systems of cyber defense should reduce the number of false alarms to prevent alert fatigue, and at the same time, ensure high detection rates to prevent successful intrusions. Adversarial attacks are also becoming a major threat to machine-learning-based systems, and thus, robustness has become a significant design consideration. The combination of various modalities of representation can enhance resilience by ensuring that the use of one feature space is minimized and that the attackers have a more complicated time escaping detection in all dimensions at the same time [9].

In this regard, the current paper suggests a safe signal and image processing design founded on machine learning to support the next-generation cyber defense. The proposed architecture uses a dual-branch structure comprising of a signal-processing branch and an image-processing branch. Network traffic is then processed into a multivariate signal with standardized numerical and categorical features that constitute a powerful baseline detection model. Simultaneously, the traffic data is converted to grayscale image representations by feature-matrix encoding, and convolutional neural networks are able to extract spatial features. The products of the two branches are combined at a higher level to generate final intrusion decisions, thus capitalizing on the strengths that are complementary and counter the weaknesses that exist individually.

This study has a narrow scope, which is the detection of network intrusion based on benchmark traffic data. UNSW-NB15 dataset is chosen because it reflects the current attack patterns and it is extensively used in the academic community. The research assesses binary classification and does not concern itself with multi-class attack classification and real-time deployment limitations. Although the suggested architecture proves to be highly performant in the controlled experimental setting, the implementation in the real world might need additional optimization to cope with the latency, scalability, and adversarial resistance. These restrictions set the paths of future studies as opposed to undermining the efforts of the current research.

This research is important in that it presents a systematic combination of signal processing, image processing, and machine learning into a single cyber defense system. This piece of work can aid in the construction of more reliable and secure intrusion detection systems by experimentally showing that fused signal-image representations are more robust and discriminative than individual modalities. The results are especially applicable to the next-generation cyber defense settings, where adjustable and multi-dimensional attack approaches require adjustable and robust security responses [10], [11].

This research has three major objectives. To begin with, to develop a secure dual branch cyber defense structure that incorporates signal and image based learning paradigms. Second, to come up with a powerful signal to image transformation plan that will facilitate learning of spatial features using network traffic data. Third, to fully test the proposed architecture on a benchmark dataset and show its benefits over single-modality intrusion detection methods.

By means of these purposes, the research will contribute to the latest knowledge of machine-learning-based cyber defense and will be used to base future studies on the topic of secure and multi-modal intrusion detection systems.

2. Literature Review

Recent innovations in the field of cyber defense studies have been focusing more and more on the potential of signal-based machine learning methods in the detection of malicious behavior in complex network settings. When network traffic is represented as multivariate signals, it is possible to extract the statistical, temporal and protocol level characteristics necessary to intrusion detection. The use of signal-based learning methods has been prevalent because of their interpretability, efficiency and their ability to analyze in real-time. In-depth research on machine learning algorithms to process signals shows that classical classifiers with the proper feature normalization and selection strategies can be used to detect abnormalities in normal traffic behavior [12]. Nevertheless, these methods can easily fail to learn high dimensional nonlinear dependencies, especially when stealthy or adaptive attacks are involved.

Simultaneously, the image-based network traffic analysis has become a promising paradigm of cyber security applications. Researchers have been able to use computer vision developments to augment intrusion detection by converting network traffic characteristics into image-like forms. Convolutional neural networks can acquire the same spatial correlations and hierarchical structure that can be difficult to identify using conventional signal representations when used to manipulate images. Some of the studies have established that feature-matrix encoding, traffic flow visualization and image-based deep learning can enhance the accuracy of detection of complex cyber attacks to a considerable degree [13]. However, the image methods can create further processing burden and can be vulnerable to the representation design decisions, which can impact its resiliency in the context of operations.

Deep learning architectures have also evolved fast, which has revolutionized intrusion detection systems. Deep neural networks such as convolutional, recurrent and hybrid networks have been widely studied as models of complex network behaviors. These architectures allow automated learning of features and learnability to dynamic attack cases. Deep learning surveys on cyber security emphasise the usefulness of deep learning models to manage large scale and high dimensional data, especially in next-generation and Industry 4.0 networks [14], [15]. Even though deep learning-based intrusion detection systems have proven to be highly effective, the systems are associated with interpretability issues, training stability, and adversarial manipulation vulnerabilities.

The issue of security and robustness has thus become an important factor in machine-learning-based cyber defenses. Since learning-based models have found use in security-sensitive applications, their susceptibility to adversarial attacks, data poisoning, and model evasion has become an issue of concern. Studies of autonomous and self-learning cyber defense architectures highlight the importance of resilient designs to be able to adjust to changing threats without compromising the detection performance [16]. The combination of several learning modalities and representation spaces has been found to be one of the promising approaches to increase the robustness and minimize single-point vulnerability.

Comparative analysis of machine learning and deep learning models applied to cyber security further indicates that there is no single method that has been found to be effective over all attack scenarios. Although the traditional machine learning models provide stability and interpretability, the deep learning models are superior in terms of capturing complex patterns, but they can produce a higher false-positive rate [17], [18]. These results indicate that hybrid and multi-mode architecture is more appropriate in the real-

life use of cyber defense because it is able to trade-off between accuracy of detection, robustness and reliability of operation.

This point of view is supported by recent reviews on cyber-physical systems and next-generation networks, which emphasize the value of integrating heterogeneous data representations and learning paradigms [19], [20]. These systems have a very dynamic environment where the attacks may be directed in both cyber and physical components and therefore require strong security mechanisms that are adaptive. Research points out that fusion-based methods have the potential to enhance resilience through the combination of complementary sources of information and the reduction of the weaknesses of single models.

Although the literature is increasing, there are still a number of limitations that have not been addressed. Numerous literature works are concerned with either signal-based or image-based representations, and there is no systematic attempt to combine the two in a single architecture. Also, fusion strategies are usually under-explored or restricted to basic ensemble methods which fail to utilize feature-level complementarities. Extensive studies show that more research needs to be done on joint signal/image learning systems to deal with false positives, robustness of detection, and responsiveness to new threats [21], [22].

Considering these constraints, the current research niche itself, suggests a safe two-branch architecture that unites signal processing and image processing into a machine-learning system. Incorporating statistical signal representations with spatial image-based features by feature-level fusion, the proposed methodology will address the gaps that have been pointed out by previous studies and help in designing improved and more robust intrusion detection systems to be used in the next generation of cyber defense.

3. Methodology

The research design of this study is a quantitative, experimental research design to design and test a safe signal and image processing structure on machine learning as a next-generation cyber defense. The approach combines traditional signal-based learning, image-based deep learning, and a feature-level fusion approach to improve the performance of intrusion detection. The proposed framework is logically tested with a benchmark cyber security data under controlled experimental conditions.

3.1 Dataset Description and Selection Rationale

The UNSW-NB15 dataset is used to conduct the experimental analysis because it is applicable to the contemporary cyber threat context and it is commonly used in the intrusion detection studies. The dataset was created within the Cyber Range Lab of the Australian Centre of Cyber Security with the use of IXIA PerfectStorm tool, which is used to simulate a realistic network traffic environment. It is a mixture of legitimate network behavior and synthetic but modern attack behavior that offers a realistic representation of real-world cyber defense problems[23].

The data contains nine types of cyber attacks such as Fuzzers, Analysis, Backdoors, Denial of Service (DoS), Exploits, Generic, Reconnaissance, Shellcode, and Worms and normal traffic cases. The processing of network flows was done in the form of Argus and Bro-IDS tools in order to obtain a full set of features that reflect statistical, temporal, and protocol-level features. In this work, the binary classification labels, which represent normal or malicious traffic are used.

The established training and testing divisions are used to guarantee reproducibility and comparability. The sample size of the training set is 82,332 and the testing set is 175,341. The UNSW-NB15 dataset is chosen as it represents next-generation cyber threats much

better than older datasets and can be learned both at signal-level and image-based learning.

3.2 Data Preprocessing and Normalization

Preprocessing of data is done to make it consistent, stable, and reliable in the process of training the model. First, non-informative identifiers and label-related attributes are eliminated in order to avoid data leakage. The other features are classified as numerical and categorical features.

Z-score normalization is used to standardize numerical features and make them have a mean of zero and a unit variance. This normalization aids in counteracting the effect of disparities in scale by all features and enhances the convergence behavior when optimizing a model. Categorical We use one-hot encoding to convert symbolic values into binary vectors suitable to be used by machine learning algorithms, like protocol type and service identifiers.

Each of the preprocessing operations is executed in a single transformation pipeline to ensure the same processing is done on training and testing data. This is a pipeline-based methodology that increases the reproducibility and makes the learned models generalize effectively to unknown data.

3.3 Signal Representation and Feature Engineering

Within the proposed framework, the network traffic records are first represented as multivariate signals. The statistical behavior of network flows is represented by the fixed length feature vector consisting of the numerical and encoded categorical features. These signal representations form the input of the signal-processing part of the architecture.

The signal-based baseline model is a logistic regression classifier because it is the most robust and is interpretable and can be used on high-dimensional data. Balanced class weighting is used to address class imbalance whereby minority attack samples are sufficiently represented in the training process. This signal-based model provides a solid foundation and gives a clue about the discriminative capability of the statistical features of traffic.

Signal representation represents the linear relationship between features and provides accuracy, which is important in reducing the false-positive rates in security-related settings.

3.4 Signal-to-Image Transformation Strategy

In order to facilitate image-based learning, the normalized numerical signal vectors are converted into two-dimensional grayscale images by a feature-matrix encoding strategy. Each feature vector is reshaped into a square matrix of size $H \times W$, where $H = W = \lceil \sqrt{N} \rceil$ and N denotes the number of numerical features. Where the use of unnecessary positions by a matrix is concerned, zero-padding is used to occupy the empty spots.

The transformation adds space to the data and retains the original values of the features. The resulting images enable the convolutional neural networks to take advantage of the spatial correlations between features that are hard to learn by only signal-based methods. The visual representation of the image is a supplementary view of the network traffic pattern and aids the further deep learning analysis.

3.5 Proposed Secure Signal and Image Processing Architecture

3.5.1 Overall System Architecture

The suggested architecture will be a dual-branch development with separate signal-processing and image-processing branches. Both branches work with the same underlying network traffic data though they derive different feature representations. The

outputs of the two branches are later merged to come up with the final decision on intrusion classification. Late-fusion strategy makes it robust and increases the reliability of detection.

3.5.2 Signal Processing Branch

The signal-processing division directly works with standardized numerical attributes and one-hot categorical attributes. The logistic regression classifier is trained to give a model of relationship between signal features and intrusion labels. It is focused on low false-positive and interpretability, which makes it appropriate in operational cyber defense systems where explainability and reliability are necessary.

3.5.3 Image Processing Branch

The image-processing division uses a convolutional neural network to process the images generated in grayscale. The CNN topology is made of several convolutional layers to extract spatial features, pooling layers to learn dimensionality and dense layers to learn high-level representations. An embedding layer is specifically designed to generate a small feature set, which learns spatial patterns on network traffic images.

Preventing overfitting is done by regularization techniques, such as dropout and early stopping. Stratified validation splitting guarantees equal distribution of classes in training which results to consistent and accurate performance.

3.5.4 Feature Fusion and Decision Layer

During the fusion stage, the signal based feature and the image based embedding are merged into one. This combined feature vector combines statistical, categorical and spatial information. An ultimate logistic regression classifier is trained using the merged features to produce intrusion classifications. The fusion method uses the complementary capabilities of both branches, which leads to enhanced separability and robustness.

3.6 Model Training Strategy and Parameter Configuration

The paradigm of model training is based on supervised learning. Signal-based model is trained using the entire training set and image-based CNN utilizes a stratified validation split to track the generalization. Weighted loss functions are used to deal with class imbalance.

Hyperparameters such as learning rate, batch size, and the number of epoch are empirically chosen to give performance and trade-off the computation efficiency. Validation ROC-AUC is used to early stop and avoid overfitting to provide a stable convergence. Python-based machine learning frameworks are used to conduct all experiments so as to be reproducible.

3.7 Security and Robustness Considerations

The proposed methodology is based on security and robustness. Precision is desired to be high and the false-positive rate should be low in order to minimize alert fatigue and operational overhead. The dual-branch design boosts the resilience of being not dependent on one performance modality of representation. The feature fusion also increases resistance to evasion attacks on particular feature spaces.

In general, the methodology facilitates the creation of robust, scalable and secure intrusion detection systems that can be used to defend next generation cyberspace.

4. Results

This part provides and discusses the experimental findings of the proposed secure signal and image processing architectures. Three learning paradigms, signal-based learning,

image-based learning and a signal-image fusion architecture are compared based on the UNSW-NB15 test dataset. To have a complete evaluation, standard metrics of intrusion detection, such as accuracy, precision, recall, F1-score, and ROC-AUC, are used. Further, confusion matrices and ROC curves are used to visualize the behavior of classification and discriminative capability.

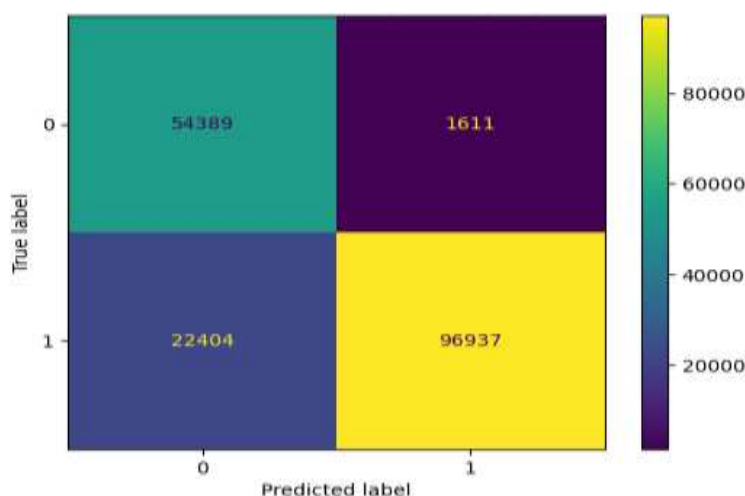
4.1 Performance of the Signal-Based Learning Model

The signal-based learning model is the baseline intrusion detection method, which directly works on numerical and categorical traffic features that have been preprocessed. The reason behind the use of logistic regression is its strength, interpretability, and applicability to high-dimensional data of cyber traffic.

The signal-based model has a test dataset accuracy of 86.30, precision of 98.37, recall of 81.23, F1-score of 88.98, and ROC-AUC of 0.9777. These findings reveal that the model is very effective in the proper identification of malicious traffic with exceptionally low false-positive rate.

The signal-based model confusion matrix presented in Figure 1 shows that the classifier correctly recognizes 96,937 attack, 54,389 normal samples, and generates only 1,611 false positives. Nevertheless, it is observed that 22,404 false negatives are achieved, meaning that not all advanced patterns of attack are well represented by signal-level representations only.

Figure 1: Confusion Matrix — Signal (LogReg).



This figure shows the classification results of the signal-based model on the UNSW-NB15 test set with a high precision and low false-positive rate but a relatively high amount of false negatives.

All in all, the signal-based model has a good baseline performance especially in precision and ROC-AUC, which is why it can be applied in security-critical settings where false alarms must be minimized. Nevertheless, the false negatives that were observed encourage the incorporation of more detailed representations.

4.2 Performance of the Image-Based Learning Model

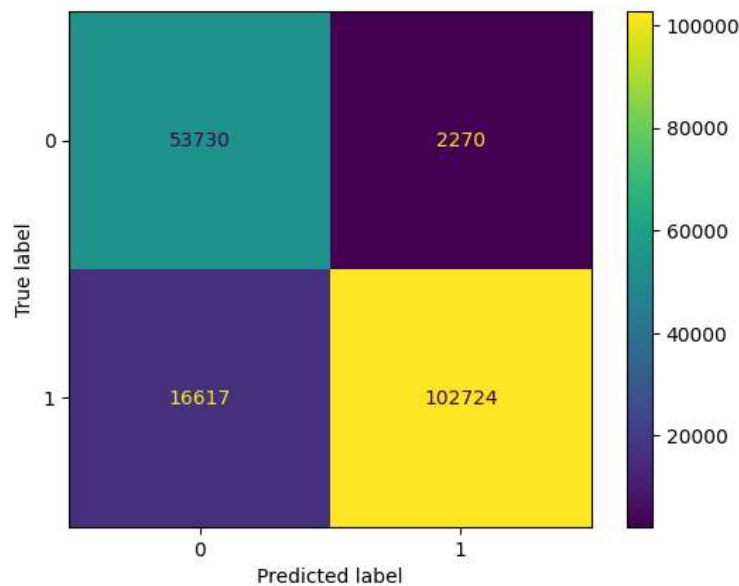
An image-based learning model is created with the help of a convolutional neural network (CNN) to learn nonlinear and spatial relations between traffic characteristics. A feature-

matrix encoding is applied to each network traffic record to convert it into a grayscale image, which makes it learn spatial features.

The CNN-based model has an accuracy of 89.26, a precision of 97.93, a recall of 86.04, an F1-score of 91.60, and ROC-AUC of 0.9792 on the test set. In comparison to the signal-based approach, the image-based one produces a significant increase in recall and F1-score, which means that it is more successful in detecting malicious actions.

As Figure 2 shows, CNN successfully recognizes 102,681 samples of attacks and 53,825 normal samples. Although the false positives marginally grow to 2,175, false negatives are greatly minimized to 16,660, which proves that the CNN is more effective in detecting the patterns of complex attacks.

Figure 2: Confusion Matrix — Image (CNN).



This figure gives the confusion matrix of the CNN-based image model where the recall is better and false negatives are lower than the signal-based approach, but false positives are slightly higher.

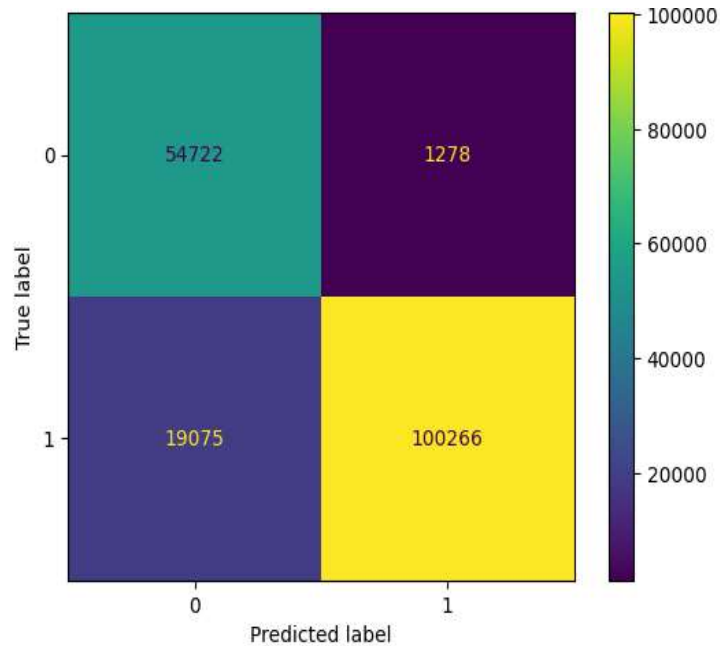
The model based on images emphasizes the usefulness of space features learning in intrusion detection. Through taking advantage of correlations between traffic features, the CNN can identify nonlinear and subtle attack signatures that can be missed by conventional signal-based classifiers.

4.3 Performance of the Combined Signal-Image Architecture

The suggested fusion architecture is a combination of the mutually complementary signal-based and image-based representations by fusing features. Under this method, standardized signal features and image embeddings produced by CNN are combined and classified through a logistic regression decision layer.

The fusion model has an accuracy of 88.30, a precision of 98.74, a recall of 83.89, F1-score of 90.71 and the highest ROC-AUC of 0.9819 of all the models considered. These findings indicate the fusion architecture has the most optimum discriminative capability.

As indicated in the confusion matrix in Figure 3, the fusion model correctly labels 100,115 attack samples and 54,718 normal samples, and the number of false positives is the lowest of all models, 1,282. The false negatives (19,226) are a bit more than the CNN model, but still, they are significantly lower than the signal-based baseline.

Figure 3: Confusion Matrix — Fusion Architecture.

This figure shows the performance of the proposed fusion model in terms of classification, which has the lowest false-positive rate and a balanced trade-off between precision and recall.

The fusion strategy is a good compromise between the detection and security reliability. The decrease of false positives is of importance especially when deploying it in the real world where too many alerts may overwhelm security operators.

4.4 Comparative Performance Analysis Using Evaluation Metrics

Table 1 offers a summarized view of evaluation metrics, a comparative analysis of all three models.

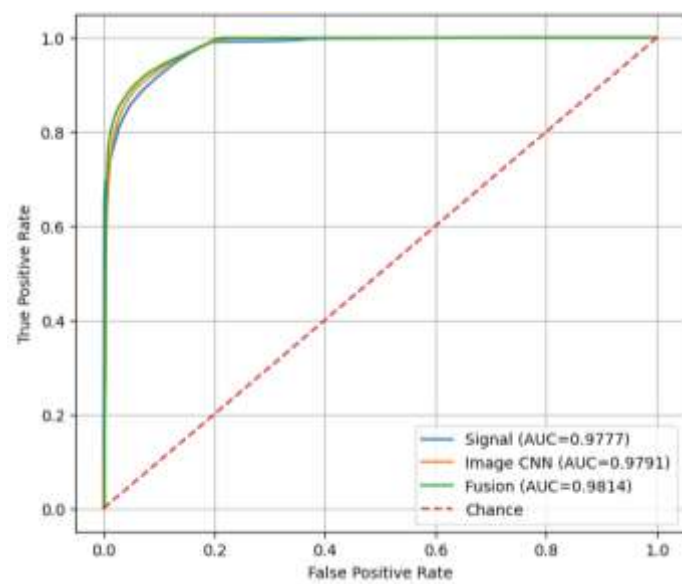
Table 1: Performance Comparison of Signal, Image, and Fusion Models.

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
Signal (LogReg)	0.8630	0.9837	0.8123	0.8898	0.9777
Image (CNN)	0.8926	0.9793	0.8604	0.9160	0.9792
Fusion	0.8830	0.9874	0.8389	0.9071	0.9819

The accuracy, precision, recall, F1-score, and ROC-AUC of the evaluated models are compared in this table and show the complementary strengths of each method.

Among the single-branch models, the signal-based model has the best accuracy which proves its appropriateness in reducing false alarms. The CNN based on images has the best recall and F1-score indicating that it is better in detecting malicious traffic. The fusion architecture has the best ROC-AUC and precision in general, which implies a better separability and robustness.

The additional information can be obtained by the ROC curves presented in Figure 4. Each of the models is a great improvement over random classification with the fusion model having the highest area under the curve.

Figure 4: ROC Curves Comparison for Signal, Image, and Fusion Models.

This value is used to compare the ROC curves of the three models and show the best discriminative ability of the proposed fusion architecture by the highest AUC value.

The trends herein observed show that signal-based and image based models represent complementary features of network traffic behavior. Signal-level features focus on the statistical regularities and accuracy, whereas image-based features reflect on the spatial and nonlinear regularities. When they are integrated by means of fusion, they come up with a more reliable and secure intrusion detection system.

It has been proven through the experiment that signal-based learning provides a solid foundation of intrusion detection due to high accuracy and low false-positive rate, which is essential in security-intensive settings. Image based learning also increases the performance in detection by greatly boosting the performance in recall and detection of complex and unfamiliar attack pattern. More importantly, the suggested signal-image fusion architecture successfully combines the strength of the two methods, which is complementary to each other, leading to the optimal performance in terms of the highest ROC-AUC and the lowest false-positive rate of all the tested models. Taken together, these results confirm the usefulness of secure signal and image processing architectures in next-generation cyber defense and offer a good rationale behind the architectural and methodological design decisions that were taken in this research.

5. Discussion

The experimental findings of this research give valuable information about the efficiency of the combination of signal processing and image processing into a single machine-learning-based cyber defense architecture. The comparative analysis shows that both signal-based and image-based models have their own advantages, and when used together, by means of feature-level fusion, they produce a stronger and more reliable intrusion detection system. The result validates the hypothesis proposed at the beginning that multi-modal representations are more capable of capturing the complexity of contemporary cyber threats as compared to single-modality representations.

Regarding the interpretation of performance, it is possible to state that the signal-based learning model is exceptionally high in precision and a high ROC-AUC, which shows that this model has a low false positive rate. This is vital in operational security settings where

too much alerts may cripple analysts and compromise trust in the system. These results are consistent with the previous studies that have highlighted the trustworthiness and comprehensibility of statistical and signal-based machine learning methods in the context of intrusion detection, especially in settings where elucidation is fundamental [12]. The false negatives however observed could mean that signal based representations might not be able to capture advanced or sophisticated attack patterns particular those that can be used to interfere with or mimic normal traffic behavior.

To overcome this shortcoming, the image-based learning model uses convolutional neural networks to derive spatial patterns of transformed traffic representations. The increased recall and F1-score of CNN prove its high ability to detect complex and nonlinear attack signatures. The same has been observed in earlier research which also uses image based encodings of network traffic to improve detection performance [13]. However, the slightly higher false-positive rate of the CNN model is an indicator of a trade-off that is often linked to deep learning methods, which are more sensitive and thus over-classify benign traffic. The fusion architecture is an important development achieved through the combination of the complementary advantages of the two learning paradigms. The fused model has the best ROC-AUC and the least false-positive rate of all the tested methods, which means that it has a better separability between normal and malicious traffic. This result shows that signal-level statistical and image-level spatial features measure two different, yet complementary, features of network behavior. The fusion methodology balances precision and recall successfully in order to counter the weakness of each branch. This type of hybrid learning approach has been more and more promoted in the recent cyber defense literature as a way of enhancing robustness and generalization [16].

The findings of this work can be compared with the existing literature, and the results are in line with the overall tendencies of research on next-generation cyber defense. Systematic analyses and surveys have highlighted that there is no single machine learning or deep learning model that can always be used in different attack situations [17]. Rather, heterogeneous representation combinations in architectures are known to provide better resilience and adaptability. The suggested signalimage fusion structure can be seen as following this trend because it shows real performance improvements without adding too much computational overhead.

Security wise, the results of such findings are quite serious. Automated intrusion detection systems must be trusted by having high precision and low false-positive rates. The fact that the fusion model can minimize false alarms without compromising the good performance in detection makes it especially applicable to the deployment in security-sensitive systems like enterprise networks, cloud systems, and cyber-physical systems. Moreover, dual representations can be used to increase resistance to evasion attacks, since an attacker would have to manipulate both statistical and spatial feature space in order to evade detection [16].

The issues of scalability and practical deployment are also significant in the assessment of the relevance of the given approach. The signal based branch is computationally efficient and interpretable, which is why it is appropriate in real-time monitoring. The image-based branch, being more computationally expensive, offers this in compact grayscale representations and can be optimized on the current hardware accelerators. The fusion strategy uses a lightweight decision layer, which makes sure that the entire architecture is viable to large scale deployment. These attributes aid the flexibility of the suggested framework to the next-generation network conditions such as the high-throughput and distributed systems [20].

Although it is a strong methodology, there are a number of limitations of the proposed methodology that should be discussed. First, the research is on binary classification and does not examine multi-class attack categorization that may give more specific threat

intelligence. Second, the assessment is performed on a benchmark dataset and practical implementation can bring further issues, including concept drift, encrypted traffic, and changing attack patterns. Third, the fusion architecture enhances robustness, but it does not specifically consider the problem of adversarial machine learning attacks, which is becoming an increasingly important issue in security-critical systems.

The limitations also point out some significant future research directions. The proposed framework can be expanded to multi-class intrusion detection to make it more useful in practice. Online or incremental learning mechanisms may be included in order to enhance flexibility to changing threats. Also, adversarial training or defensive training may be considered to make targeted attacks even more robust. It would also make the proposed approach more applicable in resource-constrained settings like IoT and industrial IoT systems [21].

Altogether, the discussion proves that joint signal and image learning is a prospect of the next-generation cyber defense. The proposed architecture is more robust, has better detection performance, and is more practically feasible due to systematic combination of complementary representations into a machine-learning structure. The results of the study help the current development of effective and safe intrusion detection systems and offer a good base to further improvements in the multi-modal research on cyber defense.

6. Conclusion

This paper introduced a safe signal and image processing framework on machine learning to support next-generation cyber defense and confirmed the functionality using the UNSW-NB15 benchmark dataset. Its primary contribution is the creation and analysis of a dual-branch structure, which simultaneously uses statistical signal representations and spatial image-based representations of network traffic. Through experiments, the signal-based learning model has been found to provide a high baseline performance with a very high precision and low false-positive rates, rendering it to be applicable in security-critical settings. The image-based learning model also enhances the detection ability by enhancing the recall and capturing the multifaceted nonlinear attack patterns using convolutional neural networks. Most significantly, the suggested signal-image fusion architecture combines the overall discriminative power of both methods, which is the highest ROC-AUC values and balanced trade-off between precision and recall. These findings substantiate that coherent multi-modal learning systems are much robust and reliable than single-modality intrusion detection systems. In a practical perspective, the proposed architecture is compatible with the next-generation cyber defense needs where dynamically, precise, and low-noise detection systems are needed in the face of more advanced attacks. The fusion based design also enhances resilience to avoid evasion since it is not dependent on a single feature space. Nevertheless, in spite of these strengths, the study is restricted to binary intrusion detection and offline evaluation based on a benchmark dataset, which might not be a full picture of the real world deployment issues. Future studies should build on the framework by adding multi-class attack classification, online and real-time learning, and adversarial robustness by defensive measures. Further research on implementation in resource-constrained systems, such as IoT and industrial cyber-physical systems, is also encouraged on a global scale.

References:

1. Z. Ali, T. Hussain, C. L. Su, M. Sadiq, A. D. Jurcut, S. H. Tsao, et al., "A New paradigm for adaptive cyber-resilience of DC shipboard microgrids using hybrid signal processing with deep learning method," *IEEE Trans. Transp. Electrification*, 2024.

2. N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," *Knowledge and Information Systems*, pp. 1-87, 2025.
3. S. Srivastava, H. K. Bhargav, V. Gurani, A. Chaturvedi, A. Gandhi, and Y. Dharangutti, "Next-Generation Cyber Defense: Deep Q-Learning-Based Adversarial Detection and Prevention in Autonomous Vehicle Networks," in *Proc. 2024 4th Int. Conf. Mobile Networks Wireless Commun. (ICMNWC)*, 2024, pp. 1-7.
4. F. O. Catak, M. Kuzlu, H. Tang, E. Catak, and Y. Zhao, "Security hardening of intelligent reflecting surfaces against adversarial machine learning attacks," *IEEE Access*, vol. 10, pp. 100267-100275, 2022.
5. R. Akbar and A. Zafer, "Next-Gen Information Security: AI-Driven Solutions for Real-Time Cyber Threat Detection in Cloud and Network Environments," *J. Cybersecur. Res.*, vol. 12, pp. 123-145, 2024.
6. S. Malik, P. K. Malik, and A. Naim, "Opportunities and challenges in new generation cyber security applications using artificial intelligence, machine learning and block chain," *Next-generation cybersecurity: AI, ML, and Blockchain*, pp. 23-37, 2024.
7. Z. Ali, T. Hussain, C. L. Su, G. Parise, K. Sayler, M. Sadiq, et al., "A novel hybrid signal processing based deep learning method for cyber-physical resilient harbor integrated shipboard microgrids," *IEEE Trans. Ind. Appl.*, 2025.
8. M. Adil, A. Farouk, H. Abulkasim, A. Ali, H. Song, and Z. Jin, "NG-ICPS: next generation industrial-cps, security threats in the era of artificial intelligence, and open challenges with future research directions," *IEEE Internet Things J.*, vol. 12, no. 2, pp. 1343-1367, 2024.
9. Z. Ali, T. Hussain, C. L. Su, I. Khan, A. D. Jurcut, S. H. Tsao, et al., "Deep learning-driven cyber attack detection framework in dc shipboard microgrids system for enhancing maritime transportation security," *IEEE Trans. Intell. Transp. Syst.*, 2025.
10. M. Kuzlu, F. O. Catak, Y. Zhao, S. Sarp, and E. Catak, "Security and privacy concerns in next-generation networks using artificial intelligence-based solutions: A potential use case," in *Wireless Networks: Cyber Security Threats and Countermeasures*, Cham: Springer, 2023, pp. 205-226.
11. D. Ghai, S. L. Tripathi, S. Saxena, M. Chanda, and M. Alazab, Eds., *Machine learning algorithms for signal and image processing*. John Wiley & Sons, 2022.
12. Y. E. Sagduyu, S. Ulukus, and A. Yener, "Task-oriented communications for NextG: End-to-end deep learning and AI security aspects," *IEEE Wireless Commun.*, vol. 30, no. 3, pp. 52-60, 2023.
13. H. Gonaygunta, G. S. Nadella, P. P. Pawar, and D. Kumar, "Study on empowering cyber security by using Adaptive Machine Learning Methods," in *Proc. 2024 Systems and Information Engineering Design Symposium (SIEDS)*, 2024, pp. 166-171.
14. J. Yu, A. V. Shvetsov, and S. H. Alsamhi, "Leveraging machine learning for cybersecurity resilience in industry 4.0: Challenges and future directions," *IEEE Access*, 2024.
15. M. Praneesh and N. Nivetha, "A Survey of Deep Learning Algorithms and Methods for Automated Cyber Security in Healthcare," in *Leveraging Artificial Intelligence (AI) Competencies for Next-Generation Cybersecurity Solutions*, pp. 473-486, 2024.
16. R. Ajayi and M. Masunda, "Integrating edge computing, data science and advanced cyber defense for autonomous threat mitigation," *Int J Sci Res Arch*, vol. 15, no. 2, pp. 63-80, 2025.
17. C. Gupta, I. Johri, K. Srinivasan, Y. C. Hu, S. M. Qaisar, and K. Y. Huang, "A systematic review on machine learning and deep learning models for electronic information security in mobile networks," *Sensors*, vol. 22, no. 5, pp. 2017, 2022.

18. K. Demertzis and L. Iliadis, "An autonomous self-learning and self-adversarial training neural architecture for intelligent and resilient cyber security systems," in Proc. Int. Conf. Engineering Applications Neural Networks, Cham: Springer, 2023, pp. 461-478.
19. H. Maryam, Z. N. Zukhruf, and R. Ullah, "Comparative Analysis of Machine and Deep Learning for Cyber Security," in Cyber Security for Next-Generation Computing Technologies, pp. 39-69, CRC Press, 2024.
20. P. S. Vijayalakshmi and M. Jayakumar, "Deep Neural Networks for Automated Cyber Security: Identification of Dynamic Malware in Cloud Computer Networks," in Leveraging Artificial Intelligence (AI) Competencies for Next-Generation Cybersecurity Solutions, pp. 139-173, Apple Academic Press, 2024.
21. M. Sagar and C. Vanmathi, "A comprehensive review on deep learning techniques on cyber attacks on cyber physical systems," SN Comput. Sci., vol. 5, no. 7, p. 891, 2024.
22. S. Gaba, I. Budhiraja, V. Kumar, S. Martha, J. Khurmi, A. Singh, et al., "A systematic analysis of enhancing cyber security using deep learning for cyber physical systems," IEEE Access, vol. 12, pp. 6017-6035, 2024.
23. N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in Proc. IEEE Military Communications and Information Systems Conf. (MilCIS), Canberra, ACT, Australia, Nov. 2015, pp. 1-6. [Online].
24. <https://www.kaggle.com/datasets/harshwardhanbhangale/unsw-complete-dataset>