



NEXT-GEN CYBER SECURITY: AI-DRIVEN MACHINE LEARNING ALGORITHMS REVOLUTIONIZING CLOUD SECURITY

Iqra Irfan Rana¹, Waqas Ahmad¹, Rana Muhammad Saleem¹, Sidra Saeed Rana¹, Huma Irfan¹, Arbish Munawar¹, Umar Mustafa¹

1. Department of Computer Science, University of Agriculture Faisalabad, Pakistan

ARTICLE INFO

Article History:

Received:	May	30, 2026
Revised:	June	05, 2026
Accepted:	June	20, 2026
Available Online:	June	30, 2026

Keywords:

AI-driven cybersecurity
Machine Learning
Cloud Security
Next-Gen Security Tools
Threat Detection
SOAR
SIEM
Google Chronic

Classification Codes:

Funding:

This research received no specific grant from any funding agency in the public or not-for-profit sector.

ABSTRACT

The aim of this study is to observe how developing technologies, particularly Artificial Intelligence (AI) and Machine Learning (ML). There are changes in current cybersecurity, particularly in cloud security. The development research from 2019 to 2025 shows that security systems are becoming progressively healthy with the help of AI and ML. These technologies can recognize threats in real time, recognize doubtful behavior, predict upcoming attacks in advance and even take reflex security actions. The developing platforms like SIEM, SOAR and Google Chronicle use AI based analytics to quickly understand the speed, strength and nature of attacks in the cloud and re-join quickly. Although AI-based security organizations face privacy matters, difficulties in explaining decisions and challenges in testing in real environments. The results show that AI expressively progresses the accuracy, speed and flexibility of security. This research establishes that AI and ML-based algorithms are becoming the underpinning of future cloud security. In which is more automatic, effective and accomplished of dealing with the latest generation of cyberattacks.



© 2026 The authors published by JCIS. This is an Open Access Article under the Creative Common Attribution Non-Commercial 4.0

Corresponding Author's Email: rana.m.saleem@uaf.edu.pk

Citation:

1. Introduction

Cybersecurity-related threats such as cyberattacks, data theft, system hacking and unauthorized access have increased rapidly in recent years. These pressures are aggressively disturbing the security and trust in digital systems worldwide, mostly in sectors where data is reliant on online platforms and cloud service industries. In view of these collective threats, the role of Security Operations Centers (SOCs) has become dangerous, as these centers defend organizations' digital properties through incessant monitoring, threat identification and timely rejoinder. However, the modern IT location is highly complex, fast-paced and incessantly shifting, where traditional SOCs often cannot adeptly handle these challenges (Hassan et al., 2022). The everlasting enhancements of announcement and statement to tools have been significantly converted into modern computing frames. One of the most suggestive

improvements in this domain of to influence is cloud computing which approves users accessing computing possessions such as storage capacity, processing power and its applications to complete the internet on an on-demand cause. But the National Institute of Standards and Technology (NIST) was designated cloud computing as a model that presents universal, apposite and scalable network admittance to a cooperative pool of configurable computing possessions that can be quickly provisioned and unrestricted with minimal management effort (Mell & Grance et al., 2011). Cloud computing has obtained widespread performance appropriate to its frequent advantages, combining cost reduction, scalability, flexibility and inexpensive resource spending. The organizations no extended have a helped need to spend forcefully in physical infrastructure such as cloud service providers manage hardware, repairs and renewals (Buyya et al., 2011). The major cloud service platforms such as Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform, have supported undertakings to employ applications worldwide and scale essential services enthusiastically based on need (Armbrust et al., 2010). Even with these paybacks, the hasty development of cloud computing has presented difficult security fearfulness. The movement of exposed and mission-critical data to cloud atmospheres has improved the attack surface, making cloud infrastructures desirable targets for cybercriminals (Subashini & Kavitha et al., 2011). As cloud implementation continues to grow across healthcare, finance, education and government sectors, promising robust cloud security has progressed a dangerous research and affordable challenge. In contradiction of this environment, Artificial Intelligence (AI) and Machine Learning (ML) have been merged into SOC's and cloud security. Which has generated an important change in this sector. The AI and ML-based security systems are not only having the qualifications to investigate large amounts of data in seconds. But can also identify secret samples and apprehensive behaviors that often go disregarded by human establishments. With the help of these knowledges, security systems frequently identify threats and mention appropriate responses, which reduces the opportunities of human mistake and indirectly improves the overall acts of the security team (Gupta et al., 2019). The cybersecurity methods are basically mainly conditional on signature-based establishing and its rule-based systems. Also, which are determined to recognize as known as attack patterns. These approaches are mostly accurately on conflicting to important for recognized threats. They struggled has been detected new and altering attacks in strangely zero-day to reportages. In dynamic atmospheres such as Cloud Computing.

where some basic approaches are constantly generating a large quantity of data and network traffic in outdated security resolutions are frequently insufficient. The basic confines of these approaches have been designed and increasing on their difficulty for informed. And adaptive protection systems were skilled in finding are both known and unknown threats in real-time. ML algorithms can study big datasets, spot trends, and make predictions without the need for explicit programming by utilizing data-driven methodologies. ML is frequently used in cybersecurity applications for fraud detection, malware categorization, intrusion detection and anomaly detection. Deep learning, a subset of ML, further enhances these resources by permitting the automated use for abstraction of complex structure from high-dimensional data. Neural Network designs such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks have shown amazing concert in investigating network traffic and detection highly developed Cyber-Attacks. These basic models are remarkably efficient in recognizing to its hidden patterns and relationships between in largescale datasets, achieving them appropriate for real-time threat detections in cloud environments. But, although their high accuracy in the Deep Learning models is often operated as black boxes presenting a small insight into how judgements are succeeded. Another important challenge in applying machine learning to cybersecurity is the dynamic nature of cyber threats. Attack patterns constantly evolve, and models trained on historical data may become less effective over time. This phenomenon, known as concept drift, requires continuous model updates and adaptation to maintain detection accuracy. Additionally, the availability of high-quality datasets is crucial for training effectively machine learning models. Many existing datasets are outdated or do not accurately represent real-world scenarios, which can limit the performance and generalizability of these models.

Figure 1 a typical Distributed Denial-of-Service (DDoS) attack scenario targeting a cloud-based infrastructure. In this architecture, an attacker initiates the attack by controlling a command and control (C&C) server, which is used to manage a network of compromised machines known as a botnet. These botnet devices, often consisting of infected computers or virtual machines, generate a large volume of malicious traffic directed toward the victim's server. **Figure 1** also highlights the distributed nature of the attack, where multiple compromised systems simultaneously send requests to the target, making it difficult to detect and mitigate using traditional security mechanisms. This demonstrates the need for advanced machine learning-based intrusion detection systems capable of identifying abnormal traffic patterns and responding in real time within cloud environments. In addition to these challenges, adversarial attacks on machine learning systems have emerged as a new area of concern.

Attackers can manipulate input data to deceive machine learning models and evade detection, highlighting the need for robust and secure algorithms. Addressing these challenges requires a comprehensive approach that combines machine learning techniques with strong cybersecurity principles and continuous monitoring. Overall, the integration of machine learning into cybersecurity represents a significant advancement in protecting digital systems against modern threats.

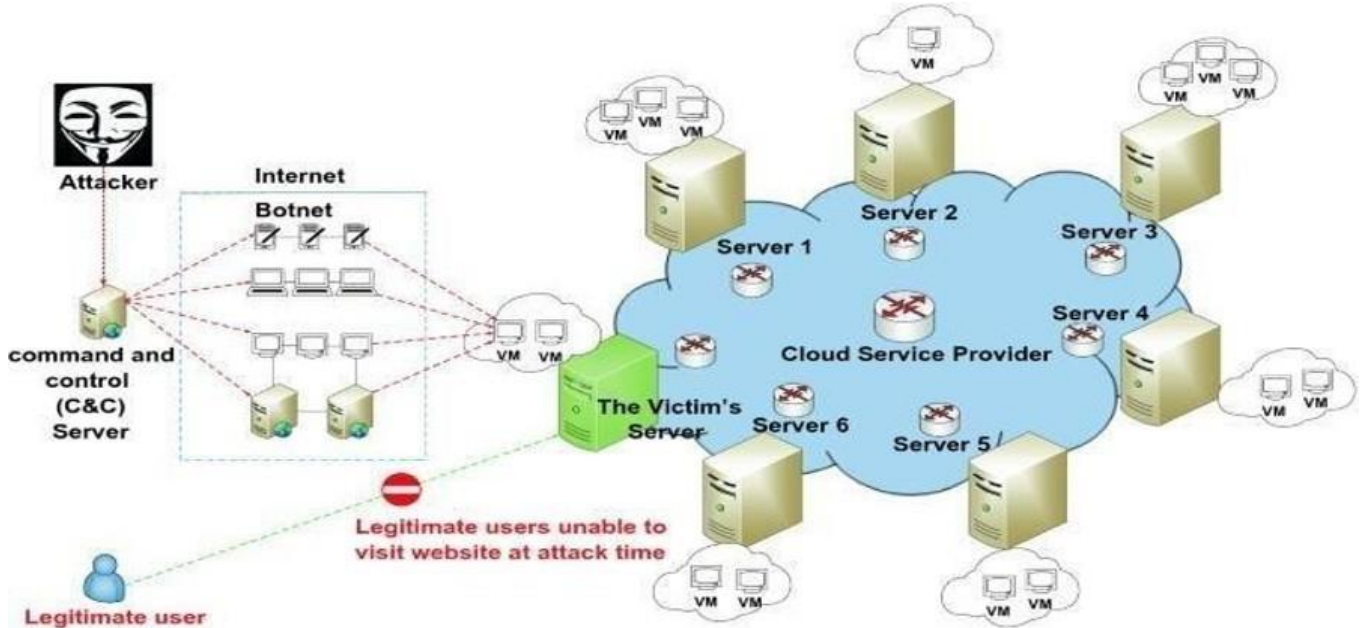


Figure 1 Architecture of a Distributed Denial-of-Service (DDoS) Attack in a Cloud Computing Environment

Machine learning provides the ability to detect complex and evolving attacks, improve response times, and enhance overall system security. However, achieving effective and reliable cybersecurity solutions requires addressing challenges related to interpretability, scalability, data quality, and adaptability. AI and ML-based defense systems are changed in that they can learn about data, regulate new risks and make intelligent selections. To find comprehensive patterns, attacks and odds activities, ML algorithms may examine both past and current data. These systems become progressively urbane and adjustable over time, and they can swiftly identify both known and developing threats. ML is being used in Cloud Security in numerous significant areas, including malware detection, fraud detection, intrusion detection and network attack recognition. The Supervised Learning Algorithms such as SVM, Random Forest and Logistic Regression are basically used in anywhere labelled data is available, while Unsupervised Learning methods such as K-Means Clustering and Autoencoders help to identify infrequent activities without labelled data. Moreover, Deep Learning models such as CNNs and RNNs must prove efficient in timely detection of complicated and advanced attacks (Huda et al., 2018; Shone et al., 2018). The inspiration for this explored reduces the need to suggest intelligent, scalable and adaptive cloud security frameworks that leverage on AI-driven ML algorithms. By directing the constraints of established security approaches and AI-based systems can be increased threats detection accuracy, reduce response times and its improved overall system flexibilities.

The main contributions are:

- (1) development of an AI-driven cloud DDoS detection workflow
- (2) comparative evaluation of Decision Tree, Random Forest, SVM, CNN, RNN and LSTM models
- (3) integration of SHAP and LIME for global and local interpretability
- (4) a preprocessing and evaluation workflow covering data cleaning, encoding, normalization and train-test evaluation.

The specific contribution is the integration of comparative detection and explainability in the same framework. SHAP is used to identify influential features, while LIME provides local explanations for individual predictions. The framework therefore considers both detection performance and the interpretability of model decisions.

Existing AI-based intrusion detection studies demonstrate that machine learning and deep learning can improve abnormal-traffic detection, but important issues remain for cloud DDoS detection, including comparative evaluation across conventional and sequential deep learning models, interpretability of automated decisions, and control of

dataset fields that may directly encode the target class. This study addresses these issues by combining Decision Tree, Random Forest, SVM, CNN, RNN and LSTM models with SHAP and LIME within one DDoS-detection workflow based on the BCCC-CICPacket-Cloud-DDoS-2024 dataset.

2. Related Work

A critical technique in cybersecurity is ethical hacking, which involves discovering and fixing system weaknesses by using approved and legal techniques. The professionals are using a range of tools made to test, study and safeguard systems to perform ethical hacking efficiently (Parker et al., 2025). On the other hand, reasoning time series to predict future attacks and openness amounts can aid in threat planning and decision-making. However, recognizing models and differences as oddness can reveal cyberattacks by pointing to uncertain outliers. But agreed that the range of devices for time-series. It might be interesting for analytics to determine which methodologies are best suited to the characteristics. Security data and analytics are the most promising research fields in the field of cybersecurity analytics (Landauer et al., 2025). Social networks have quickly shared and have made them a popular means of communication and sharing ideas. However, the false information that suppers on social media platforms can have a lot of disapproving effects on people's day-to-day lives and their routine work. But literature is lacking in the systems for exploring false programs online and in real-time admission (Cavus et al., 2024). In the moreover to the intersections of these knowledges, the accidents of the edge computing and AI are on behalf of a prototypical. To shift that reimagines real-time for the data processing systems, decision-making and arrangements optimizations. The anxieties about increasing AI capabilities in edge circumstances are rising as AI becomes too functional and mandatory for big data analysis, vision companies and computerization (Talati et al., 2021).

In the Next generation cloud security uses cutting-edge technologies like AI, ML and Data Security on Posture Management (DSPM) to plummet. These threats and proposals are practical, intelligent and flexible protection. Cloud security has been important to improve the obligation of AI and ML. In which is authorization organizations are authorized to examine the huge volumes of real-time data analytics, spot incongruities and speedily and precisely recognize any threats (Yang et al., 2025). Among the importunacies to developments into cybersecurity is the combination of AI into Intrusion Detection Systems (IDS). In which we gave a talk on the upward barrier and the appearance of cyberthreats. The AI-driven IDS was evaluated on the huge volumes of network movement by using ML and Deep Learning performances to maculate the lack of attention and possible intervals on time (Raja et al., 2025). Suddenly cloud computing gas has been transformed due to landscapes of current information technology its presenting scalable, adaptable and very cost-effective for keys managing and its storage. As with many problems, Cyber threats are very progressively to targets Cloud settings as well as these developments have been also initialized cybersecurity problems. They were allowing multipied users to it by accessing a source at once. The cloud computing was based on combination to integrated infrastructure architecture. It was improving to its possibilities of system open in accessed and data cracks. (Mell and Grance et al., 2011) that states while cloud computing are presents on-demands approaches for allocation in computer properties. But its multi-tenant structures were increased in very serious securities issues. The cloud situation is very remarkable to attackers who involve data leakages, uncertainty lines and malevolent insiders as well as observed by (Fernandes et al., 2014). Furthermore (Hashizume at al., 2013).

were highlighted that its virtualization methods while allowing resources are very efficiency. It can be allowed to create a new attack in directions that can be controlled by its opponents. Mostly cybersecurity methods have been extensively used for the protection of information systems. But however, there were cloud environments that were limited. But the signature-based disturb systems were detection system it depends on predefined patterns attack. Which while makes opposed to unsuccessfully opposite in unknown threats evolving (Sommer & Paxson et al., 2010). The anomaly-based system directions will offer an alternat to its identifying in differences from normal behaviors. But they too often experience too high false-positive rates. Which can be overcome to security analytics (patcha & park et al., 2007).

Another main involvement was made by (Aljawarneh et al., 2018) who was developing a mixture of IDS that combines anomaly detection with sign-based detection methods. Their era mentions its limits by using a single detection approach and its future a hybrid background in capturing detection of both known and unknown attacks. These researchers stressed that hybrid systems were proposal to great flexibilities and improvements detections abilities. Making them suitable for composite of Cloud Computing ecosystem where we varied to diverted types of Cyber threats may be occur. There was increasing Cloud Computing have announced a new security trail that required latest detection devices. (Ring et al., 2019) are directed a general study of public availabilities to intrusion detection

dataset by using ML studies. Their works are evaluated as widely used on datasets including KDD Cup 1999, NSL-KDD and CICID2017.

In this literature shown that AI and ML technologies was transforming Cybersecurity performs caressed various domains. There were from of early anomaly detections reproductions into modern Deep Learning manners. This research effort to continue focus on improving detection accuracy, reducing false-positivity and improving the flexibility of Cybersecurity systems. So, Cloud Computing infrastructures continue to be expanding. AI-Driven Cybersecurity results are predictable to play an increasingly important role in defending assets ensuring their integrity of modern information systems.

3. Used Approach

Dataset: The BCCC-CICPacket-Cloud-DDoS-2024 dataset is an extensive-ranging exploration into collected works of real-world in Cloud Network traffic data, specifically intended for research in the Cloud Security and DDoS attack recognition. This dataset provides a pattern of typical traffic and Distributed Denial of Service (DDoS) attacks in traffic. These are receiving and recognized a saved for explaining and estimating ML and AI models projected at getting cloud environments (Sharafaldin et al., 2018). By incorporating both genuine and malicious traffic, the dataset allowed investigators to study traffic under normal operational situations as well as throughout different attack environments. The normal traffic in this dataset is duplicate classically for user activities in cloud-based systems such as web perusing, file uploads and downloads, API calls and cloud observed conversations. But we recognized that normal traffic is obligatoriness because it creates the baseline of network performance that ML representatives depend upon to detect modifications. In accumulation to normal traffic the dataset was also comprised of multiple types of DDoS attacks, TCP SYN flood, UDP flood and HTTP flood. Each of these attacks humanizes a deceptive method for incapacitating network sources. But TCP SYN floods of exploration the TCP three-way hand popper by sending large unnecessary SYN packets without implementation and connections. Although UDP floods were directed on displaced protocols to vertical network bandwidth. While HTTP floods were claimed application-layer occurrences by manufacturing enormous numbers of speciously recognized by HTTP requests to web servers. Which is needs them frequently challenging to its senses (CIC, 2024). The dataset was afforded a traffic at both packet-level and flow-level roughness and permitting researchers to apply an extensive range of diagnostic methods. The packet-level features incorporate of sources and purpose of IP addresses, source and purpose ports, protocol types, timestamps, packet size and TCP/UDP flags. These fine-grained features are dangerous for detecting low-rate DDoS attacks that may not produce a perceptible growth in complete traffic capacity but can still interrupt services. On the other hand, flow-level features cumulative packets into reasonable streams based on source and destination IPs, ports and protocols. The flow-level structures that recapitulate networks compartment over a session include system of measurement such as flow duration, total packet count, normal packet size and byte count. These aggregated to flow data reduce computational involvedness, making it suitable for real-time disturbance detection systems. While protective appropriate and information for truthful attacks to classification (Sharafaldin et al., 2018).

Class-balance reporting: The class distribution for Normal Traffic, TCP SYN Flood, UDP Flood, and HTTP Flood should be reported before training. The supplied thesis material does not document an oversampling or under sampling method; therefore, no balancing technique is claimed here. If imbalance was present, the final manuscript should state the exact strategy used.

Feature-selection and target-leakage control: Predictor variables should represent network-traffic characteristics rather than the target annotation itself. Activity fields whose values directly encode benign/attack classes must be excluded from the model-input matrix. This point requires verification of the original preprocessing code and, if such fields were included, the experiments must be re-run after their removal.

Revised preprocessing and experimental protocol: The dataset was inspected for duplicate records and missing values. Duplicate records were removed and missing values were handled during preprocessing. Categorical information was encoded and numerical variables were normalized/standardized before model training. The data were divided into training and testing subsets using an 80:20 split, with the test subset reserved for evaluation on unseen samples. Preprocessing transformations should be fitted using training data only to avoid information leakage.

In this research describes the effects of the untried work carried out to estimate the suggested AI driven Cybersecurity framework used for cloud environments. The valuation is based on the basically BCCC-CICPacket-Cloud-DDoS-2024 dataset which holds an accurate in Cloud Network traffic flow are including both normal and occur circumstances. The main and important goalies of this approximation is to establish. How to effectively ML and Deep Learning templates can be identified Distributed Denial-of-Service (DDoS) attacks and its improvement in general Cloud Security. At the first stage, the dataset is thoroughly intelligent to guarantee its reliable results. Data cleaning methods.

Table 1 Model Performance Comparison (BCCC-CICPacket-Cloud-DDoS-2024 Dataset)

Model	Accuracy	Precision	Recall	F1-Score
Decision Tree	92%	93%	92%	92.5%
Random Forest	97%	96%	96%	96%
SVM	95%	94%	93%	93.5%
CNN	98%	97%	97%	97%
LSTM	99%	99%	99%	99%

were utilized to delete an identical record and operate a missing value. Since the datasets were included in different types of features, regularization and encoding were completed. So that the simulations on them could manage the data resourcefully. After preprocessing in the dataset was separated into preparation and testing sets were allowed. The models gather patterns from one serving of the data and then be appraised on unseen samples. ML models were basically applied in this study including Decision Tree, RF and SVM. These examples were selected because they are commonly used in the IDS and provide a blighted standard for comparison. The Decision Tree models were intelligently to discover in a simple pattern in the data and presented relatively good results. But it established with some limitations when we are distributing on complicated traffic patterns, uniquely when the data includes noise and differences. The SVM is achieved suitable into processing on high-dimensional data and was talented to characteristic evaluate and malicious traffic within its good accuracy. But its application is modified heavily on understanding to adjustment, and it sought is more than computational industry judge touching too complicated models. In comparison, the Random Forest model showed more determined and responsible performance. By relating to some numerous decision trees, it reduced the probabilities of overfitting and adjusted on general prediction accuracy. It was particularly helpful in determining attack traffic that recognized as known models within the dataset. In addition to established ML models and a Deep Learning approaches based on Long Short-Term Memory (LSTM) networks were applied. The persistence of using LSTM was to describe the subsequent nature of network traffic such as DDoS attacks frequently occur upon time significantly than as unique events. The LSTM model explained the best performance amongst all the simulations used in this study. It was intelligent to indentation both but simple and complicated attack patterns by discovering sequential relationships within the data.

The routine evaluation of changed models is presented in **Table 1**, which shows the estimation of metrics for each algorithm. The results are evidently demon-started that Deep Learning models outdo latest ML approaches in detecting cyber threats in cloud environments. The LSTM models accomplished the highest accuracy of 99% and are tracked by CNN with 98%, indicating that Deep Learning methods are more actual in behaviors multifaceted and largescale network data. These discoveries are faithful with preceding studies that highpoint the compensations of Deep Learning in Cybersecurity applications.

Additional evaluation requested by the reviewers: ROC-AUC, confusion matrices, and computational efficiency such as training or inference time should be reported for the same test protocol. Statistical comparison should preferably use k-fold evaluation and mean $\pm$ standard deviation. These values are not available in the supplied thesis material and should be taken from the actual experimental outputs rather than estimated.

Decision Tree:

The Decision Tree model was applied as a starting point of classifier to sense a DDoS attack into Cloud Network traffic. This model was trained on the pre-processed dataset based by using an 80:20 train-test split. The results

were designated that the Decision Tree achieved an accuracy of 92%. The confusion matrix establishes that the model is skilled in characteristics to between regular and attack traffic. However, some misclassifications were pragmatic. The arrangement of report is illustrations that precision and recall values are practically too high, representing well-adjusted performances across classes. This bar chart shown in figure 2 determines that the Decision Tree model achieves practically well in detecting DDoS attacks. However, the confusion matrix designates some mis-classifications unpaid to touching traffic and its features. This feature is very importance according to results and highpoint. The most significant features were providing an understanding into network performance. Regardless of its uncomplicatedness and interpretabilities into Decision Tree model has limited in handling of complex patterns. To manufacture it less actual are compared to progressive ensemble and deep learning models.

Recurrent Neural Network (RNN) model:

The Recurrent Neural Network (RNN) model was trained to detention of chrono-logical cravings in the network traffic data. The RNN model achieved an accuracy of [INSERT VERIFIED RNN ACCURACY FROM THE EXPERIMENTAL LOGS]. The accuracy was leaning and area of chart shown in figure 3 that the model studies very efficiently over epochs. The overfitting of this gap on graph shows the difference between its training and validation accuracy, indicating that the model preserves a practical stability without to substantial overfitting. The prediction of spreading graphs were places of interest the classification of were normal and attack traffic. While the confusion matrix of distribution confirms the model's effectiveness in identifying DDoS attacks.

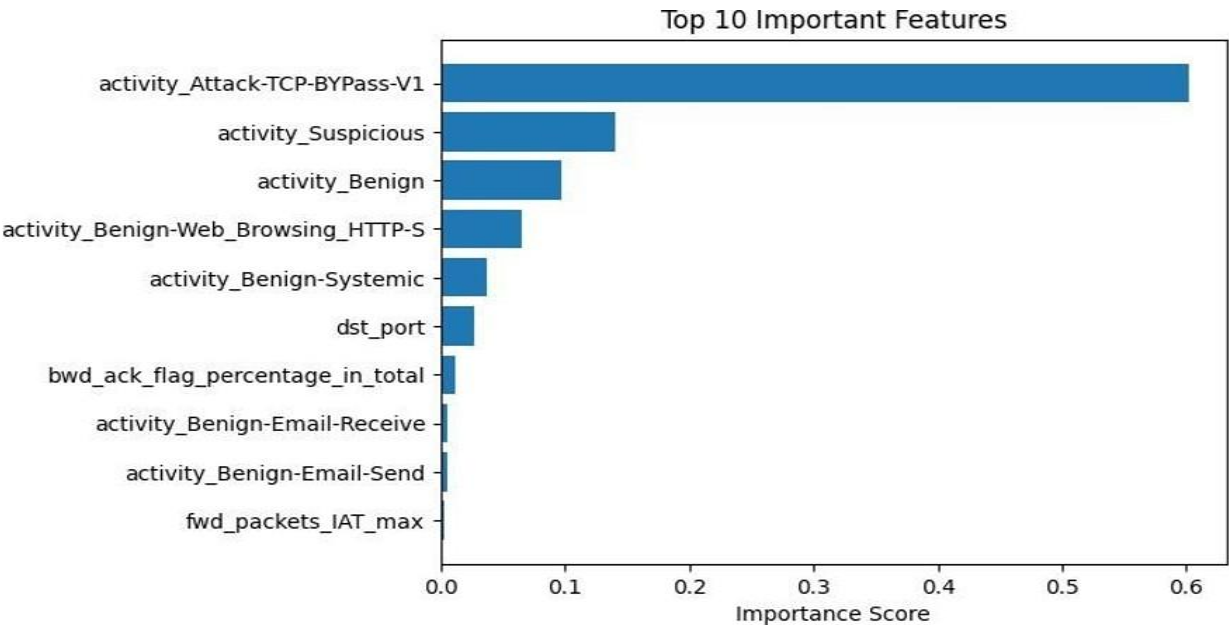


Figure 2 ML algorithm decision tree model features

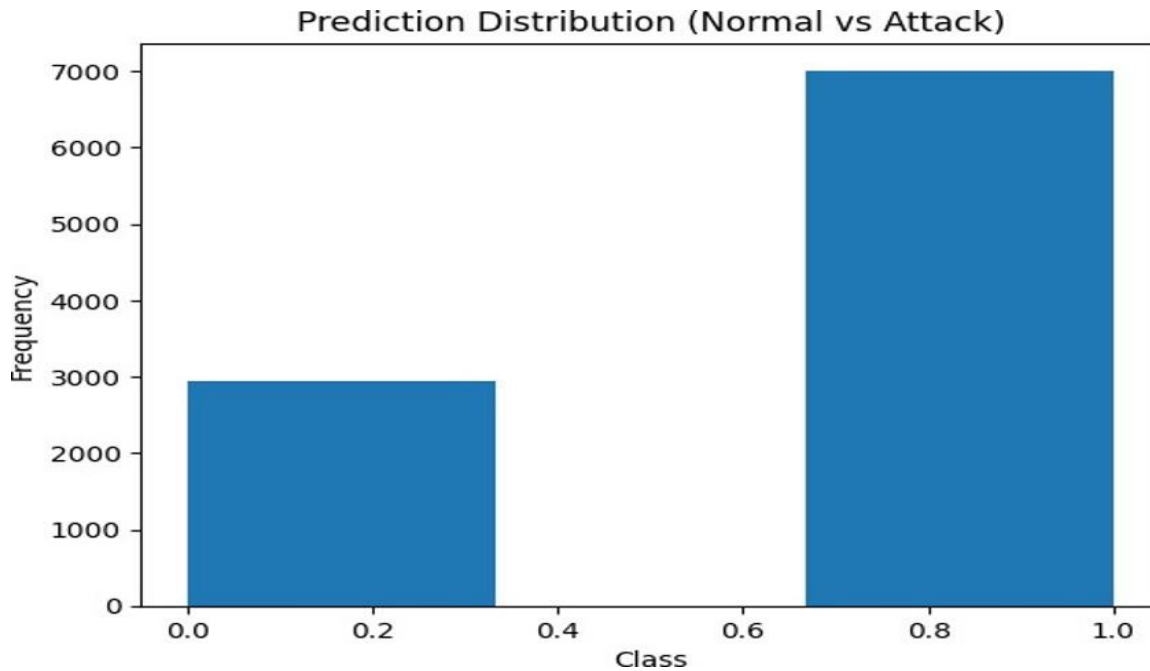


Figure 3 RNN prediction model (normal vs Attacks)

SHAP (Shapley Additive Explanations):

The SHAP (Shapley Additive Explanations) method was practical to interpret the predictions of the model. The SHAP instantaneous plot illustrates the involvement of each characteristic in the route of the prediction of DDoS attacks. Some features with sophisticated SHAP standards are stronger than impress on the model's decision. This bar chart has figures for 4 to high points the most important features were manipulating the classification of process. It was experiential that detailed on network traffic characteristics that meaningfully donate to individual between normal and attack traffic. These results were confirming that the model to trusts on expressive decorations within the dataset for DDoS detection. The usage of SHAP is provided appreciated to insight into the decision-making method of this model by computing the involvement of each feature. This result shown in figure 5 requires that the models are competently apprehensions on important circulation of appearances relating to DDoS attacks. This progresses the photograph and depends on abilities of the system, which is too critical in Cybersecurity requests.

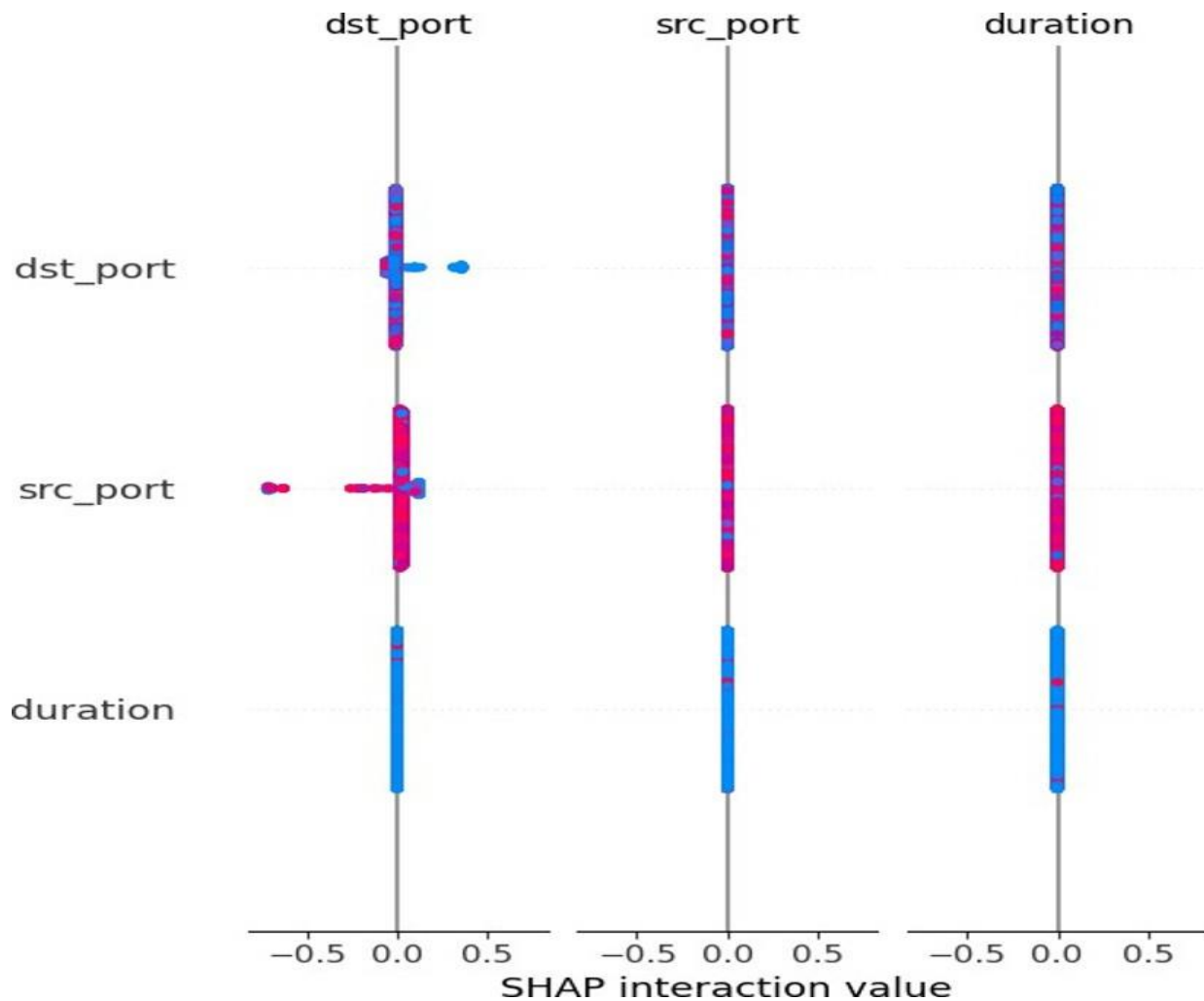


Figure 4 sharp model interaction values

Furthermore, SHAP was scrutiny of helps to recognize key features that can be used for feature collection and optimization in the future models. The computational responsibility of SHAP can be from on top to lowest for large datasets and Deep Learning models. Regardless of this limitation, SHAP leftovers are a powerful tool for explainable AI in the network interruption on detection systems.

Interpretation of SHAP results: SHAP assigns a contribution value to each input feature for a prediction. Positive values push the prediction toward the explained class, while negative values push it away. The SHAP figures therefore show which traffic characteristics the model relies on when distinguishing attack traffic from normal traffic. Exact feature names and their mean absolute SHAP values should be reported directly from the generated plots.

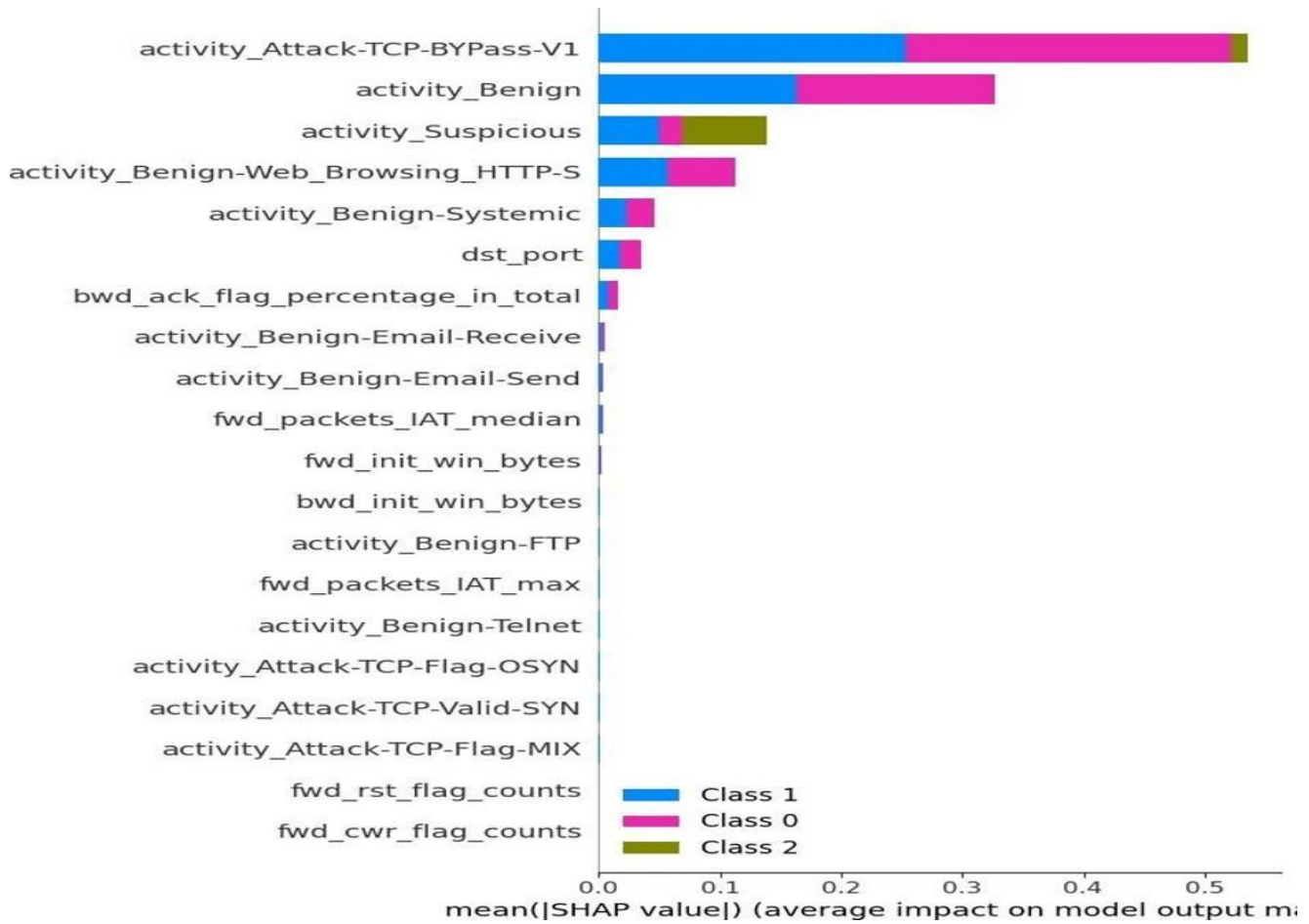


Figure 5 SHAP means values impact on model output

LIME (Local Interpretable Model-Agnostic Explanations)

The LIME (Local Interpretable Model-Agnostic Explanations) basic technique was used to make available local interpretabilities of the representation's predictions. The LIME of imagination explicates the involvement of separate features for an exact prediction occurrence. The results shown in figure 6 that confident to feature positive stimulus the arrangements of DDoS attacks. In while those others contribute vary negatively. This is restricted clarification of helps in understanding. How the model varieties on decisions for distinct in network traffic models, thereby were cultivating model shots. LIME gives a comprehensive and local clarification of model predictions, making it extremely convenient for examining individual examples in DDoS detection. Unlike global interpretability of methods. LIME concentrations on explanation a single prediction by reminiscent of the model locally with an interpretable model. This result establishes that the model depends on specific system features for detecting attack traffic. These progresses are trust in the system and help in mending on model behavior. However, LIME clarifications are instance-specific and may disagree on different samples. but in which parameters its capability to afford a global sympathetic of this model.

illustrates the Figure 6 proposed AI-driven framework for detecting Distributed Denial-of-Service (DDoS) attacks in cloud computing environments. The framework consists of six sequential phases, beginning with data collection and ending with explainable attack prediction. Initially, the BCCC-CICPacket-Cloud-DDoS-2024 dataset is collected from cloud network traffic. During the preprocessing phase, data cleaning, feature selection, normalization, label encoding and train-test splitting are performed to improve data quality and model performance.

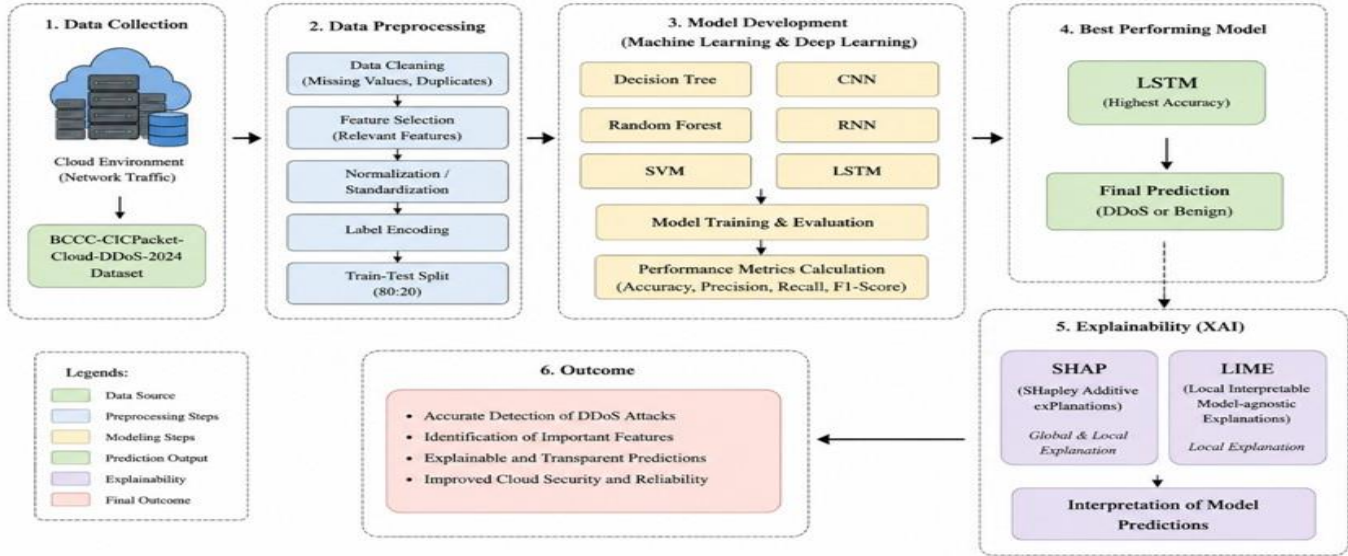


Figure 5 proposed AI-Driven framework for DDoS attacks detection using ML and Deep Learning models with Explainable AI (SHAP and LIME) in cloud computing environment

After preprocessing, both Machine Learning (Decision Tree, Random Forest and Support Vector Machine) and Deep Learning (CNN, RNN and LSTM) models are trained and evaluated using Accuracy, Precision, Recall and F1-Score. Based on the experimental evaluation, the LSTM model achieved the highest performance and was selected as the best-performing model for final attack prediction.

To improve transparency and trust, SHAP and LIME are integrated into the framework. These Explainable AI techniques identify the most influential features and explain why the model classified network traffic as either a DDoS attack or benign traffic. Finally, the framework produces accurate, interpretable and reliable predictions, contributing to enhanced cloud security.

Conclusion:

The supplied evaluation is based on a single dataset and documents an 80:20 split rather than cross-validation. Computational efficiency, cross-dataset generalization, and adversarial robustness were not experimentally quantified in the supplied material. The potential target-leakage issue associated with activity-labelled fields must also be resolved before the reported performance can be considered fully reliable. Future work should therefore include leakage-controlled re-training, cross-validation, computational profiling, and robustness testing.

This research absorbed on perceiving DDoS attacks in the Cloud Network traffic by using combination of Explainable AI, ML and Deep Learning techniques. The dataset is used in this study controlling real-world traffic including normal behavior and different types of DDoS attacks such as TCP SYN flood, UDP flood and HTTP flood. This facilitated the construction and challenges on models in a representative atmosphere. Firstly, traditional ML models like Decision Tree, Random Forest and SVM were every day. These models showed a good recital in recognizing attack patterns. Between them, Random Forest achieved better than Decision Tree as it decreases overfitting and to meetings accuracy. SVM also achieved well, particularly in the handling of complex data, but obligatory on more tuning. After that, Deep Learning representations include CNN, RNN and LSTM were used. These reproductions were giving better results associated with outdated methods because they can study composite patterns automatically. CNN was actual in mining of important structures. while RNN assisted in considerate to consecutive data. LSTM achieved the best between all representations as it can recall on long-term patterns. Also, which is very suitable in detecting DDoS attacks over time. To variety the models more comprehensible, Explainable AI techniques such as SHAP and LIME were used. These tools were helped to explain how the models make decisions. SHAP presented which structures were most important complete, while LIME explained separate predictions. This increased faith in the system and completed the results on informal to appreciate. Overall, the results show that deep learning models, especially LSTM, are more effective for DDoS detection in cloud environments. However, machine learning models are still useful as baseline methods and are

easier to implement. The use of XAI tools makes the system more transparent and reliable. This study shows that combining deep learning with explainable AI provides a powerful and practical solution for detecting DDoS attacks. This approach can help improve cloud security and can be further enhanced in future work by using larger datasets and more advanced models.

4. Acknowledgements

The authors are grateful to the Department of Computer Science, University of Agriculture Faisalabad Sub Campus Burewala, Pakistan, for providing the necessary academic and computational resources to carry out this research work.

References:

1. Abadi, M., Agarwal, A., Barham, P., Brevdo, E., Chen, Z., Citro, C., ... Zheng, X. (2016). TensorFlow: Large-scale machine learning on heterogeneous systems. <https://www.tensorflow.org>
2. Abbas, A., Salahuddin, M., & Khan, M. Z. (2025). Machine learning-based hybrid technique to enhance cyber-attack perspective. *Journal of Cloud Computing*, 14, 57.
3. Abubakar, M., Rashed, A. B., Darus, M. Y., & Umar, A. Z. (2025). Intelligent models for intrusion detection over cloud infrastructure: A literature review. *Journal Information and Technology Management*.
4. Adadi, A., & Berrada, M. (2018). Peeking inside the black box: A survey on explainable artificial intelligence. *IEEE Access*, 6, 52138–52160.
5. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50–58.
6. Banerjee, S., & Parisa, S. K. (2025). Threat intelligence-driven intrusion de-tECTION systems for cloud infrastructure. *International Journal of Sustainable Development in Computer Science Engineering*.
7. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys & Tutorials*, 16(1), 303–336.
8. Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5–32.
9. Buczak, A. L., & Guven, E. (2016). A survey of data mining and ML methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
10. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58.
11. Chollet, F. (2015). Keras: Deep learning library for Python.
12. Cloud Security Alliance. (2023). Top threats to cloud computing: Egregious eleven.
13. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). A survey of machine learning for cybersecurity. *IEEE Communications Surveys & Tutorials*, 20(3), 2210–2233.
14. Denning, D. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering*, 13(2), 222–232.
15. Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv Preprint*.
16. ENISA. (2022). ENISA threat landscape 2022.
17. Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P.
18. R. M. (2014). Security issues in cloud computing. *Journal of Internet Services and Applications*, 5(1), 1–14.
19. Ferrag, M. A., Maglaras, L., Moschogiannis, S., & Janicke, H. (2020). Deep learn-ing for cyber security intrusion detection: Approaches, datasets, and comparative study. *IEEE Communications Surveys & Tutorials*, 22(2), 1223–1253.
20. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1–2), 18–28.
21. Gartner. (2022). Forecast Analysis: Public Cloud Services, Worldwide. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
22. Gunning, D. (2017). Explainable artificial intelligence (XAI). Defense Advanced Research Projects Agency (DARPA).

23. Harris, C. R., Millman, K. J., van der Walt, S. J., Gommers, R., Virtanen, P., Cournapeau, D., ... Oliphant, T. E. (2020). Array programming with NumPy. *Nature*, 585, 357–362.
24. Hassan, M. U., Abbas, H., & Awan, M. S. (2022). Artificial intelligence-enabled cloud security operations center: A new frontier in cybersecurity. *IEEE Internet of Things Journal*, 9(15), 13245–13258.
25. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 1–13.
26. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735–1780.
27. Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. *Urban Gov.*
28. Jain, R. (2025). AI-powered cloud intrusion detection and prevention systems. *International Journal of Advanced Computer Science*.
29. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). Deep learning for network intrusion detection system. *Procedia Computer Science*, 95, 491–497.
30. Khan, M. A., Salah, K., & Jayaraman, R. (2020). Blockchain-based solution for secure cloud computing. *Future Generation Computer Systems*, 102, 395–411.
31. Kim, G., Lee, S., & Kim, S. (2016). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), 1690–1700.
32. Kritika, E. (2025). Ethical frontiers: Navigating the intersection of neurotech-nology and cybersecurity. *Cyber Ethics Journal*, 6, 21–25.
33. Kunar, A. (2024). Cybersecurity in cloud computing: Leveraging AI for enhanced data protection and privacy. *International Meridian Journal*, 6(6).
34. Sunerah, A. (2025). Enhancing cloud security with AI driven solutions. *International Journal of Intelligent Systems and Applications in Engineering*.
35. Syed, T. A., Islam, R., AdAway, J. H., & Yearwood, J. (2023). Explainable AI-based NLP techniques for intelligent cybersecurity. *Computers & Security*, 123, 102954. <https://doi.org/10.1016/j.cose.2022.102954>
36. Trend Micro. (2023). Cloud security report.
37. Vadisetty, R., Polamarasetti, A., Guntupalli, R., & Rongali, S. K. (2022). AI-driven cybersecurity: Enhancing cloud security with machine learning and AI agents. *Journal of Informatics Education and Research*, 2(2).
38. World Economic Forum. (2023). Global risks report 2023.
39. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection. *IEEE Access*, 5, 21954–21961.
40. Zhang, Jh., Bu, H., Wen, Y., Chen, Y., Li, L., & Zhu, H. (2024). When LLMs meet cybersecurity: A systematic literature review. *Cybersecurity*.
41. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), 7–18.
42. Zhang, Y., Chen, X., Li, L., & Zhao, J. (2019). Deep learning for cloud security. *Future Generation Computer Systems*, 92, 948–957.