Integrative Insights into Hybrid CNN–Autoencoder Models for Security Threat Detection in Cloud Environments

D. Fernandez Raj[1], Dr B V V Siva Prasad[2]
[1]*Research Scholar, Texas Global University*
[2]*Research Supervisor, Texas Global University*

***Abstract*—This synthesizing paper summarizes the conclusions of the four previous papers that look at the Hybrid CNN -Autoencoders to detect security threats in clouds. With the gradual but steady increase in scale and complexity of cloud computing emergence, traditional intrusion detectors systems (IDS) are becoming unsuitable in the face of the advanced and dynamic character of cyber threats. The papers collectively examine different areas of Hybrid CNN - Autoencoder model such as its performance, optimization approaches, comparative analysis, and the architectural mechanisms that have been employed in the effective identification of known and unknown threats. This hybrid model is much better in detection accuracy, computational efficiency, and scalability than the traditional machine learning (ML) and deep learning (DL) models because it utilizes the Convolutional Neural Networks (CNNs) to extract the features and the Autoencoders to detect the anomalies. These techniques are combined in a manner that enables the model to efficiently model the spatial relationship of network traffic and log data as well as detect new attack patterns via the reconstruction error of the Autoencoder. These papers have been synthesized to show that the model is viable in real time cloud security applications. These and many other optimization methods, including hyperparameter tuning, feature selection, and model regularization, are also covered in the study and contribute to making it more efficient and consume fewer resources, thus it is applicable in resource-constrained cloud environments. Moreover, the paper discusses the implication of these findings, which can be of great importance in the future research context and practical implementation of such systems to achieve strong cloud security. The findings of the synthesis indicate that the Hybrid CNN-Autoencoder model is a prospective solution to such dynamic and complex security issues of the cloud environment, where both high-detection rates and low-computation rates are provided. Future work suggestions are to broaden the capabilities of the model in order to deal with a broader variety of attack vectors, to optimize it more in real-time cloud environments, and to investigate how to make use of it with edge computing and low-power devices.**

***Index Terms*—Hybrid CNN–Autoencoder, Cloud Security, Intrusion Detection, Anomaly Detection, Feature Extraction, Deep Learning, CNN, Autoencoder.**

I. INTRODUCTION

With the emergence of cloud computing, the information technology arena has been transformed in the sense that it offers organizations unprecedented flexibility, scalability, and cost-efficiency [1]. The cloud platform enables companies to store large volumes of data, perform intricate calculations, and dynamically increase or decrease their infrastructure to satisfy the variable demands [2]. Nevertheless, there are serious security issues that have also been posed by cloud computing in addition to the advantages. As cloud systems continue to grow in complexity and scale, new and advanced cyber threats are becoming a reality and it is becoming more difficult to effectively detect and address them using the old security mechanisms [3]. There is a rise in cyber-attacks such as DDoS (Distributed Denial of Service), data breaches, malicious insiders and zero-day attacks that are threatening sensitive cloud-based data. Another element that is becoming unsuccessful in addressing these sophisticated threats is traditional security systems including rule-based Intrusion Detection Systems (IDS) [4][5]. Rule based IDS use predefined patterns or signatures to identify known

attacks, and fail to identify new and unknown attack patterns, particularly in dynamic and changing cloud settings. This shortcoming has led to the use of machine learning (ML) and deep learning (DL) models, which can change and learn the data patterns in real-time, which is more appropriate in detecting complex and previously unknown threats [6][7][8].

Deep learning architectures and specifically Convolutional Neural Networks (CNNs) and Autoencoders have attracted much interest as having the potential to enhance the performance of Intrusion Detection Systems (IDS). CNNs are especially good at learning spatial and hierarchical representations of massive quantities of unstructured data like network traffic and logs, whereas Autoencoders are skilled at detecting anomalies through learning the standard data distribution and reporting outliers [9][10]. These two methods combined to create a Hybrid CNN-Autoencoder can be used as a potential solution to enhance detection accuracy and efficiency in cloud-based IDS. The CNN part of the model derives useful features of raw input data, i.e., network traffic and system logs, which are usually complex and high-dimensional data. The Autoencoder then becomes trained to recreate the normal behavior of the system and detects abnormalities by studying the reconstruction error which points out the deviations of normal patterns. The hybrid model can be used to identify known and novel threats with high accuracy, robustness, and computational efficiency by utilizing both CNNs and Autoencoders. In this paper, the author summarizes the results of the four papers presented above discussing the use of the Hybrid CNNAutoencoder model to detect security threats in the cloud environment. The collective aspect of these papers deals with the key areas like the model architecture, performance evaluation, optimization techniques, and comparative evaluation with other state-of-the-art models. This integrative work aims to unify these findings and provide a holistic view on the possibility of using this hybrid model to enhance cloud security not only in the accuracy of detection but also in the computational efficiency. The synthesis will also examine the implication on the future research, and the applications that these findings will have into the reality of cloud environments. The paper will be useful in contributing to the knowledge of the advantages and drawbacks of the Hybrid CNN-Autoencoder model, and it will form a basis of future developments in securing clouds. The application of machine learning and deep learning models to improve the security of clouds is an important step towards meeting the increasing security concerns in clouds.

II. OVERVIEW OF HYBRID CNN–AUTOENCODER MODEL

Hybrid CNN-Autoencoder model combines two highly effective deep learning models; Convolutional Neural Networks (CNNs) and Autoencoders to help solve the challenging and dynamic problem of threat detection on clouds. With cyber threats recently becoming more advanced, the conventional Intrusion Detection Systems (IDS) cannot detect unknown or zero-day attacks. The solution is a powerful combination of the two worlds by taking the best out of both feature extraction and anomaly detection: the two worlds.

Convolutional Neural Networks (CNNs) for Feature Extraction

Convolutional Neural Networks (CNNs) is the first element of the hybrid model and it is famous because of its capability to automatically acquire hierarchical features of input data. In cloud security, CNNs can especially be useful in feature extraction of large, high-dimensional data, including network traffic and system logs. Such datasets, which may be unstructured data (such as raw logs or traffic flow data), may be hard to analyze effectively using traditional methods. CNNs are good at identifying patterns in space and hence are suitable in managing the multidimensional nature of cloud data. Indicatively, CNNs are capable of establishing correlations and dependencies among several network traffic properties including packet size, protocol type, and connection length. CNNs convert raw input data into meaningful feature maps by use of convolutional filters and pooling operations and subsequently, it is processed further, e.g., classification or anomaly detection. This capability to find spatial relationships in the data is particularly valuable in the cloud, where the traffic and system logs are usually large and complex, whose trends might not be instantly apparent to conventional signature-based IDS.

Autoencoders for Anomaly Detection

The second part is Autoencoders which is a form of unsupervised learning algorithm employed in detection of anomalies. Autoencoders are trained so as to generate a low-dimensional representation of the input data, which captures the key features and eliminates the unwanted noise. These are divided into two components, namely, the encoder, or compression of the input data into a lower-dimensional latent space, and the decoder, or reconstruction of the original input using this compressed representation. Within the framework of the Hybrid CNN -Autoencoders model, the Autoencoders part is utilized to identify anomalies through the difference between the reconstructed information and the original input. This discrepancy can be termed as reconstruction error and it indicates the effectiveness of the model in learning the normal patterns of network traffic and system behaviour. In case the reconstruction error is too large, then this is an indication that the input information is not within the normal range that the model has been taught to be normal and as such, an anomaly exists, possibly an attack or intrusion.

Autoencoders are also effective because they identify new attacks, which lack predefined signatures, and as such, can be used especially to identify new or emerging threats. Autoencoders are able to indicate previously unknown anomalies, unlike traditional signature-based approaches, which are based on known attack patterns, providing a clear benefit in dynamic clouds, which are constantly changing attack vectors.

Hybrid Approach for Improved Detection

The Hybrid CNN-Autoencoder model is a combination of CNNs and Autoencoders that exploits the capabilities of the two architecture models to provide a complete solution to the problem of detecting cloud security threats. The CNN module is concerned with learning significant spatial features of the raw input data, whereas the Autoencoder is concerned with detecting anomalies of learned normal behavior. The combination of these elements renders the model strong and adaptable and is able to identify both familiar and unfamiliar threats within cloud environments. The CNN is useful in learning both local and global trends based on network traffic and system logs, whereas the Autoencoder has the potential to identify abnormal behaviors based on the re-created data that do not match the normal patterns that had been learned. This combination enables the model to encompass a wider range of attacks including known signature attacks and new unknown attacks which can arise in the dynamic cloud environment.

Optimization Strategies

In order to make sure that the model will be efficient in real-time cloud environment, a number of optimization strategies have been adopted to improve the performance and computational efficiency:

- Hyperparameter Tuning: Hyperparameters of the model are adjusted to optimize the model, including the learning rate, the batch size, and the number of CNN filters. This is to ensure that this model converges in an effective way and does not over or underfit.
- Feature Selection: In cloud security, the amount of data may be massive, and it is significant to pay attention to the most important features. The use of feature selection methods, including Principal Component Analysis (PCA), allows to reduce data dimensionality, which will make the model more efficient without losing important patterns to identify.
- Regularization: In order to prevent overfitting and enhance the performance of the model in generalizing to unseen data, regularization methods like L2 regularization (Ridge) and Dropout are used. These methods make the model to be robust even in cases where it is subjected to noisy or incomplete information.
- Model Pruning and Quantization: These methods of optimization can be used to minimize the complexity and cost of computations of the model, which is especially relevant when using it in constrained resources (such as edge devices or low-power cloud servers). Quantization minimizes the accuracy of the weights of the model, and pruning eliminates the irrelevant connections between the neurons, enabling faster inference.

Scalability and Efficiency

The Hybrid CNN Autoencoder model has been shown to be scalable which is one of its main strong

points. It is capable of managing the huge cloud computing environment with plenty of network traffic and system logs, without incurring performance losses. The model can be used in real time by employing optimized methods and consumes less resources. It is important to cloud security applications, in which speed of detecting threats is essential, and the amount of computational capacity is frequently constrained. Hybrid CNNAutoencoder model integrates the advantage of CNNs in extracting spatial features and Autoencoders in anomaly detection, which presents a powerful and versatile solution to cloud security threat detection. This capability of the model to identify known and new threats, along with its optimization mechanisms, makes it ideal to operate in dynamic cloud environments, and the model provides a scalable and computationally efficient approach to real-time security surveillance.

III. SYNTHESIS OF KEY FINDINGS FROM PAPER 1

Hybrid CNN–Autoencoder Model for Anomaly and Intrusion Detection

Paper 1 presented the Hybrid CNNAutoencoder model as a new approach to the problem of anomaly and intrusion detection in a cloud environment with a particular focus on its innovative architecture and the mutual interaction between Convolutional Neural Networks (CNNs) and Autoencoders. This paper mainly focused on how the two deep learning methods can be used together to deal with the dynamic and multifaceted nature of cyber threats to cloud infrastructure. This hybrid architecture capitalizes on the strengths of CNNs in feature extraction and Autoencoders in anomaly detection to offer a powerful, scalable and efficient architecture to solve the problem of real-time security monitoring in clouds. Among the most important contributions of Paper 1 was the fact that CNNs were shown to be effective in extracting features of complex data sources, including network traffic and system logs. CNNs are characterized with the capacity to acquire hierarchy and spatial connections in data. When it comes to cloud security, network traffic and system logs are usually unstructured and high-dimensional and cannot be easily processed using the traditional approach. CNNs are good at automatically detecting and identifying spatial characteristics of the data, e.g. packet size, packet duration, protocol types, connection state, and other traffic patterns. The CNNs operate on the principle of convolutional layers to identify local patterns in the input data and transfer them to more abstract representations in the lower layers. This spatial dependence ability between various features is necessary to understand the correlation between various properties of network traffic or system logs. The CNN module can detect attack patterns and differentiate normal and malicious behavior in the cloud-based systems by using several convolutional filters. The second significant element of the hybrid model is the Autoencoder that is significant in identifying anomalies. The Autoencoder is based on a data-driven approach in contrast to traditional signature-based methods that are based on a predefined pattern of attacks to learn the underlying structure of normal behavior. The Autoencoder is trained on a dataset of normal behavior, and is then asked to encode the input into a lower-dimensional latent representation, and then is asked to decode the input with this compressed encoding. When an input data point does not match the learned normal patterns significantly, the reconstruction error will be large, which means that the input is an anomaly. This renders the Autoencoder especially useful in identifying new or the first occurrence of attacks, which might not be detected by the conventional approach that uses signature databases. The error of reconstruction is an important metric to detect possible intrusions and is important to make sure that the model can identify even the zero-day attacks or a new attack pattern.

Ability to Detect Both Known and Unknown Attacks

The fact that the Hybrid CNN–Autoencoder model is capable of detecting known and unknown attacks is one of the strongest points of this model. The conventional signature-based IDS solutions are poor in detecting new attacks that are not observed or registered in their signature databases. CNNAutoencoder hybrid, however, does not have this shortcoming, and it uses the power of CNNs in terms of feature extraction and the strength of Autoencoders in terms of the anomaly detectors. The capability of the CNN to recognize well-defined patterns of attacks is due to its capability of capturing intricate spatial patterns. In the meantime, the

Autoencoder offers the possibility of identifying unknown attacks or zero-day attacks, which do not conform to the patterns that the conventional models already know. This twofold strategy will increase the overall strength and adaptability of the model and will allow it to adjust to the quickly changing environment of cyber threats.

High Detection Accuracy Across Various Threat Types

Paper 1 showed that Hybrid CNN Auto encoder model exhibited high detection accuracy with various forms of threats. The architecture of the model helps it to effectively categorize normal and malicious behavior even in the presence of complicated attacks. The spatial feature learning property of CNN enables it to effectively address the fluctuations in network traffic and logs, and the anomaly detection mechanism of the Autoencoder also increases the capabilities of the model to detect uncommon and new threats. The model was tested on a wide range of datasets, both with known and unknown attack scenarios, and could achieve high accuracy and minimize false positives, a typical issue with conventional IDS systems. The system of the hybrid model that enables it to detect high rates and reduce false alarms is an important resource towards cloud security. The paper has also presented the necessary data preprocessing methods which help to make the model effective. Time-window aggregation is employed to synchronize network traffic and system logs, so that the data is consistent and comparable at the various time periods. The cloud environments are known to produce large volumes of data over time, therefore, time-window aggregation aids in the division of the data into manageable units which can be processed efficiently by the model. The model can identify patterns of behavior that can change over time by aggregating the data over certain time windows and this is important in identifying slow moving attacks such as DDoS or data exfiltration. Also, the paper has emphasized the role of feature normalization in the input data preparation of deep learning models. The normalization process guarantees that every feature is scaled to a comparable value so that an individual feature does not overtake the learning process. This process is essential to deep learning models such as CNNs and Autoencoders as it assists the models in learning the association between features better and enhances model convergence in training.

Conclusion from Paper 1

To sum up, Paper 1 provided the foundation to the knowledge of the architecture and the benefits of the Hybrid CNN-Autoencoder model in cloud networks when it comes to intrusion detection. The results highlighted how the model was able to identify known and unknown attacks, as well as its high detection rate, and the successfulness of data preprocessing methods such as time-window aggregation and feature normalization. All these features precondition that the hybrid model will be a successful proposal to modern dynamical cloud environments where threats are constantly changing, and the amount of data is constantly increasing.

IV. SYNTHESIS OF KEY FINDINGS FROM PAPER 2

Evaluating the Performance of the CNN–Autoencoder Model

The theme of Paper 2 was the analysis of the Hybrid CNN -Autoencoder model performance in the security threat detection in clouds. It directly compared this hybrid framework with the other popular machine learning (ML) and deep learning (DL)-based Intrusion Detection System (IDS) frameworks including CNNs, Autoencoders, and Long Short-Term Memory (LSTM) networks. The objective was to test the capability of the model in terms of detecting known and unknown threats as well as its efficiency and scalability in terms of calculation and robustness. The notable results of Paper 2 were that the Hybrid CNN-Autoencoder model performed well compared to the conventional CNN, Autoencoder and LSTM-based IDS models. The comparison showed that the proposed hybrid model was always doing better than these existing models in various performance measures, such as accuracy of detection, precision, and recall.

- Detection Accuracy: The hybrid model had a much greater detection accuracy in detecting intrusions and anomalies in the cloud environments. The hybrid model could detect anomalies more accurately than either CNNs to extract features or Autoencoders to detect anomalies because it could combine the strengths

of both models. The capability of CNN module to obtain the spatial relationship in the traffic and logs was coupled with the capability of the Autoencoder to identify new attacks leading to an enhanced precision.

- Precision and Recall: The hybrid model was also found to perform remarkably in terms of precision and recall besides accuracy. Precision is the quality of the model to identify all attacks with low number of false positive, whereas recall is the quality of the model to identify all attacks (i.e. identify all attacks correctly). The hybrid model could continue to achieve a trade-off between precision and recall to reduce the false positives and false negatives. This feature is of particular importance in a cloud environment, where false alarms cost can be high.

Ability to Detect Known and Novel Threats

One of the strongest points of the Hybrid CNN - Autoencoder model discussed in Paper 2 was that it had the capability to identify known and unknown threats. Conventional IDS, including signature systems, do not have sufficient capabilities of detecting unknown or zero-day attacks. Nevertheless, the hybrid model can successfully overcome this limitation by integrating CNNs and Autoencoders.

- CNNs can be used to learn spatial features, which capture typical network traffic behaviors in order to detect known attack patterns. The model is storing these pre-existing patterns in the form of signatures that enable it to classify the known attacks correctly.
- Autoencoders, in their turn, are concentrated on the detection of anomalies, which are not normal by the learned behavior, and the hybrid model is really efficient when it comes to detecting new forms of attack that have never been observed previously. The reconstruction error of the Autoencoder can be used as an effective signal to identify previously unknown attacks and thus can add a great deal of value to the model of making it more robust and capable of addressing the changing threats.

Consequently, the Hybrid CNN-Autoencoder model proved to be flexible enough to work in a real-world environment of clouds, where new strategies are being invented by attackers. The capability of the model to identify new and old threats helps organizations to remain ahead of a possible attack even in cases where the attack has not been detected or listed. The other important metric that was discussed in Paper 2 was the Area Under the Curve (AUC) of the Receiver Operating Characteristic (ROC) curve, which is employed to measure the capability of the model to differentiate normal behavior and attacks. The AUC score is useful in the determination of the ability of the model to discriminate between the two classes with varying threshold values. The Hybrid CNNAutoencoder model had an AUC of 0.85, which is a promising outcome of IDS models in the cloud. The AUC of 0.85 shows that the model is moderately to good in performance because it is good in distinguishing between normal and attack classes. This score still puts the model in a good position to be used in real-time cloud security systems though the AUC can be further enhanced. The capability to obtain a high AUC and at the same time high precision and recall highlight the fact that the model has a balanced performance and thus can be used as a reliable and robust IDS solution in dynamic settings. Paper 2 also pointed out the importance of model optimization to improve the performance of the Hybrid CNN - Autoencoder model. It was demonstrated that hyperparameter tuning, feature selection, and regularization techniques were significant to enhance the work of the model and reduce the computational costs.

- Hyperparameter Tuning: With the modification of the following important hyperparameters, including the learning rate, batch size, and the number of layers within the CNN and Autoencoder components, the model could attain a faster convergence and increased detection accuracy. The fine-tuning of these hyperparameters can be useful in making the model fit particular cloud conditions so that they can work well in different conditions.
- Feature Selection: The feature selection process was to select the most applicable features among the raw network traffic and log information to enhance the training efficiency of the model. The model was made to concentrate on main patterns related to attacks by eliminating irrelevant or noisy features.

- Regularization Techniques: To avoid overfitting that is a usual issue in deep learning models, regularization techniques were used (dropout and L2 regularization). This makes sure that the model is very generalizable to unseen data and this enhances its performance in real-world setting.

Conclusion from Paper 2

Finally, as it was shown in Paper 2, Hybrid CNN-Autoencoder model is significantly more effective than the traditional CNNs, Autoencoders, and LSTM-based IDS models in identifying cloud security threats. The fact that it can detect both known and novel attacks and is highly accurate, precise, and recalls it as ideal solution in real time security monitoring. Moreover, optimization methods of the model, including hyperparameter tuning, feature selection, and regularization, help to obtain high performance and guarantee the efficient utilization of resources, which is why the hybrid model can be successfully deployed in the dynamic cloud environment.

V. SYNTHESIS OF KEY FINDINGS FROM PAPER 3

Optimizing Cloud Security Performance and Computational Efficiency

Paper 3 was concerned with optimizing the cloud security performance and computational efficiency of the Hybrid CNN -Autoencoder model by using a number of optimization methods. Although the CNN-Autoencoder model proved effective through its performance in the detection accuracy and its capability to detect known and unknown threats, scale and complexity of cloud environment meant that more attention had to be paid to the way the model could be optimised to be deployed in real-time. In this paper, a detailed discussion of some optimization techniques that will aid in enhancing detection latency, resource overhead, and energy consumption without compromising on high-performance and scalability was given. The essence of the optimization process was to increase the efficiency of the model without affecting its accuracy of detection. Real-time intrusion detection systems (IDS) are required more than ever in cloud environments, as they are getting increasingly complex. Conventional models may be computationally intensive and hence slow which makes it hard to identify threats in dynamic clouds. In order to overcome these issues, Paper 3 proposed a number of optimization measures that have been of great help to the efficiency of the model in its operation.

1. Learning Rate Scheduling

The learning rate scheduling was one of the main optimization methods described, and it is essential to ensure that the convergence is faster and that the model performance is also stable. The learning rate in deep learning dictates the extent to which model weights are changed at a given time. When the learning rate is excessive, the model can be prone to converging faster and missing the best solutions whereas low learning rate can cause the model to converge slowly hence consuming more time to train. Paper 3 demonstrated that the model was capable of changing the learning rate in training according to its performance by applying the dynamic learning rate scheduling. This adaptive method assisted the model to converge faster, thus increasing the effectiveness of the training process and accelerating the detection procedure. The paper established that the model could converge much faster by beginning with a high learning rate and slowly decreasing the rate, achieving accuracy and thus it would be more applicable in real-time detection in cloud settings.

2. Batch Normalization

Another important method is the batch normalization that is employed to enhance the performance and stability of the model. It solves the issue of internal covariate shift that happens when the distribution of activations varies throughout training, and thus, it becomes more difficult to learn effectively by the model. The process of batch normalization is used to normalize the activation of every layer and is used to maintain the data distribution across the network. The addition of batch normalization to the CNNAutoencoder model demonstrated that the model was able to train more effectively and less prone to overfitting resulting in better generalization (Paper 3). This also assisted in cutting down the training time and the model is more appropriate in the real time application where latency of the detection is vital.

3. Network Pruning

Network pruning is a method of making a neural network smaller and less complicated without impairing the performance of a network to a great degree. Model size and computational overhead can be important bottlenecks in large-scale cloud environments, where the amount of computational resources can be small. Pruning is the process of eliminating redundant neurons or connection in the network and this reduces the parameters and memory footprint of the model. Network pruning was used in Paper 3 to apply the CNN-Autoencoder model to eliminate unnecessary model parameters that did not lead to a better detection accuracy. The pruning of the network enabled the model to be more efficient and consume fewer computational resources in order to be faster and use less energy with high detection accuracy. The pruned model was particularly useful in resource-constrained environments, including edge devices or low-power cloud systems. Balancing high detection accuracy and low computation cost was one of the major issues in Paper 3. Computational overhead and latency are key issues in a cloud environment, especially when there is a need to detect the threat in real-time. Although deep learning models, such as CNNAutoencoder model, are characterized by the high detection accuracy, they may be resource demanding and slow, particularly when used with large-scale datasets or when multi-source data processing is required. The paper has stressed on the aspect of tuning model architecture to achieve the best trade off of accuracy and efficiency. The model could be customized to be effective in real-time by using fewer parameters, adjusting the number of CNN layers, and the size of the latent space of the Autoencoder without compromising the threat detection capabilities of the model. Among the key findings of Paper 3, it can be said that the optimized Hybrid CNN-Autoencoder model is not only precise but efficient to the extent of being able to detect security threats in clouds in real-time. The optimization strategies mentioned combined, i.e. learning rate scheduling, batch normalization, network pruning, allowed the model to run at high speeds and still achieve high accuracy. This qualifies it to be used in large-scale cloud security system where speedy detection and reaction are of the essence in reducing the effects of cyber-attacks. Besides, these optimizations manifested that the model was able to operate in dynamic cloud-based systems where the amount and nature of data could vary quickly. The large data-handling capability and minimum latency and resource utilization of the model leading to its use in cloud environments due to the need to use it to monitor and detect threats in real-time. According to the results of Paper 3, the Hybrid CNN -Autoencoder model, optimized, is a scalable solution and can be deployed on large cloud infrastructures. The large scale of the cloud environment means that security systems should be able to handle high amounts of data and dynamically respond to the ever-changing approach of attacks. The hybrid model is also a useful tool to large-scale cloud security systems that require resource efficiency and performance because it optimizes the architecture of the model and makes it computationally efficient.

Conclusion from Paper 3

To conclude, in Paper 3, the significant role of the model optimization is mentioned to enhance the cloud security performance and the computational efficiency of the Hybrid CNN -Autoencoder model. Through the application of methods such as learning rate scheduling, batch normalization and network pruning, the model offered a compromise between high detection and low computation cost which made it a good option in real time security monitoring in large scale cloud applications. The optimized model did not only preserve high performance in detecting known and unknown threats but also minimized the time taken to detect and the amount of resources used, which ensures that it can be deployed effectively in cloud security applications.

VI. SYNTHESIS OF KEY FINDINGS FROM PAPER 4

Comparative Evaluation with Existing Models

Paper 4 was devoted to a comparative analysis of the Hybrid CNNAutomatic encoder model of security threat detection in cloud environments, its effectiveness in comparison with other popular machine learning (ML) and deep learning (DL) models. These were CNN, Autoencoders and Long Short-Term Memory (LSTM) networks that are utilized as well in cloud security in intrusion detection systems (IDS) as well. The present paper

played a significant role in presenting the advantages of the Hybrid CNNAutoencoder model and showing how the model outperforms the classical models in such important metrics as detection accuracy, precision, recall, and AUC (Area Under Curve), which should be considered when assessing the performance of IDS systems.

Comparative Performance Across Key Metrics

The comparative analysis of the paper has shown that the Hybrid CNN -Autoencoder model was always superior in performance metrics to the other deep learning models. These measurements are essential to any security system, especially when using the cloud, where the data quantity and intricacy may overwhelm the conventional security frameworks. The Paper 4 results of performance indicated that the hybrid model had better performance in various aspects:

1. Accuracy: Hybrid CNN-

Autoencoder model had the best accuracy in identifying known and unknown threats. This was more noticeable compared to CNN, Autoencoders and LSTM that had lower detection accuracy in real-life cloud security settings. The hybrid model could combine the feature extraction power of CNNs and the anomaly detection power of Autoencoders, which enabled the hybrid model to perform better than other models, particularly the ability to detect novel attack vectors and zero-day attacks.

2. Precision:

Precision is a metric of importance because it evaluates the percentage of attacks that the model correctly identified out of the total number of predictions that the model makes. The Hybrid CNN-Autoencoder model was best in accuracy, i.e. it was lower than the traditional models in terms of false positives. The hybrid model is an efficient and reliable solution as it allows cloud security systems to not be overloaded with unnecessary notifications, which are generated by false alarms, and the malicious activities are accurately classified.

3. Recall:

Recall, or sensitivity, is the rate of true attacks that the model detects successfully. The Hybrid CNN -Autoencoder model also performed better than CNN, Autoencoders, and LSTM models in terms of recall. This implies that the hybrid model was extremely useful in identifying actual positives (i.e. actual attacks), reducing the chance of overlooking any malicious activity. This is especially relevant to the dynamic cloud environment, where the new threats are constantly being generated, and the system should be capable of detecting them on the fly.

4. AUC (Area under Curve):

This is an important measure of the overall performance of a model because it is the score of the model to distinguish between normal behavior and attack behavior at each of the possible threshold values. The Hybrid CNN -Autoencoder model was found to have an AUC of 0.75, which was much better than CNN, Autoencoders and LSTM models. The larger AUC the stronger the discriminatory ability of the model that is, the more effective it is at correctly distinguishing between malicious activity and benign behavior. This capability to attain a high AUC is particularly significant in cloud security systems, where it is essential to detect minor, advanced attacks to guarantee integrity of a system.

Scalability and Robustness of the Hybrid Model

Besides the high performance in detection accuracy and key evaluation indicators, Paper 4 also demonstrated the scalability and strength of the Hybrid CNN -Autoencoder model. Cloud platforms are dynamic and large-scale by nature, and volumes of data are produced in real-time and of different origins. A scalable IDS model must be capable of keeping up with this increasing data volume at a high detection rate with minimum resource usage. The hybrid model was discovered to be scalable in large cloud infrastructure, serving data of multiple sources (including network traffic, system logs and user activity logs) without a great decline in performance. CNNs and Autoencoders had been integrated together, which made the model very flexible because CNNs are able to work with complex patterns in large datasets, and the Autoencoders are able to work with the anomaly detection without having to rely on huge datasets that are labeled. It was found that the hybrid model was strong in the changing attack scenarios, proving to be able to detect attacks that were not observed before or those that were in transition. The ability of the Autoencoder to train normal behavior patterns and alert abnormalities in real-time was also

a critical issue that enhanced the strength of the model. This enabled the model to be able to deal with zero-day attacks, which might not be detected by conventional signature-based techniques. The hybrid model can detect new threats, unlike CNNs, which only focus on the feature extraction process, although the latter also has the anomaly detection function, provided by the Autoencoder. Autoencoders, however, are efficient in detecting anomalies, but may need a significant amount of computing power, particularly when used in large scales. The hybrid model can be considered the most efficient implementation of CNNs to extract features, thus minimizing the computational cost of the process of anomaly detection by the Autoencoder. The Hybrid CNN-Autoencoder model combines the two worlds as compared to LSTM networks that are good in temporal modeling but might have difficulties in identifying spatial patterns in data. CNNs are able to effectively extract spatial patterns, whereas Autoencoders are interested in anomalies, so that the model is capable of addressing the known and unknown threats.

Conclusion from Paper 4

In Conclusion, Paper 4 established that the Hybrid CNN-Autoencoder model performs better with respect to key performance indicators such as accuracy, precision, recall, and AUC when compared with the existing machine learning and deep learning models such as CNN, Autoencoders, and LSTM. The scalability and strength of the model make it a better option in identifying the changing cloud security threats. The hybrid model will offer reliable, scalable and efficient approach to real time cloud security surveillance by using CNNs to extract features and Autoencoders to identify anomalies. The paper was able to conclude that this hybrid solution, because of its high performance and efficiency, is a perfect candidate to cloud-based IDS in the contemporary cloud environments.

VII. IMPLICATIONS FOR FUTURE RESEARCH AND PRACTICE

The conclusion drawn by the synthesis of four previous papers has been very insightful in understanding the Hybrid CNN-Autoencoder model and how it can be used to improve the detection of threat in the security of clouds. On the basis of the overall analysis of the model performance, scalability and efficiency, a number of important implications to subsequent research and work applications can be defined. All these implications, not only reflect the strengths and capabilities of the hybrid model, but also indicate the opportunities and the prospects of further development to make this model effective in various and real-life cloud environment.

1) Integration with Real-Time Systems

A major implication on future research is that the Hybrid CNN-Autoencoder model should be further tested and implemented into the real-world cloud setting. Although the model has shown good performance in virtualized environments, it is important to test the performance of the model in real and high traffic conditions that is typical of dynamic cloud infrastructures. Detection of security threats in real time is essential to cloud systems and any delay in the detection process can be very costly such as data loss, system failures, or even loss of money. Further investigations ought to be directed at determining the functionality of the model in the real-time cloud settings where the volume of traffic and the attack vectors are under a continuous transformation. To be sure that the model will be able to detect emerging threats, the latency optimization, scalability, and resource consumption under real operational conditions should be prioritized and make sure that the detectable threats have a minimum detectable latency and resource overhead. The practicality of the model to be deployed in the production systems of enterprises will depend on its real-time capability.

2) Adaptive Model Tuning

As the cloud environments and attack patterns keep changing, a major future research direction will be on how to develop techniques of dynamically tuning of the model at runtime. The success of the Hybrid CNN Autoencoders model in identifying old and new threats is in the fact that this model adapts constantly to new trends in data. Nevertheless, due to the introduction of new forms of attacks and vulnerability, the static models may be less efficient in the long-term, particularly when they are not able to evolve in accordance with the new trends. To resolve this, future studies should aim at the

introduction of dynamic tuning mechanisms that enable the model to adapt the parameters, thresholds and decision rules to new types of attacks, cloud infrastructure changes, and changing traffic patterns. One of the possible techniques that can be considered is online learning, reinforcement learning, or transfer learning that would allow the model to keep learning and changing its actions according to the emerging threats. This would not only increase the accuracy of detection but it would also increase the robustness of the model to zero-day or novel attacks that were not included in the original training data.

3) Edge Computing and Low-Power Devices

The other area of future development that can be promising is optimization of the Hybrid CNN-Autoencoder model to run on edge devices and low-power hardware. With further development of cloud computing, edge computing is becoming more and more popular, in which processing is relocated to the source of data (i.e., IoT devices, mobile devices or sensors). This could be used to minimize latency and bandwidth expenses since data does not need to be sent to a central cloud server to analyze it. Future studies should focus on optimization methods like model pruning, quantization, and scalable architectures that are specially optimized to run on low-power devices, including Tensor Processing Unit (TPUs) and Field-Programmable Gate Arrays (FPGAs) to provide the scalability and energy efficiency of the model in edge environments. With edge computing optimization, the model can deliver near-instant threat detection to even a low-computational-resource and constrained-energy environment, which is why it is very applicable to a distributed security system in an IoT-heavy or mobile cloud environment.

4) Broader Threat Detection

Nowadays, the Hybrid CNN -Autoencoder model is mainly concerned with the detection of known and novel attacks in the network traffic and system logs. Nevertheless, further studies are necessary to expand the scope of the model to identify a wider scope of cyber threats such as insider threats, data exfiltration, fraudulent activities, and unauthorized access. As much as network traffic analysis is important, it is not the only part of cloud security. The capability of the model to monitor and analyze a large number of cloud data sources, including API calls, user behavior, and cloud storage activities, may result in a large number of applications in a variety of cloud environments. Another layer of security to cloud systems would be expanding the model to identify insider threats malicious or negligent actions by authenticated users and exfiltration of data. The hybrid model would be more effective in detecting abnormal behaviors that would signify possible threats that could circumvent standard security measures by incorporating behavioral analysis and user activities tracking. Multi-modal threat detection capabilities will not only ensure that the model is more comprehensive but also more versatile since all aspects of cloud security will be covered.

5) Future Development of Explainability and Transparency

Another field of the future study is to make the Hybrid CNNAutoencoder model more explainable and transparent. Since deep learning models, particularly CNNs, may be viewed as black-box systems, it is important to have insight on the decision-making process of the model, particularly in security-sensitive applications. The hybrid model could be complemented by explainable AI (XAI) methods that will enable the security analyst to comprehend the reasoning behind the identification of certain behaviors as suspicious or anomalous. This would offer more trust and confidence towards the system and may help overcome the apprehension towards the decision-making process of the model. The Hybrid CNNAutoencoder model has great potential in terms of cloud security threat detection, and there are still a few critical implications to consider in the future research and practical use. Bringing the model into the realm of real-time cloud systems, creating adaptive tuning strategies, optimizing to the edge computing setting, increasing its range of threats detected, and improving its explainability are all areas where the model will be further enhanced to serve a better purpose in cloud security. Overcoming such hurdles, the hybrid model may become a foundation of the next-generation IDS systems, which would allow being more dynamic and adaptable as well as efficient in detecting cloud security threats in different settings.

VIII. CONCLUSION

The Hybrid CNN Autoencoder model offers a very promising and innovative method of dealing with the continuously increasing emergent issues of cloud security. Using the strong feature extraction properties of Convolutional Neural Networks (CNNs) and the good properties of Autoencoders in detecting anomalies, the hybrid model is particularly effective in enhancing the performance of detecting both familiar and unfamiliar threats in the cloud environment. With this integration, the model can capture complex trends and dependencies on network traffic and system logs, which offer strong detection of various categories of cyber threats. The overall results of the four papers synthesis prove that the Hybrid CNN -Autoencoder model has essential benefits over the conventional Intrusion Detection System (IDS) models in a variety of the most important aspects. Such benefits are high accuracy, precision and recall, which are essential in effective threat detection in the cloud. This is because the model is capable of detecting with high accuracy and reducing a false positive and false negative as well as other rule based or signature-based systems. Also, the hybrid model is very scalable, and thus it can easily deal with large scale cloud infrastructures. The latter is especially relevant to cloud systems, where data size may be enormous and constantly changing and where real-time detection is a key element of reducing the effect of possible threats. The other important feature of the Hybrid CNNAutoencoder model is its computational efficiency. This hybrid model in contrast to others that are resource intensive and slow in their application is optimized to be deployed in a real time. It is able to balance the trade-off between high performance and low computational overhead so that the model can be effectively executed in dynamic cloud computing environments without necessitating high computing resources. The combination of the optimization techniques, including hyperparameter optimization, feature selection, and regularization of the model, also helps the model to work with large-scale data and respond to the changing environment. These measures are especially significant towards making sure that the model is functional even with the changing cloud traffic and threat patterns with time. Regardless of its amazing functions, the model still has a number of prospects to develop further. Further development in the model should be aimed at optimizing it further and especially with regard to real-time performance in terms of high traffic conditions so that it is able to detect emerging threats more quickly and accurately. It would also be necessary to extend the applicability of the model to more types of cloud settings, by adding more types of cloud security threats, like insider threats, data exfiltration and fraud, to the model. The addition of edge computing and low-power devices may also enhance scalability and energy efficiency of the model, thus making it more appropriate to be deployed in a wider scope of cloud services, such as the IoT and the mobile cloud services. Lastly, the Hybrid CNNAutoencoder model also paves new avenues in the future research of cloud security. As the methods of deep learning are continuously improved, along with the model interpretability and data privacy concerns, the combined efforts of the sophisticated methods like explainable AI (XAI) and transfer learning might further contribute to the increased robustness and versatility of the model. With the progress of cloud technologies, the necessity of intelligent, adaptive, and efficient security models is becoming more important, and Hybrid CNN-Autoencoder model can be considered as a promising basis of the next-generation cloud IDS.

REFERENCES

[1] O. G. Lira, A. Marroquin, and M. A. To, “Harnessing the advanced capabilities of LLM for adaptive intrusion detection systems,” in Advanced Information Networking and Applications, L. Barolli, Ed. Cham, Switzerland: Springer, 2024, pp. 453–464.

[2] M. Guastalla, Y. Li, A. Hekmati, and B. Krishnamachari, “Application of large language models to DDoS attack detection,” in Security and Privacy in Cyber-Physical Systems and Smart Vehicles, Y. Chen et al., Eds. Cham, Switzerland: Springer, 2024, pp. 83–99.

[3] M. Hassanin, M. Keshk, S. Salim, M. Alsubaie, and D. Sharma, “PLLM-CS: Pre-trained large language model (LLM) for cyber threat detection in satellite networks,” Ad Hoc Networks, vol. 166, Art. no. 103645, Jan. 2025.

[4] N. Alsaedi, N. Moustafa, Z. Tari, A. N. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," IEEE Access, vol. 8, pp. 165130–165150, 2020.

[5] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," Sensors, vol. 23, no. 13, p. 5941, Jun. 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/13/5941

[6] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "X-IIoTID: A connectivity-agnostic and device-agnostic intrusion dataset for industrial Internet of Things," IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3962–3977, Mar. 2022.

[7] S. Saxena, D. Yagyasen, C. N. Saranya, R. S. K. Boddu, A. K. Sharma, and S. K. Gupta, "Hybrid cloud computing for data security system," in Proc. 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Oct. 2021, pp. 1–8.

[8] B. Hazela, S. K. Gupta, N. Soni, and C. N. Saranya, "Securing the confidentiality and integrity of cloud computing data," ECS Transactions, vol. 107, no. 1, p. 2651, 2022.

[9] S. K. Gupta et al., "Biometric authentication for healthcare data security in cloud computing—A machine learning approach," in Advancements in Science and Technology for Healthcare, Agriculture, and Environmental Sustainability. CRC Press, 2024, pp. 318–324.

[10] N. M. S. Soumik, "A comparative analysis of network intrusion detection using artificial intelligence techniques," International Journal of Science and Research Archive, vol. 13, no. 2, pp. 4014–4025, 2024.

[11] S. K. Gupta et al., "Integrated model of encryption and steganography for improving data security in communication systems," in Advancements in Science and Technology for Healthcare, Agriculture, and Environmental Sustainability. CRC Press, 2024, pp. 333–338.

[12] L. D. Manocchio et al., "FlowTransformer: A transformer framework for flow-based network intrusion detection systems," Expert Systems with Applications, vol. 241, Art. no. 122564, May 2024.

[13] M. Ismail, H. Hussain, and A. A. Khan, "A machine learning-based classification and prediction technique for DDoS attacks," IEEE Access, vol. 10, pp. 21443–21454, 2022.

[14] A. A. Jihado and A. S. Girsang, "Hybrid deep learning network intrusion detection system based on CNN and BiLSTM," Journal of Advanced Information Technology, vol. 15, no. 2, pp. 219–232, 2024.

[15] M. Jouhari and M. Guizani, "Lightweight CNN-BiLSTM based intrusion detection systems for resource-constrained IoT devices," in Proc. IWCMC, 2024, pp. 1558–1563.

[16] C. Liu and S. Zhong, "DDoS attack detection method based on machine learning," in Proc. ICSESS, 2024, pp. 1–5.

[17] N. Moustafa and J. Slay, "A new distributed architecture for evaluating AI-based security systems at the edge," Sustainable Cities and Society, vol. 72, Art. no. 102994, 2021.

[18] A. A. Najar and M. Naik, "A robust DDoS intrusion detection system using convolutional neural network," Computers & Electrical Engineering, vol. 117, Art. no. 109277, 2024.

[19] S. Naiem, A. E. Khedr, A. M. Idrees, and M. I. Marie, "Enhancing the efficiency of Gaussian naïve Bayes machine learning classifier in the detection of DDoS in cloud computing," IEEE Access, vol. 11, pp. 124597–124608, 2023, doi: 10.1109/ACCESS.2023.3051156.

[20] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in Proc. IEEE ICCST, 2019, pp. 1–3.