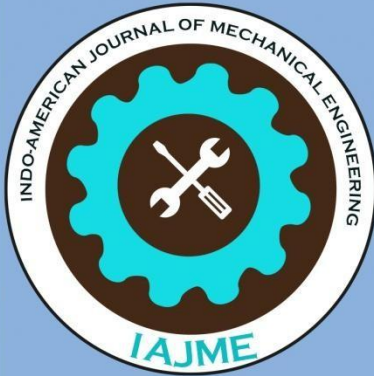




ISSN : 2321-9416

Indo - American Journal of Mechanical Engineering



www.iajme.org

Email : iajme.editor@gmail.com or editor@iajme.org



Cybersecurity Attack Detection Using LSTM and ResNet-50 Hybrid Model with Cloud Deployment

¹Venkata Surya Teja Gollapalli

Senior System Engineer,
Centene Management Company LLC,
Missouri, USA,
venkatasuryagollapalli@gmail.com

²Kannan Srinivasan

Senior Software Engineer
Saiana Technologies Inc, New Jersey, USA
kannan.srini3108@gmail.com

³Guman Singh Chauhan

John Tesla Inc,
Texas, USA
gumanc38@gmail.com

⁴Rahul Jadon

Cargurus, USA
rahul.jadon0@gmail.com

⁵Rajababu Budda

IBM, San Francisco, California, USA
RajBudda55@gmail.com

⁶R Padmavathy

Anna University, Coimbatore
dr.padmabarathi@gmail.com

ABSTRACT

As the number of complex cybersecurity threats accelerates at a fast pace, real-time attack identification is now essential in defending computer systems. These methods are challenged by high-dimensional data, class imbalance, and low scalability, resulting in low accuracy and increased false positives. This paper introduces a hybrid DL archetype combining ResNet-50 for feature extraction and LSTM in learning lay sequences, running on AWS Sage Maker for scalable cloud inference and training. The method involves extensive data pre-processing, including imputation, one-hot encoding, and feature scaling, with model training optimized through the Adam algorithm. Experimental results show excellent performance, with 99.50% of accuracy, 99.20% of precision, 99.30% of recall, 99.40% of F1-score, and an AUC of 0.999998. These findings demonstrate the strength and efficiency of the framework in real-time detection of cybersecurity attacks, providing an enhancement over previous solutions through the ability to efficiently process intricate data patterns and deploy quickly in cloud environments.

Keywords: Cybersecurity, LSTM- ResNet-50 Hybrid, Cloud, AI, AWS Sage maker, Adam Optimizer.

1. INTRODUCTION

Cybersecurity is an ever-growing concern in today's digitally driven world [1]. With the expansion of the internet and IoT devices, individuals and organizations face an increased risk of cyberattacks [2]. These attacks can range from malware and phishing attempts to more complex threats like

ransomware and advanced persistent threats (APTs) [3]. Traditional security measures, such as firewalls and signature-based intrusion detection systems (IDS), are becoming less effective in defending against increasingly sophisticated attacks [4]. To combat this, there has been a shift toward more



advanced technologies, including machine learning (ML) and artificial intelligence (AI) [5]. These technologies, particularly models like Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN) such as ResNet-50, have shown great potential in detecting anomalies and predicting cyber threats [6]. These deep learning models can analyze vast amounts of data, identifying patterns and behaviors indicative of a security breach, thereby offering a more proactive and adaptive defense system in the cybersecurity field [7].

The causes of cybersecurity breaches are numerous and often complex [8]. One major contributing factor is the rapid pace of technological advancement [9]. As more devices become connected to the internet, the potential attack surface grows significantly, providing cybercriminals with more opportunities to exploit vulnerabilities [10]. Many attacks are fueled by human error, such as weak passwords, lack of awareness about phishing schemes, and misconfigurations in systems, making organizations more susceptible to breaches [11]. Additionally, attackers are becoming increasingly sophisticated, using advanced techniques such as social engineering, zero-day vulnerabilities, and botnets to bypass traditional defenses [12]. Another factor is the growing reliance on cloud computing and third-party services, which can introduce new vulnerabilities if not properly secured [13]. With such a large and continuously evolving landscape, traditional defense mechanisms are often unable to keep up with new threats, creating a need for innovative solutions like machine learning models that can adapt to emerging risks [14].

Despite their promise, machine learning models such as LSTM and ResNet-50 face several challenges in cybersecurity applications [15]. One major drawback is the computational resources required to train and deploy these models effectively [16]. Deep learning models can be extremely resource-intensive, requiring powerful hardware like GPUs, which may not be feasible for smaller organizations or environments with limited infrastructure [17]. Another disadvantage is the lack of interpretability in these models [18]. While they can identify patterns and make predictions, the complexity of LSTM and ResNet-50 networks makes it difficult for security analysts to understand how and why specific threats are detected, potentially undermining trust in the system [19]. Furthermore, these models are not immune to adversarial attacks, where attackers intentionally modify data to deceive the model, leading to false positives or false negatives [20].

To address the challenges associated with LSTM and ResNet-50 models in cybersecurity, a hybrid approach combining the strengths of both models is gaining traction. LSTM networks are well-suited for sequential data, such as network traffic logs, which allows them to detect patterns over time and predict potential threats based on historical behavior. On the other hand, ResNet-50's deep convolutional layers excel at recognizing complex features in large datasets, such as images or multi-dimensional data. By combining these two models, cybersecurity systems can benefit from a more comprehensive detection framework that captures both temporal and spatial patterns. Additionally, deploying these models in the cloud offers several advantages, including scalability, flexibility, and the ability to leverage high-performance computing resources, reducing the computational burden on local systems. This hybrid and cloud-based approach enhances the model's accuracy, efficiency, and adaptability, making it more resilient to advanced cyberattacks and improving overall security.

OBJECTIVES

- ✚ Develop a strong hybrid deep learning architecture integrating LSTM and ResNet-50 frameworks to achieve robust cybersecurity attack identification and deploy it optimally on a scalable cloud-based infrastructure.
- ✚ Utilize the dataset, comprising rich network traffic data, to train and validate the suggested framework for precise attack classification.
- ✚ Implement the ResNet-50 architecture to derive high-level spatial features from the network traffic and identify complex patterns necessary for detecting attacks.
- ✚ Apply the LSTM network to capture temporal needs and sequential forms from spatial features to enhance the detection of evolving and dynamic cyber-attacks.

2. LITERATURE SURVEY

This research explores the uses of AI in cyber safety, noting structural shifts and new trends in the discipline [21]. It maps research hotspots and gives an overall role of AI in cyber security, helping researchers and organizations strategize applications of AI [22]. The research also finds collaboration networks and analyses significant factors that determine research directions in this space [23]. The study explores AI applications in cyber safety, with its capacity to deliver real-time insights in the face



of multiple daily security notifications [24]. It identifies a scarcity of visual analysis in the current literature on AI applications in cyber security and stresses structural transformation in the discipline ever since the advent of AI [25]. The study is intended to formulate theoretical frameworks, inform future research streams, and act as a reference guide for businesses and governments contemplating AI applications in the cyber security space [26]. The research maps research hotspots and future direction in AI in cyber security, using five measures of evaluation and a heat map to indicate global research activity in the field [27].

The study introduces an AI-driven Intrusion Detection System that can identify botnet attacks, especially on financial institutions, based on the dataset on AWS [28]. The structure, which is proposed using artificial neural networks, has a high accuracy of 95.97%, a ROC curve area of 0.900, and a low false positive rate of 0.101, showing its suitability for real-time network traffic analysis [29]. The study paper makes use of AI in improving cyber alerts, citing its capacity to automate threat analysis and enhance system resilience [30]. It talks about how leading technology firms are incorporating GAI into their security tools to counter the rising sophistication of cyber-attacks, also recognizing the drawbacks and risks of GAI technologies [31]. Presently, in cyber safety, the credentials of negative events are quite challenging because of the enormous diversity, volume, and speed of deep packet inspection data. The latest detection methods have failed to identify the newest attacks following a massive data breach event. In contrast, computational intelligence methods like machine learning have again fueled the quest for solutions for various monitoring issues [32].

The rise of new cyber threats and increased reliance on infrastructures of the digital world immensely demanded effective intrusion detection systems to be set up in networks as well as to protect sensitive information [33]. Strong cybersecurity mechanisms are required to protect digital infrastructures from the increasing rate of cyber-attacks and the rapid expansion of the internet. It examines the role of AI for enhancing cybersecurity practices, particularly highlighting the assessment between signature-based and anomaly-based IDS [34]. ML and DL algorithms such as DNN, SVM, and Random Forest classifiers are employed here to categorize cybersecurity threats and identify possible threats based on the dataset UNSW-NB15 [35]. The aim of the current research is to review and comparatively examine several methods and techniques of both ML

and DL in order to improve cybersecurity in general, with special emphasis on such subdomains as cybersecurity threat analysis and intrusion detection [36]. The current research attempts to recognize and classify cybersecurity threats more precisely by employing sophisticated computation techniques [37].

AI is being used to strengthen cybersecurity and threat intelligence by automatically detecting threats and vulnerabilities in companies [38]. This technology assists decision-making in security operations centres through rapid analysis of different sources of data, thus offering another layer of protection from advanced cyber-attacks [39]. This paper gives details of GAN in cybersecurity, especially Intrusion Detection Systems [40]. It discusses their application in producing synthetic data for unbalanced datasets, adversarial example generation, and data augmentation for rare attack classes, acting as a tutorial for security experts and ML scholars alike [41]. SecGNN is an innovative system to enable privacy-conserving drill and implementation of GNN in the cloud, addressing serious privacy issues related to proprietary graph data. The system integrates lightweight cryptography and machine learning approaches, and experiments prove that it attains comparable accuracy and inspiring performance to conventional techniques [42].

The paper stresses the need for good cybersecurity management in Cloud Computing, resolving security threats and vulnerabilities of this technology [43]. It suggests an integrated framework in terms of ISO and NIST standards to assist organizations in managing and averting cyber risks, along with specifying metrics for assessing the maturity of organizations that deploy the framework [44]. The study explores cybersecurity threats within cloud computing, focusing on anomaly finding and insider attacks. It suggests a feature selection technique based upon the black widow function and an RNN for improving the accuracy of classification and reducing training errors, eventually improving the detection of real-time threats in cloud computing environments. It explores RNN applications, like LSTM and Bidirectional RNNs, toward malware detection in the cloud. The research proves that both models perform well in detection rates [45].

2.1 PROBLEM STATEMENT

Current cybersecurity approaches usually lack performance in high-dimensional data, class imbalance, and inefficient clustering, causing higher



computational complexity, biased detection, and longer training durations [46]. Most conventional approaches are also plagued by high false positive and false negative ratios, capping their applicability in the real world [47]. Further, an inability to integrate seamlessly into the cloud curbs scalability and adaptability to changing patterns of attack. The suggested framework addresses such challenges by implementing Principal Component Analysis for reducing dimensionality without losing crucial features, as well as minimizing complexity [48]. The SMOTE is employed in balancing minority attack classes to enhance fairness in detection. An Autoencoder-based classifier improves accuracy further by concentrating on attack-specific data, eliminating noise and training time [49]. Implemented on AWS cloud infrastructure, the framework makes use of cloud scalability for contemporary, efficient intrusion detection with substantial improvements over current solutions in terms of speed, accuracy, and adaptability [50].

3. PROPOSED METHODOLOGY

The suggested method is Cybersecurity Attack Forecast using deep learning. It starts with

the Dataset (Cybersecurity Attacks), which holds important information like protocols, ports, IP address and traffic patterns. The process starts with Pre-processing, where the dataset goes through various transformations. It includes missing data handling with imputation techniques to make it complete, followed by feature encoding to convert categorical variables into mathematical form. Feature scaling is subsequently used to normalize the numeric data so that all features contribute equally while training the model. Model Development is the following step when the dataset undergoes a passage through a hybrid LSTM + ResNet-50 model. ResNet-50 features the extraction of features, while LSTM deals with sequential dependencies present in the data, which plays an important role when dealing with attacks that run in a chronological sense. Upon model development, data enters Model Training, whereby Adam optimizer comes into play as a method for efficient training of the model. Lastly, the Performance Matrix assesses how well the model performs, whether it can efficiently distinguish attack, non-attack. The whole process is made possible by AWS Sage maker to provide scalable and optimized training and deployment as shown in Figure 1.

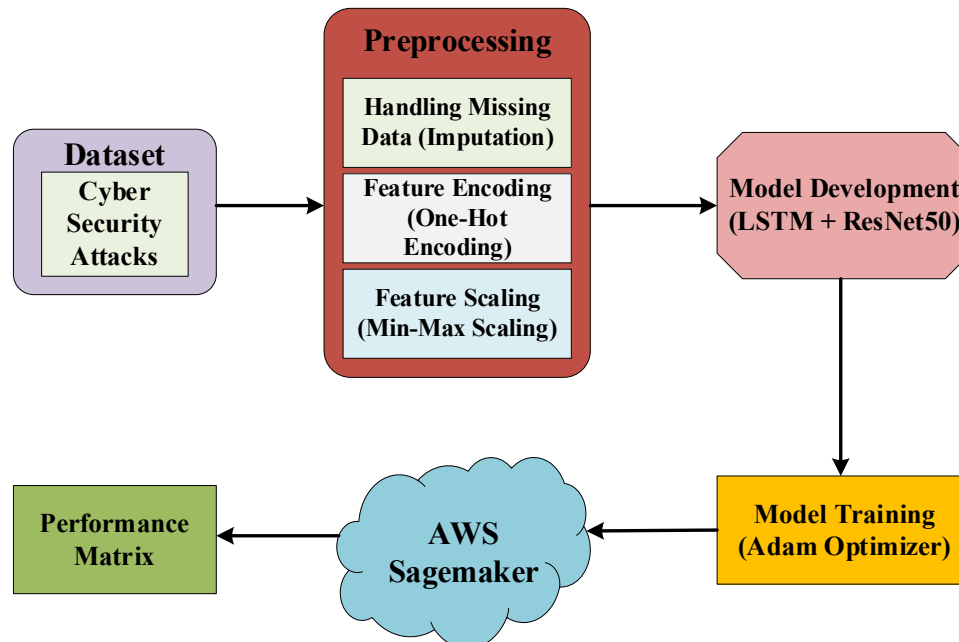


Figure 1: Proposed methodology diagram

3.1 DATA COLLECTION

The process starts by capturing important network traffic information from multiple sources. The dataset contains data like Destination IP Address, Source IP Address, Protocol, Source Port,

Traffic Type, Destination type, Payload Data. All these features capture network traffic flow, which gives information about possible attack patterns. Moreover, Action Taken (Blocked, Logged,



Ignored) is gathered to be used as the target variable for classification purposes, denoting whether the traffic was an attack or not. Other supporting data such as Geo-location Data, IDS/IPS Alert, User Information, and Device Information may also be used to enhance the model's capacity to classify anomalies. The information is necessary in order to upskill a deep learning archetype potential to classify traffic as attack or non-attack. Lastly, the dataset guarantees overall coverage of many network activities and is, therefore, aptly suited for detection of cybersecurity attacks.

3.2 PREPROCESSING

3.2.1 Handling Missing Data (Imputation):

Missing data may adversely affect the performance of a machine learning algorithm. Imputation involves substituting estimated missing values using other values from the data. For your cybersecurity dataset, systems such as median, mean, or mode imputation can be used for mathematical data and mode imputation for qualitative data. This helps make the model capable of handling complete datasets without the possibility of error while training, which is expressed mathematically as,

$$\hat{x} = \frac{\sum_{i=1}^n x_i}{n} \quad (1)$$

were, $\hat{x}$ is imputed value, x_i is observed value, n the total no of available values in feature.

3.2.2 Feature Encoding (One-Hot Encoding):

The Attack Type attribute in the dataset is nominal and needs to be transformed to a numerical one for machine learning models. In order to perform this, One-Hot Encoding is used. One-Hot

Encoding generates binary columns for distinct group of the Attack Type attribute (i.e., Malware, DDoS, Intrusion). Each category has a vector represented by where the position corresponding to the category has a value 1, while all others are 0. This conversion enables the machine learning model to treat categorical features as numerical data with no inherent ordering or relationships.

$$\text{Malware} \rightarrow [1,0,0], \text{DDoS} \rightarrow [0,1,0], \text{In} \left(\begin{array}{c} 2 \\ \end{array} \right)$$

3.2.3 Feature Scaling (Min-Max Scaling):

Feature scaling is required to regularize the data series, particularly for algorithms that are magnitude-sensitive to input feature values, like LSTM and ResNet-50. Min-Max Scaling scales all numerical features to a range from 0 to 1. This makes all features equally contribute during the model training process without any feature dominating the process because of its higher numerical range, which is mathematically expressed as,

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (3)$$

were, X is original value, $X_{\min}$, the minimum value, $X_{\max}$ is maximum value in feature, X' the scaled value.

3.3 MODEL DEVELOPMENT USING LSTM-ResNet-50

The development of the model in this study combines two strong architectures, namely LSTM and ResNet-50. It is a hybrid model that captures temporal dependencies (through LSTM) and spatial features (through ResNet-50), which enables it to perform extremely well on cybersecurity attack detection tasks as shown in Figure 2.

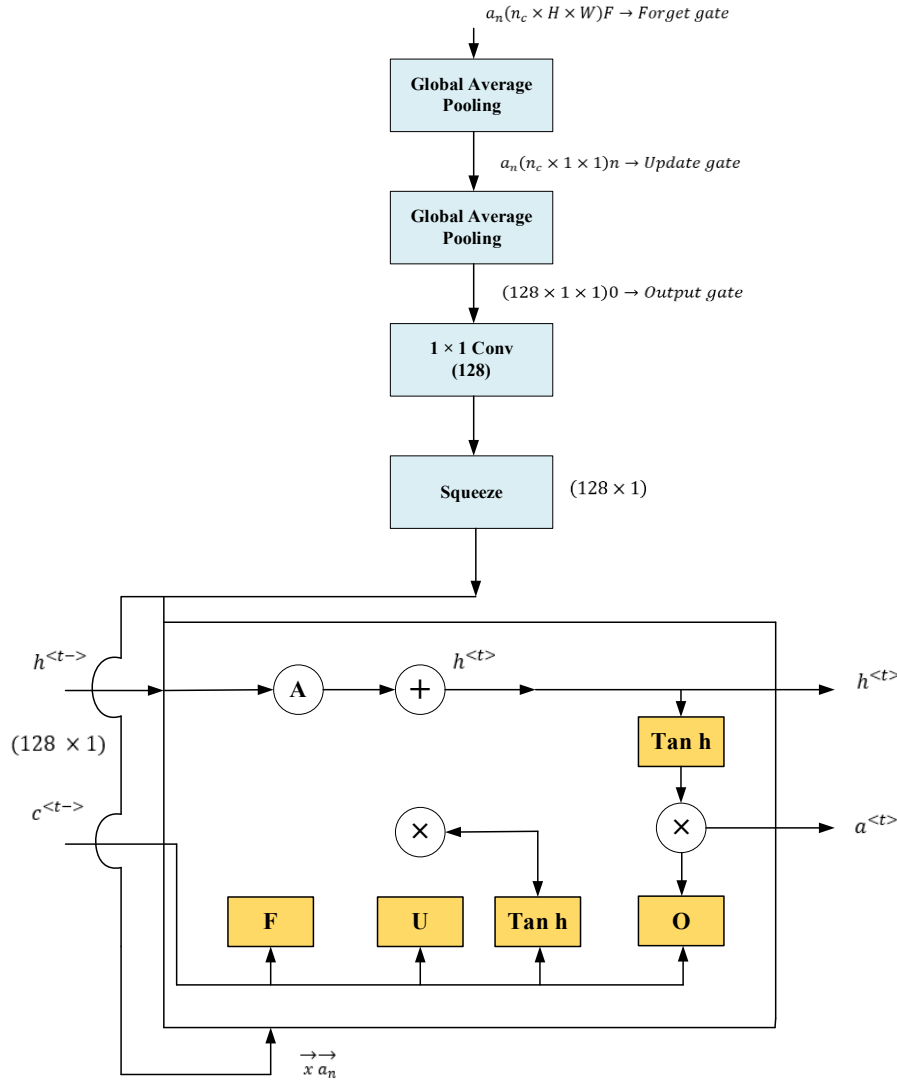


Figure 2: Architecture of LSTM-ResNet-50

3.3.1 ResNet-50 Component for Spatial Feature Extraction:

Global Average Pooling (GAP): It is a spatial aggregation operation that decreases the spatial dimensions of feature map. It calculates the average of each map, giving tensor shape $(nc \times 1 \times 1)$. For a given feature map with size $(nc \times H \times W)$, were, nc is no of channels, H is the height, W is the width. GAP is mathematically expressed as,

$$a_n^{GAP} = \frac{1}{H \times W} \sum_{h=1}^H \sum_{w=1}^W a_n(h, w) \quad (4)$$

Were, $a_n(h, w)$ is activation value at h -th row and w -th column for the n -th feature map.

Residual Block: The ResNet-50 block employs residual connections, which assist in

backpropagation of gradients. The output of a residual block is expressed as,

$$\text{Output} = F(x) + x \quad (5)$$

were, $F(x)$ is learned function, x is the input of residual block.

For every residual block, input x traverses a sequence of steps (most commonly convolutions, batch regularization, initiation functions). Output is then added to the input x , creating a skip connection. This architecture reduces the vanishing gradient problem and eases the flow of very deep networks.

when including convolution operation with residual block, the expression becomes,



$$\text{Output} = F(x, W) + x \quad (6)$$

were, $F(x, W)$ is a set of convolutions and nonlinear activations (ReLU) applied to input x , and W represents the weight associated with convolutions.

Convolutional Layer: This is the core work of ResNet-50. For a given input x , convolutional operation is expressed as,

$$y = W * x + b \quad (7)$$

were, W is convolutional filter, $*$ the convolutional operation, x the input feature map, x is the input feature map, b the bias term.

1x1 Convolution: It is applied after pooling operation, 1x1 Convolution is used to change depth of feature map. It is mathematically expressed as,

$$y = W_{1 \times 1} * x + b \quad (8)$$

Were, $W_{1 \times 1}$ is 1x1 Convolutional filter, x is input feature, y the output feature, b the bias term. The 1x1 convolution aids in shrinking or expanding the depth of feature maps and facilitates the network in learning more advanced representations by enhancing no of channels in the network.

Squeeze Layer: The Squeeze operation decreases the dimensionality by eliminating the spatial dimensions (height and width), leaving a tensor with shape (128×1) . This can be achieved by taking the global average pooling output and reshaping it,

$$\text{Squeeze}(a_n^{\text{GAP}}) \rightarrow (128 \times 1) \quad (9)$$

This downscales the feature map into a small, lower-dimensional space, readying it for downstream processing by the LSTM module.

3.3.2 LSTM Component for Temporal Feature Learning:

LSTM component captures temporal dependencies in the data. It is modelled as,

Forget Gate (F):

$$F = \sigma(W_f x_t + U_f h_{t-1} + b_f) \quad (10)$$

The forget gate chooses how much percentage of last cell state must be "forgotten." It operates on the current input x_t and the last hidden state h_{t-1} , and applies the sigmoid activation function to give an output 0 or 1.

Update Gate (U):

$$U = \sigma(W_u x_t + U_u h_{t-1} + b_u) \quad (11)$$

Update gate determines the quantity of the inward info to append the cell state. Update gate also feeds a sigmoid transformation of the sum of the inputs and past hidden state.

Cell State Update:

$$c_t = F \cdot c_{t-1} + U \cdot \tanh(W_c x_t + U_c h_{t-1} + b_c) \quad (12)$$

The cell state c_t is computed by updating the current cell state c_{t-1} and new information (modified by the update gate). The hyperbolic tangent function is used on the weighed input sum and previous hidden state in computing the new info.

Output Gate (O):

$$O = \sigma(W_o x_t + U_o h_{t-1} + b_o) \quad (13)$$

The output gate decides how much portion of c_t be output as hidden state and employs the sigmoid activation function to make this decision.

Final Hidden State (h_t):

$$h_t = O \cdot \tanh(c_t) \quad (15)$$

Then, h_t is calculated by increasing the output O with the updated cell state (c_t). Tanh activation is employed to make the hidden state between -1 and 1.

Final Output a_n :

The last output of LSTM, represented as a_n , obtained from h_t , is forwarded for last classification or decision-making process.

3.4 MODEL TRAINING USING ADAM OPTIMIZER

The Adam optimizer, or Adaptive Moment Estimation, is a broadly used for optimization algorithm updating neural network weights during training. It incorporates the best of both Momentum and RMSprop to calculate adaptive learning rates for each parameter, making it more efficient and effective for training deep learning models, particularly large ones. It calculates adaptive learning rate for every parameter based on both first-order momentum (m) and second-order variance (v)



gradient estimates. These are calculated at every time step during training of the model.

First Moment Estimate (m_t): is the Ave of running gradients $\nabla_{\theta}J(\theta)$. It encodes the mean direction of the gradients, which assists in dynamically adapting the learning rate during optimisation.

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) \nabla_{\theta}J(\theta) \quad (16)$$

Were, $\nabla_{\theta}J(\theta)$ is gradient loss of function of θ at time t .

Second Moment Estimate (v_t): It is the moving average of the gradients squared $\nabla_{\theta}J(\theta)^2$. It accumulates the alteration of the gradients and is used to regulate the learning rate according to the gradient magnitude and stabilize the training.

$$v_t = \beta_2 v_{t-1} + (1 - \beta_2) \nabla_{\theta}J(\theta)^2 \quad (17)$$

Were, β_2 is the decline rate of 2nd moment. Here, the first term m_t is the exponentially moving average of the gradients, and the 2nd term v_t is the exponentially moving average of the squared gradients.

Bias-Corrected Moment Estimates: It estimates $\hat{m}_t$ and $\hat{v}_t$ correct the 1st and 2nd moment approximations by counteracting their initial bias towards zero, particularly at the initial phase of training. The corrections aid in generating better estimates of gradients' 1st and 2nd moments as training proceeds.

The first moment estimate, mathematically expressed as,

$$\hat{m}_t = \frac{m_t}{1 - \beta_1^t} \quad (18)$$

The second moment estimate is mathematically expressed as,

$$\hat{v}_t = \frac{v_t}{1 - \beta_2^t} \quad (19)$$

Here, t is time step, and these corrections prevents the estimates from being biased from zero, in initial interactions.

Parameter Update Rule: Once the moment estimate confirmed and bias-corrected, parameters are updated using this mathematical expression,

$$\theta_t = \theta_{t-1} - \eta \frac{\hat{m}_t}{\sqrt{\hat{v}_t} + \epsilon} \quad (20)$$

Were, η the learning rate, ϵ small constant added to avert separation by zero, $\hat{m}_t, \hat{v}_t$ are bias corrected estimates of first and second moments.

3.5. CLOUD INTEGRATION

AWS Sage Maker is a fully accomplished cloud service that pillars the deployment, development, and training of ML models at scale. It offers an integrated environment to pre-process data, train models, tune hyperparameters, and deploy trained models for inference. With built-in support for popular ML frameworks such as SageMaker, MXNet, PyTorch, and TensorFlow simplifies the machine learning lifecycle. It also enables easy scaling of resources, giving perfect scope for big datasets to hard models.

Loss function: It measures the change amongst the forecasted and observed values during model training and directs the optimization process. Some of the popular loss functions are Mean Squared Error (MSE) for a regression task and Cross-Entropy Loss for a classification task.

$$J(\theta) = \frac{1}{N} \sum_{i=1}^N \text{Loss}(y_i, f(x_i; \theta)) \quad (21)$$

Were, $J(\theta)$ is loss function, y_i are true labels, $f(x_i; \theta)$ is model predictions for input x_i and θ .

Gradient Update: It entails the calculation of the gradient of loss function over model parameters and update the parameters to reduce loss. This is commonly achieved through the application of optimizers like Adam or Stochastic Gradient Descent for enhancing model precision.

$$\theta_t = \theta_{t-1} - \eta \nabla_{\theta}J(\theta) \quad (22)$$

Were, η is rate of learning, $\nabla_{\theta}J(\theta)$ is loss gradient function of θ .

4. RESULT AND DISCUSSION

Experimental outcomes verify the proposed LSTM-ResNet cross model's capacity to identify cybersecurity attacks by superior exactness and reliability. The model performs well across various evaluation criteria, validating its capacity to correctly classify attack and non-attack modes. Integration of spatial and temporal feature extraction



and cloud deployment via AWS Sage Maker supports scalable and efficient processing of large network data. Key findings like the confusion matrix, ROC curve, and performance measures highlight the superior detection rate and low error

rates of the model. These results substantiate the proposed framework as a feasible solution for up-to-date cybersecurity threat recognition in effective cloud environments.

4.1 CONFUSION MATRIX

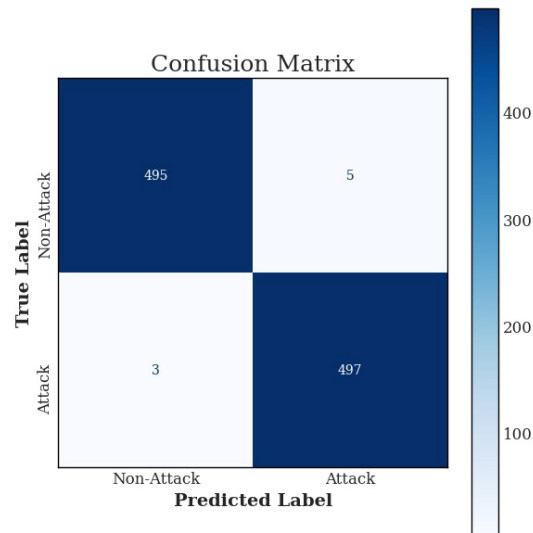


Figure 3: Confusion Matrix (Attack and Non-Attack)

Confusion matrix of this suggested workflow shows excellent classification performance. 495 out of 500 non-attack samples were correctly classified, and 5 were misclassified as attacks. Likewise, 497 out of 500 attack samples were correctly detected, and 3 were misclassified as non-attacks as shown in Figure 3. This gives an overall accuracy of 99.2%, which shows the model has high capability to discriminate between attack and non-attack possibilities. The fact that there were few misclassifications indicates the strength and trustworthiness of the cybersecurity attack detection system.

4.2 PERFORMANCE METRICS

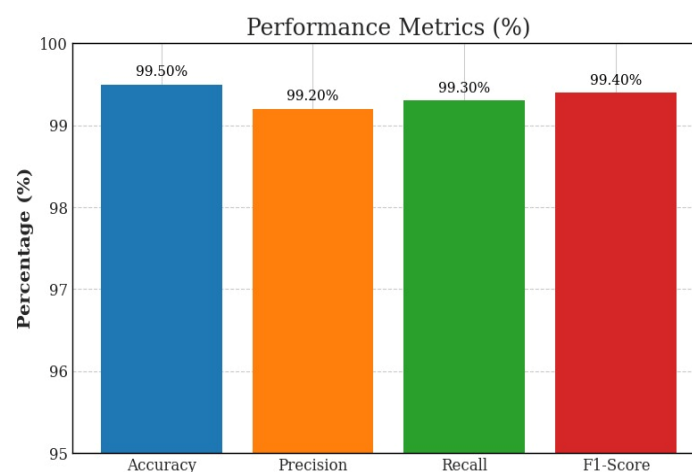


Figure 4: Performance Metrics for Cyber Security using (LSTM+ ResNet)

The performance parameters of the model show outstanding efficacy in detecting cybersecurity attacks. The model is 99.50% accurate, which means that overall correctness in the classification process. The precision



ratio is 99.20%, reflecting the capacity of the archetypal to suppress false positives. It accurately identifies true attacks with a recall rate of 99.30%, suppressing false negatives. The well-balanced performance is also evident in the F1-score of 99.40%, which illustrates outstanding balance between precision and recall for trustworthy detection outcomes as shown in Figure 4.

4.3 ROC CURVE

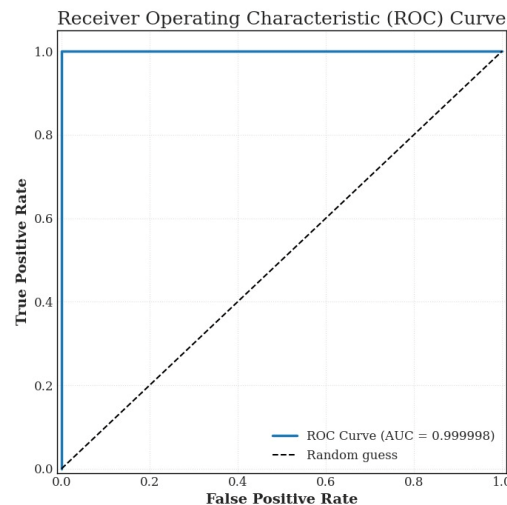


Figure 5: ROC curve - Cyber Security (LSTM+ ResNet)

The ROC curve of the suggested model is indicative of great classification performance, with the curve tightly following the top-left region of the plot. This suggests a highly high True Positive Rate and a highly low False Positive Rate for every threshold. The AUC is at about 0.999998, which indicates virtually perfect discrimination amongst attack, non-attack as shown in Figure 5, and a high AUC value such as this indicates the archetype's strength and accuracy in separating positive from negative examples. Generally, this ROC curve shows the reliability and efficacy of the cyber-attack recognition structure.

5. CONCLUSION AND FUTURE ENHANCEMENT

The new LSTM-ResNet-50 hybrid model with AWS Sage Maker cloud deployment with effective cybersecurity attack detection. The new framework effectively integrates spatial feature learning and temporal sequence learning and outperforms others with better attack and non-attack traffic classification. Experimental results obtained 99.50% of high accuracy, 99.20% precision, 99.30% recall, and 99.40% of F1-score indicating the model's superior robustness and reliability. The AUC of almost perfect value 0.999998 again supports the strong discrimination power of the framework. Cloud deployment ensures efficient, scalable training and real-time inference with a

perfect fit for dynamic, large-scale networked environments. For further research, the model can be extended to process more varied and dynamic cyber threats by adding other data sources like encrypted traffic and IoT device logs. Augmenting the framework with federated learning would facilitate privacy preservation and collaborative attack detection in distributed networks. Investigating other explainable AI methods might yield improved interpretability of the model's choices, improving trust and usability among cybersecurity analysts.

REFERENCE

- [1] Boyapati, S., & Kaur, H. (2022, July–August). Mapping the urban-rural income gap: A panel data analysis of cloud computing and internet inclusive finance in the e-commerce era. *ISAR International Journal of Mathematics and Computing Techniques*, 7(4).
- [2] Tsimenidis, S., Lagkas, T., & Rantos, K. (2022). Deep learning in IoT intrusion detection. *Journal of network and systems management*, 30(1), 8.
- [3] Samudrala, V. K., Rao, V. V., Pulakhandam, W., & Karthick, M. (2022, September–October). IoMT platforms for advanced AI-powered skin lesion



- identification: Enhancing model interpretability, explainability, and diagnostic accuracy with CNN and Score-CAM to significantly improve healthcare outcomes. *ISAR International Journal of Mathematics and Computing Techniques*, 7(5).
- [4] Awan, M. J., Masood, O. A., Mohammed, M. A., Yasin, A., Zain, A. M., Damaševičius, R., & Abdulkareem, K. H. (2021). Image-based malware classification using VGG19 network and spatial convolutional attention. *Electronics*, 10(19), 2444.
- [5] Ganesan, T., Devarajan, M. V., Yallamelli, A. R. G., Mamidala, V., Yalla, R. K. M. K., & Sambas, A. (2022). Towards time-critical healthcare systems leveraging IoT data transmission, fog resource optimization, and cloud integration for enhanced remote patient monitoring. *International Journal of Engineering Research and Science & Technology*, 18(2).
- [6] Malliga, S., Nandhini, P. S., & Kogilavani, S. V. (2022). A comprehensive review of deep learning techniques for the detection of (distributed) denial of service attacks. *Information Technology and Control*, 51(1), 180-215.
- [7] Devi, D. P., Allur, N. S., Dondapati, K., Chetlapalli, H., Kodadi, S., & Perumal, T. (2022). Neuromorphic and bio-inspired computing for intelligent healthcare networks. *International Journal of Information Technology & Computer Engineering*, 10(2).
- [8] Karar, M. E., Reyad, O., Abdel-Aty, A. H., Owyed, S., & Hassan, M. F. (2021). Intelligent IoT-Aided Early Sound Detection of Red Palm Weevils. *Computers, Materials & Continua*, 69(3).
- [9] Dondapati, K., Deevi, D. P., Allur, N. S., Chetlapalli, H., Kodadi, S., & Perumal, T. (2022). Strengthening cloud security through machine learning-driven intrusion detection, signature recognition, and anomaly-based threat detection systems for enhanced protection and risk mitigation. *International Journal of Engineering Research and Science & Technology*, 18(1).
- [10] Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access*, 10, 93104-93139.
- [11] Narla, S. (2022). Big data privacy and security using continuous data protection data obliviousness methodologies. *Journal of Science and Technology*, 7(2).
- [12] Kim, K. (2020). Intrusion detection system using deep learning and its application to Wi-Fi network. *IEICE TRANSACTIONS on Information and Systems*, 103(7), 1433-1447.
- [13] Ubagaram, C., Mandala, R. R., Garikapati, V., Dyavani, N. R., Jayaprakasam, B. S., & Purandhar, N. (2022, July). Workload balancing in cloud computing: An empirical study on particle swarm optimization, neural networks, and Petri net models. *Journal of Science and Technology*, 7(07), 36-57.
- [14] Abu Al-Haija, Q., & Alsulami, A. A. (2022). Detection of fake replay attack signals on remote keyless controlled vehicles using pre-trained deep neural network. *Electronics*, 11(20), 3376.
- [15] Srinivasan, K., Chauhan, G. S., Jadon, R., Budda, R., Gollapalli, V. S. T., & Kurunthachalam, A. (2022). Secure healthcare data storage and access control in cloud computing environments using AES and ECC encryption. *International Journal of Information Technology & Computer Engineering*, 10(3).
- [16] Choi, K., Ryu, H., & Kim, J. (2021). Deep residual networks for user authentication via hand-object manipulations. *Sensors*, 21(9), 2981.
- [17] Radhakrishnan, P., & Padmavathy, R. (2019). Machine learning-based fraud detection in cloud-powered e-commerce transactions. *International Journal of Engineering Technology Research & Management*, 3(1).
- [18] Hendrawan, Y., Widyaningtyas, S., Fauzy, M. R., Sucipto, S., Damayanti, R., Al Riza, D. F., ... & Sandra, S. (2022). Deep learning to detect and classify the purity level of luwak coffee green beans. *Pertanika Journal of Science & Technology*, 30(1), 1-18.
- [19] Musham, N. K., & Aiswarya, R. S. (2019). Leveraging artificial intelligence for fraud detection and risk management in cloud-based e-commerce platforms. *International*



- Journal of Engineering Technology Research & Management, 3(10)
- [20] Irkham, I., Ibrahim, A. U., Nwekwo, C. W., Al-Turjman, F., & Hartati, Y. W. (2022). Current technologies for detection of COVID-19: Biosensors, artificial intelligence and internet of medical things (IOMT). *Sensors*, 23(1), 426.
- [21] Musam, V. S., & Rathna, S. (2019). Firefly-optimized cloud-enabled federated graph neural networks for privacy-preserving financial fraud detection. *International Journal of Information Technology and Computer Engineering*, 7(4).
- [22] Manisha, R. (2022). Effective network intrusion detection by addressing class imbalance with deep neural networks multimedia tools and applications. *Multimedia Tools and Applications*, 81(6), 8499-8518.
- [23] Deevi, D. P., & Padmavathy, R. (2019). A hybrid random forest and GRU-based model for heart disease prediction using private cloud-hosted health data. *International Journal of Applied Science Engineering and Management*, 13(2).
- [24] Aouedi, O., Sacco, A., Piamrat, K., & Marchetto, G. (2022). Handling privacy-sensitive medical data with federated learning: challenges and future directions. *IEEE journal of biomedical and health informatics*, 27(2), 790-803.
- [25] Vallu, V. R., & Arulkumaran, G. (2019). Enhancing compliance and security in cloud-based healthcare: A regulatory perspective using blockchain and RSA encryption. *Journal of Current Science*, 7(4).
- [26] Ch, A., Ch, R., Gadamsetty, S., Iwendi, C., Gadekallu, T. R., & Dhaou, I. B. (2022). ECDSA-based water bodies prediction from satellite images with UNet. *Water*, 14(14), 2234.
- [27] Gudivaka, R. L., & Mekala, R. (2018). Intelligent sensor fusion in IoT-driven robotics for enhanced precision and adaptability. *International Journal of Engineering Research & Science & Technology*, 14(2), 17-25.
- [28] Djigal, H., Xu, J., Liu, L., & Zhang, Y. (2022). Machine and deep learning for resource allocation in multi-access edge computing: A survey. *IEEE Communications Surveys & Tutorials*, 24(4), 2449-2494.
- [29] Basani, D. K. R., & RS, A. (2018). Integrating IoT and robotics for autonomous signal processing in smart environment. *International Journal of Computer Science and Information Technologies*, 6(2), 90-99. ISSN 2347-3657.
- [30] He, Y., Meng, G., Chen, K., Hu, X., & He, J. (2020). Towards security threats of deep learning systems: A survey. *IEEE Transactions on Software Engineering*, 48(5), 1743-1770.
- [31] Peddi, S., & Aiswarya, RS. (2018). Securing healthcare in cloud-based storage for protecting sensitive patient data. *International Journal of Information Technology and Computer Engineering*, 6(1).
- [32] Dini, P., & Saponara, S. (2021). Analysis, design, and comparison of machine-learning techniques for networking intrusion detection. *Designs*, 5(1), 9.
- [33] Natarajan, D. R., & Kurunthachalam, A. (2018). Efficient Remote Patient Monitoring Using Multi-Parameter Devices and Cloud with Priority-Based Data Transmission Optimization. *Indo-American Journal of Life Sciences and Biotechnology*, 15(3), 112-121.
- [34] Yuan, B., Wang, J., Wu, P., & Qing, X. (2021). IoT malware classification based on lightweight convolutional neural networks. *IEEE Internet of Things Journal*, 9(5), 3770-3783.
- [35] Bobba, J., & Prema, R. (2018). Secure financial data management using Twofish encryption and cloud storage solutions. *International Journal of Computer Science Engineering Techniques*, 3(4), 10-16.
- [36] Saraswat, D., Bhattacharya, P., Verma, A., Prasad, V. K., Tanwar, S., Sharma, G., ... & Sharma, R. (2022). Explainable AI for healthcare 5.0: opportunities and challenges. *IEEE Access*, 10, 84486-84517.
- [37] Kethu, S. S., & Thanjaivadivel, M. (2018). SECURE CLOUD-BASED CRM DATA MANAGEMENT USING AES ENCRYPTION/DECRYPTION. *International Journal of HRM and Organizational Behavior*, 6(3), 1-7.
- [38] Liaqat, S., Dashtipour, K., Shah, S. A., Rizwan, A., Alotaibi, A. A., Althobaiti, T., ... & Ramzan, N. (2021). Novel ensemble



- algorithm for multiple activity recognition in elderly people exploiting ubiquitous sensing devices. *IEEE Sensors Journal*, 21(16), 18214-18221.
- [39] Vasamsetty, C., & Rathna, S. (2018). Securing digital frontiers: A hybrid LSTM-Transformer approach for AI-driven information security frameworks. *International Journal of Computer Science and Information Technologies*, 6(1), 46–54. ISSN 2347–3657.
- [40] Hammad, B. T., Jamil, N., Ahmed, I. T., Zain, Z. M., & Basheer, S. (2022). Robust malware family classification using effective features and classifiers. *Applied Sciences*, 12(15), 7877.
- [41] Ganesan, S., & Kurunthachalam, A. (2018). Enhancing financial predictions using LSTM and cloud technologies: A data-driven approach. *Indo-American Journal of Life Sciences and Biotechnology*, 15(1).
- [42] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 23(3), 1622-1658.
- [43] Kushala, K., & Rathna, S. (2018). Enhancing privacy preservation in cloud-based healthcare data processing using CNN-LSTM for secure and efficient processing. *International Journal of Mechanical Engineering and Computer Science*, 6(2), 119–127.
- [44] Hu, M., Zhang, K., You, R., & Tu, B. (2022). Multisensor-based continuous authentication of smartphone users with two-stage feature extraction. *IEEE Internet of Things Journal*, 10(6), 4708-4724.
- [45] Bhadana, D., & Kurunthachalam, A. (2020). Geo-cognitive smart farming: An IoT-driven adaptive zoning and optimization framework for genotype-aware precision agriculture. *International Journal in Commerce, IT and Social Sciences*, 7(4).
- [46] Barrak, A., Petrillo, F., & Jaafar, F. (2022). Serverless on machine learning: A systematic mapping study. *IEEE Access*, 10, 99337-99352.
- [47] Ramar, V. A., & Rathna, S. (2018). Implementing Generative Adversarial Networks and Cloud Services for Identifying Breast Cancer in Healthcare Systems. *Indo-American Journal of Life Sciences and Biotechnology*, 15(2), 10-18.
- [48] Shaikh, T. A., Rasool, T., & Lone, F. R. (2022). Towards leveraging the role of machine learning and artificial intelligence in precision agriculture and smart farming. *Computers and Electronics in Agriculture*, 198, 107119.
- [49] Garikipati, V., & Pushpakumar, R. (2019). Integrating cloud computing with predictive AI models for efficient fault detection in robotic software. *International Journal of Engineering Science and Advanced Technology (IJESAT)*, 19(5).
- [50] NAIEM, S., AMIRA, M. I., MARIE, M., AYMAN, E. K., GAMAL, I., ABDEL-GALIL, H. A. L. A., ... & TJHIN, V. U. (2022). DDOS attacks defense approaches and mechanism in cloud environment. *Journal of Theoretical and Applied Information Technology*, 100(13), 4632-4642.