International Journal in Physical and Applied Sciences
Volume 07 Issue 5, May 2020 ISSN: 2394-5710 Impact Factor: 4.657
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

ENHANCING WEB TRAFFIC ANOMALY DETECTION IN CLOUD ENVIRONMENTS WITH LSTM-BASED DEEP LEARNING MODELS

[1]Venkat Garikipati
Network Architect,
latidude 36,
California, USA
venkat44556@gmail.com

[2]S Bharathidasan
Sree Sakthi Engineering College, Karamadai, Coimbatore
India
sbharathiece@gmail.com

Abstract
Web traffic forms the core of cloud applications but poses numerous security threats such as DDoS, SQL injections, and several unauthorized access attempts. Therefore, detecting any abnormal traffic patterns like spikes or random-access properties bring significance in the protection of cloud environments. This study is focused on discovering web traffic anomalies using Long Short-term Memory networks (LSTM). In contrast to the conventional rule-based systems with pre-set thresholds, excellent capturing of sequential dependencies in traffic data makes it favorable to use LSTM models for spotting intricate and changing trends in web traffic. For the given data about LSTM model which attained: 98.5% accuracy, 98.4% precision, and 98.7% recall, wherein the model characterized normal and suspicious traffic. The training of the model has been accomplished over a dataset of 1500 samples. Model classified traffic as 'normal' or 'suspicious', with these results True Positives (TP) = 430, True Negatives (TN) = 1048, False Positives (FP) = 15, and False Negatives (FN)= 7. Also, the validation of the developed model was carried out with a ROC-AUC score of 0.98. This clearly proves the model has a strong ability to differentiate normal from anomalous traffic. This would be a dynamic scalable solution for real-time anomaly detection, automatic identification, and response mechanism against security threats in cloud environments, thereby improving overall security and reducing possible risks.

Keywords: *Web Traffic, Anomaly Detection, LSTM, Cloud Security, Deep Learning, Real time detection*

1. Introduction

Web traffic remains the lifeblood of cloud applications and services in the current digital age [1]. As businesses migrate their operations to cloud environments, the complexity and volume of web traffic have increased tremendously [2]. While this traffic is critical for service delivery, it simultaneously paves the way for multiple cyber-security threats, within which malicious actors take advantage of the various vulnerabilities present in web infrastructure to perform different attacks like Distributed Denial of Service (DDoS), SQL injections, and other unauthorized ways of entry [3] [4]. Hence, abnormal behavior detection in web traffic such as sudden spikes, unusual access patterns, and suspicious requests is essential for identifying and mitigating impending cyber threats [5] [6]. Without early detection, organizations may face an enormous compromise of sensitive data and downtime, with probable long-lasting damages to their reputation [7] [8]. The current need for advanced detection systems that monitor and respond to traffic anomalies within cloud environments is unprecedented [9].

Over the last decades, web traffic analysis has mostly revolved around techniques such as rule-based systems and statistical algorithms for anomaly detection [10]. As the size and complexity of cloud environments keep increasing, these old approaches have become less useful for accurate detection of complex anomalies [11]. In many regards, rule-based systems establish their predefined thresholds and rules that work for simpler datasets and small volumes but fail because of rapid changes in modern web traffic [12]. The core attributes associated with a cloud environment are high data ingestion, fast-changing traffic patterns, and a diverse nature of user behaviors [13]. These attributes cannot be represented adequately using static rules or straightforward models [14]. As a result, inaccurate markings become rampant with false positives and false negatives, which means either delayed threat detection or overlooks of

ongoing attacks [15]. The sophistication with which cyber threats are evolving has ensured that the need for more advanced, flexible, and scalable approaches to anomaly detection have arisen to deal with the complexities posed in modern cloud infrastructures [16] [17].

The long short-term memory (LSTM) model is a type of RNN that can effectively solve the problems of web traffic anomaly detection in the cloud environment [18]. Unlike classical methods, LSTM networks function better in processing sequential data where the current event is dependent on the previous ones such as in the case of web traffic that deals with time-series data [19] [20]. The ability of LSTM to capture long-term dependencies and temporal relations enables the model to learn complex patterns in traffic over the period of time and can differentiate between normal variations from abnormal traffic behavior [21] [22]. Sudden spikes in requests, several failed login attempts, or even odd session durations may be recognized by LSTM as possible attack signatures [23]. Because it is trained on datasets obtained from history, the LSTM model can also be tuned to accommodate evolving traffic patterns and hence provide a more accurate and dynamic solution for the detection of anomalies in cloud-based systems, thereby helping improve their security posture [24] [25].

The main purpose of this research is to develop LSTM-based deep learning models to enhance cloud web traffic anomaly detection. This detection relies on observing and classifying abnormal behavior from normal traffic patterns using LSTM networks processing sequential web traffic data in near real time. The approaches differ from conventional rule-based systems in that LSTM models learn dynamically from the data unlike traditional systems that lay hard rules, enabling traffic pattern adaptation as well as scaling to adequately support a very large cloud environment. The research will look at modeling and testing for an LSTM model that can classify web traffic as normal or suspicious in real-time. This is proposed for stronger automation in anomaly detection and helping the enhancement of cloud security systems in their response to changing threats. The work develops strength for other effective, adaptive, and scalable approaches to web traffic monitoring security in cloud environments.

Objectives

- By virtue of their inherent ability to capture temporal dependencies from data, LSTM-based models can be utilized here to analyze such files for web traffic pattern anomalies.
- The LSTM model thus achieved would also be validated in terms of the performance metrics i.e., accuracy, precision, and recall for differentiating suspicious from normal traffic patterns with regard to its effectiveness.
- This may include devising a more effective anomaly detection scheme for cloud environments toward mitigating security risk by applying deep learning techniques like LSTM on web traffic data.
- The traffic data in cloud environments could then be monitored in real-time to note any abnormal behavior and react accordingly, thereby increasing security for clouds and reducing associated risks.

2. Literature Survey

Cardiovascular diseases (CVDs) are recognized as a significant global health problem, requiring innovative approaches to improve care [26]. This includes leveraging network analysis, comparative effectiveness research (CER), ethnography, and big data tools such as electronic health records (EHRs), molecular data, and AI-based analytics to evaluate heart medications and patient care plans [27]. The goal is to systematically develop cost-effective, personalized treatments based on genetic, clinical, biological, and socioeconomic factors to enhance clinical outcomes and cardiovascular healthcare decisions [28]. Improving decision-making in IoT systems can be achieved through integrating Device Management Platforms (DMPs) with Self-Organizing Maps (SOMs) for dynamic data processing [29]. SOMs cluster and visualize high-dimensional IoT data to detect patterns and anomalies early, while DMPs facilitate data collection and communication [30]. This integration supports live monitoring and performance tuning, offering improvements over conventional approaches [31].

A model combining social influence-based learning reinforcement with metaheuristic optimization of tensor networks built on neuro-symbolic paradigms aims to enhance adaptive AI [32]. By integrating social reinforcement, evolutionary optimization, and neuro-symbolic processing, the system supports real-time collaborative adaptive behavior influenced by social and environmental factors [33]. This approach promotes robust, self-improving solutions in software development through logical and data-driven decision-making [34]. A comprehensive healthcare framework integrates Artificial Intelligence, Big Data Mining, and Internet of Things (IoT) technologies [35]. IoT enables continuous data acquisition, Big Data Mining extracts actionable insights, and AI supports predictive modeling and decision-making [36]. This combination optimizes resource utilization, enhances productivity, and facilitates patient-specific care, addressing traditional healthcare challenges with sustainable solutions [37].

A hybrid fog-cloud AI architecture combines cloud computing's analytical capabilities with fog computing's proximity to data sources for real-time ECG analysis [38] [39]. Fog nodes process signals near the source, reducing latency and bandwidth use, while advanced machine learning algorithms in the cloud deliver accurate cardiovascular anomaly detection [40] [41]. This approach enhances scalability, energy efficiency, and continuous patient monitoring for early diagnosis [42]. A trust prediction model uses deep learning, Bayesian inference, and reinforcement learning to assist dynamic decision-making in cloud environments [43] [44]. Historical trust data, anomaly detection results, and behavioral metrics feed into a deep neural network, while Bayesian inference continuously updates trust scores for real-time risk assessment [45] [46]. This hybrid method supports secure cloud resource management through optimal allocation and risk mitigation, with future exploration of blockchain, federated learning, and quantum computing for further optimization [47] [48].

An ML-based detection system for IoT networks addresses Ping Flood attacks by combining Decision Trees and K-Nearest Neighbors (KNN) algorithms [49]. This multi-model approach improves attack detection accuracy and efficiency while reducing computational overhead. It effectively separates normal and attack-prone traffic in real-time, offering a scalable and resource-efficient solution [51]. Future work includes exploring deep learning and federated learning to enhance model performance and data privacy [52]. An LSTM-based threat detection framework targets healthcare cloud security by capturing anomalies and abnormal user activities, such as unauthorized access, ransomware, and insider threats [53]. Deployed on cloud platforms integrated with security centers and machine learning services, it analyzes security logs for scalable anomaly detection [54] [55]. This framework contributes to AI-driven cloud security solutions tailored for healthcare infrastructures.

An integrated Graph Neural Network (GNN) and Long Short-Term Memory (LSTM) approach addresses security and performance in distributed software systems [56]. GNN captures spatial relationships between system components, while LSTM predicts temporal patterns for anomaly and intrusion detection [57]. This framework surpasses traditional methods in detection accuracy and alert response time but faces scalability challenges when optimized for large systems [58]. An IoT-Fog-Cloud hybrid architecture optimizes signal processing, resource management, and Quality of Service (QoS) for improved patient monitoring beyond healthcare facilities [59]. It coordinates data collection from IoT devices, real-time processing via fog computing, and cloud storage and analysis [60]. Adaptive filtering and wavelet transforms enhance signal quality, while dynamic scheduling maximizes computing resource utilization. QoS improvements include reduced response time through bandwidth maximization and latency minimization.

2.1 Problem Statement

The streaks of technological changes via IoT, AI, and Cloud Computing are evidently spraying showers of benefits over myriad fields, with healthcare being one of the many. However, inseparable from these boons are the greater demons in the form of security, resource management, and real-time data processing challenges. Conventional approaches serve to be inadequate under the harsh and dynamic modifying environments of modern systems, especially the distributed ones [61]. Growing complexities such as cybersecurity threat detection, optimization of resources for efficient delivery of care, and large-scale management of data have come to the forefront [62] [63]. While solutions are not far-off with the advent of advanced modeling using Graph Neural Networks, Long Short-Term Memory, fog-cloud hybrids and others, problems facing real-time processing remain scalability, latency, and complexity [64]. In realistic terms, predictive analytics for the optimized decision-making process with low resource usage and multi-faceted attack scenarios shall be greatly improving IoT systems, cloud security, and healthcare infrastructure. The above scenarios call for a shifting need of solutions toward being more dynamic, efficient, and secure.

3. Proposed Methodology

Such anomaly detection models in web traffic exist primarily through the use of LSTM methods. Real-time web traffic data are acquired in the AWS CloudWatch environment, where they enter a preprocessing phase consisting of data cleaning and normalization. Feature extraction is then used to extract suspicious patterns like IP behavior, session duration, and request type into the model. Afterward, the models are trained, and predictions are made, with their results stored on the cloud so that real-time monitoring can happen, with an automatic response compilation to threats.

International Journal in Physical and Applied Sciences
Volume 07 Issue 5, May 2020 ISSN: 2394-5710 Impact Factor: 4.657
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

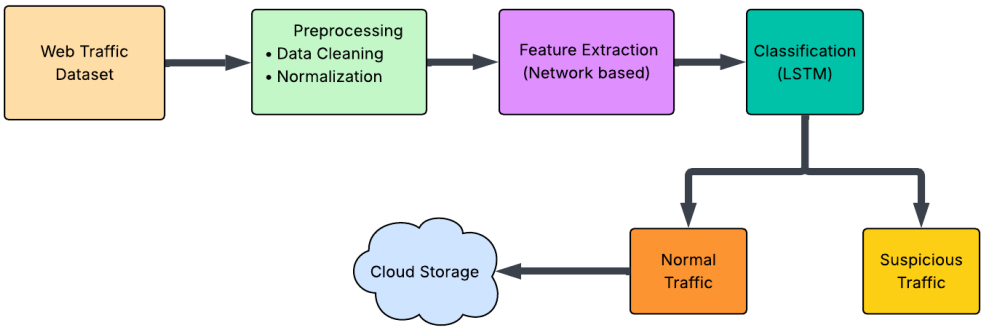

Figure 1: Workflow for Web Traffic Anomaly Detection using LSTM-Based Classification

3.1 Dataset

Web traffic data is gathered from various cloud environments through AWS CloudWatch. Metadata involved consists of request types, response codes, time stamping, IP addresses, and HTTP headers. The main objective is to grant proper access to those logs with all the relevant access permissions. This data is used in the monitoring of traffic behavior, in anomaly detection, as well as in the prediction of different security threats to cloud-based systems including activities associated with real-time anomaly detection and threat response.

3.2 Preprocessing

Preprocessing is another very arduous task in the conversion of raw data to usable data for analysis and model training. It involves various methods to maintain quality, uniformity, and compatibility of this data with machine learning models. Generally, data cleaning and normalization standardization are the activities carried out during this stage.

3.2.1 Data Cleaning

One feature of this process is dealing with missing values most often by replacing them by imputation or deleting; duplicates are dealt with, and irrelevant data points are cleaned to maintain only valid and useful data. Most common imputations use mean value imputation:

$$\text{Imputed Value} = \frac{\sum x}{n} \tag{1}$$

where x represents the feature values and n is the total number of data points.

3.2.2 Normalization

Normalization processes numerical features into a standard range, usually between 0 and 1. This is important under several conditions, when some data have different scales, such as request sizes or response times. Min-Max normalization is the most popular of them:

$$X_{\text{norm}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{2}$$

where $X_{\min}$ and $X_{\max}$ are the minimum and maximum values in the dataset

3.3 Feature Extraction

Feature extraction entails identifying those web traffic patterns that could indicate anomalies or possibly hint at some irregular behavior. Some of them may include analyzing the behavior patterns of the source IP to identify unusually high request frequency, measuring the session length used to identify abnormal sessions, or looking at the types of requests made (GET, POST, etc.) in order to find herbaceous access patterns. With the detection of abnormal behavior in such network-based features, botnet activity, brute-force attacks, or possible injection attacks may be detected and flagged for further investigation.

3.3.1 Source IP Behavior Patterns

Abnormalities may include request frequency from certain IPs where there could be repeated requests or certain suspicious activities. A frequent practice is to compute request frequency per IP in a time window.

$$\text{Request Frequency} = \frac{\text{Total Requests}}{\text{Time Window}} \tag{3}$$

High frequency of requests within a short period can indicate botnet activity or brute-force attacks.

3.3.2 Session Duration

Keeping track of the sessions length is a means to identify anomalous behavior in the system, such as being too long or too short, which implies suspicious activities. The session duration is calculated as:

$$\text{Session Duration} = \text{End Time} - \text{Start Time} \quad (4)$$

Unusual session durations can be flagged as anomalies for further inspection.

3.3.3 Request Types

By analyzing the frequency in which different HTTP request types (e.g., GET, POST) occur, we can also identify unusual access patterns. A sudden spike in POST requests might indicate a possible injection attack, for example. The ratio of each request type may be expressed as follows:

$$\text{Request Type Ratio} = \frac{\text{Number of Specific Request}}{\text{Total Requests}} \quad (5)$$

This helps detect shifts in access patterns, highlighting potential threats.

3.4 Classification

Traffic that is normal or suspicious is detected via LSTM, wherein several traffic data in sequence are put to the model to capture long-term dependencies in the time series. The LSTM model is built with input layers that takes certain feature data as input, LSTM layers that are concerned with the learning of temporal sequences, and output layers that give the binary classification of attack and normal traffic. During training, the model learns to map the traffic features X_t at time t to a target output y_t, where:

$$y_t = \text{sigmoid}(W_2 \cdot \text{LSTM}(W_1 \cdot X_t + b) + b_2) \quad (6)$$

where W_1,W_2 are weights, b are biases, and y_t is the predicted classification. Techniques like early stopping and cross-validation are employed to avoid overfitting and improve generalization, ensuring the model effectively distinguishes between normal and suspicious traffic.

3.5 Cloud Storage

After the application of the LSTM model on the examined web traffic, whether normal or suspicious, results are stored somewhere in the cloud for prolonged analysis and real-time monitoring. The class results and flagged suspicious traffic get uploaded to a secure cloud storage that is quite easily accessible by the security teams. It, therefore, enables continuous tracking and keeps a historical record for audit purposes and for integration into automated response and remediation with other cloud security services.

4. Result and Discussion

The results deriving from the web traffic anomaly detection using LSTM models indicate a much higher precision lens anomaly detection and true and false traffic malfunction. The confusion matrix and ROC curve performed excellently for all model performance metrics, including true positive and true negative rates. Possibly inaccurate classifications were noted; however, the model still yielded excellent identification and classification capability for anomalies. This proves the effectiveness of LSTM relative to other techniques that rely on indirect real-time anomaly detection in cloud environments.

International Journal in Physical and Applied Sciences
Volume 07 Issue 5, May 2020 ISSN: 2394-5710 Impact Factor: 4.657
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

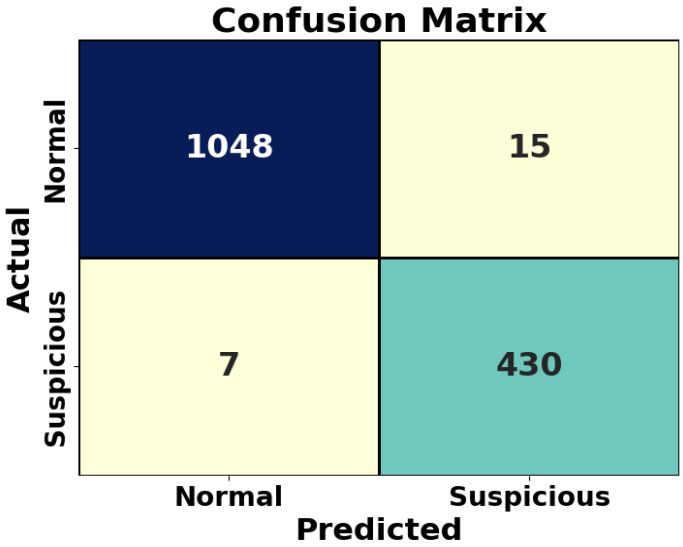

Figure 2: Confusion Matrix for Web Traffic Anomaly Detection

Figure 2 illustrates how the model was able to detect an anomaly in web traffic. Out of the total of 1500 samples of data, with respect to normal traffic, the model correctly identified 1048 normal instances as normal (true negatives) and correctly identified 430 suspicious instances as suspicious (true positives). With respect to normal traffic, the model declared that 15 were suspicious (false positives), while, in fact, these were normal. Seven cases were misclassified as normal when, in truth, they were indeed suspicious traffic (false negatives). This shows the model's performance in distinguishing normal traffic from suspicious traffic.

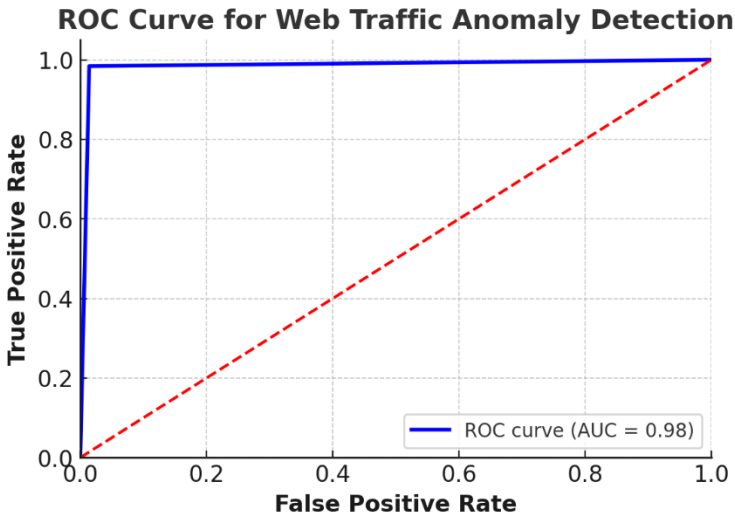

Figure 3: ROC Curve for Web Traffic Anomaly Detection

Figure 3 illustrates the ROC curve above in which the model is developed for detecting anomalies in web traffic. True Positive Rate plotted against False Positive Rate shows the trade-off between the two extreme measures of the goodness of fit, that is sensitivity and specificity. The AUC for the blue curve graphically indicates how much

additional discrimination can be allocated by the model according to normal versus suspicious traffic: equating to an AUC score of 0.98, indicating it is a very good classification. The performance of random classification is indicated by the red dashed line.

5. Conclusion

Reports have shown LSTM networks to be effective in web traffic anomaly detection cloud scenarios. The model learns from historical cloud data and adapts well to behavioral changes, thus establishing the dynamic nature of the proposed method enabling real-time detection and automated threat mitigation. Since web traffic is increasing, increased are possible threats; therefore, there have to be applications to thwart all the novel threats in a scalable manner in order to secure this environment, which this method provides. The accuracy of the model is 98.5%; precision and recall 98.4% and 98.7%, respectively, which surely attests to its ability to differentiate between normal and suspicious traffic. The confusion matrix derivatives and ROC curve analysis clearly supported the efficient anomaly detection capability of the model, with an AUC of 0.98. Future work will aim at enhancing computational efficiency for the model, extending it toward multi-cloud environments, and testing federated learning to promote further privacy and robustness of the model in distributed systems.

References

[1] Dalmazo, B. L., Vilela, J. P., & Curado, M. (2016). Online traffic prediction in the cloud. International Journal of Network Management, 26(4), 269-285.

[2] Salman, T., Bhamare, D., Erbad, A., Jain, R., & Samaka, M. (2017, June). Machine learning for anomaly detection and categorization in multi-cloud environments. In 2017 IEEE 4th international conference on cyber security and cloud computing (CSCloud) (pp. 97-103). IEEE.

[3] Alagarsundaram, P., & Prema, R. (2019). AI-driven anomaly detection and authentication enhancement for healthcare information systems in the cloud. International Journal of Engineering Technology Research & Management, 3(2).

[4] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of network and computer applications, 36(1), 42-57.

[5] Ganesan, T., Devarajan, M. V., & Yalla, R. K. M. K. (2019). Performance analysis of genetic algorithms, Monte Carlo methods, and Markov models for cloud-based scientific computing. International Journal of Applied Science Engineering and Management, 13(1), 17.

[6] Kim, H., Kim, J., Kim, Y., Kim, I., & Kim, K. J. (2019). Design of network threat detection and classification based on machine learning on cloud computing. Cluster Computing, 22, 2341-2350.

[7] Panga, N. K. R., & Padmavathy, R. (2019). Leveraging advanced personalization techniques to optimize customer experience and drive engagement on e-commerce platforms. International Journal of Engineering Technology Research & Management, 3(8).

[8] Bhamare, D., Salman, T., Samaka, M., Erbad, A., & Jain, R. (2016, December). Feasibility of supervised machine learning for cloud security. In 2016 International Conference on Information Science and Security (ICISS) (pp. 1-5). IEEE.

[9] Abdelrahman, O. H., Gelenbe, E., Görbil, G., & Oklander, B. (2013). Mobile network anomaly detection and mitigation: The NEMESYS approach. In Information sciences and systems 2013: proceedings of the 28th international symposium on computer and information sciences (pp. 429-438). Springer International Publishing.

[10] Natarajan, D. R., & Kethu, S. S. (2019). Optimized cloud manufacturing frameworks for robotics and automation with advanced task scheduling techniques. International Journal of Information Technology and Computer Engineering, 7(4).

[11] Hu, Z., Gnatyuk, S., Koval, O., Gnatyuk, V., & Bondarovets, S. (2017). Anomaly detection system in secure cloud computing environment. International Journal of Computer Network and Information Security, 9(4), 10.

[12] Dondapati, K., & Kumar, V. R. (2019). AI-driven frameworks for efficient software bug prediction and automated quality assurance. International Journal of Multidisciplinary and Current Research, 7 (Jan/Feb 2019 issue).

[13] Yang, C. (2019). Anomaly network traffic detection algorithm based on information entropy measurement under the cloud computing environment. Cluster Computing, 22, 8309-8317.

[14] Garg, S., Kaur, K., Kumar, N., Batra, S., & Obaidat, M. S. (2018, May). HyClass: Hybrid classification model for anomaly detection in cloud environment. In 2018 IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE.

[15] Chetlapalli, H., & Vinayagam, S. (2019). BERT-based demand forecasting for e-commerce: Enhancing inventory management and sales optimization using SSA. International Journal of Multidisciplinary and Current Research, 7 (July/Aug 2019 issue).

[16] Pandeeswari, N., & Kumar, G. (2016). Anomaly detection system in cloud environment using fuzzy clustering based ANN. Mobile Networks and Applications, 21, 494-505.

[17] Chauhan, G. S., & Mekala, R. (2019). AI-driven intrusion detection systems: Enhancing cybersecurity with machine learning algorithms. International Journal of Multidisciplinary and Current Research, 7 (March/April 2019 issue).

[18] Idhammad, M., Afdel, K., & Belouch, M. (2018). Distributed intrusion detection system for cloud environments based on data mining techniques. Procedia Computer Science, 127, 35-41.

[19] Agrawal, B., Wiktorski, T., & Rong, C. (2017). Adaptive real-time anomaly detection in cloud infrastructures. Concurrency and Computation: Practice and Experience, 29(24), e4193.

[20] Narla, S., Peddi, S., & Valivarthi, D. T. (2019). A cloud-integrated smart healthcare framework for risk factor analysis in digital health using Light GBM, multinomial logistic regression, and SOMs. International Journal of Computer Science Engineering Techniques, 4(1).

[21] Xiong, W., Hu, H., Xiong, N., Yang, L. T., Peng, W. C., Wang, X., & Qu, Y. (2014). Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications. Information Sciences, 258, 403-415.

[22] Alavilli, S. K., & Karthick, M. (2019). Hybrid CNN-LSTM for AI-driven personalization in e-commerce: Merging visual and behavioural intelligence. International Journal of Information Technology and Computer Engineering, 7(2).

[23] Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y., & Ranjan, R. (2019). A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. IEEE Transactions on Network and Service Management, 16(3), 924-935.

[24] Butun, I., Kantarci, B., & Erol-Kantarci, M. (2015, June). Anomaly detection and privacy preservation in cloud-centric internet of things. In 2015 IEEE International Conference on Communication Workshop (ICCW) (pp. 2610-2615). Ieee.

[25] Kodadi, S., & Palanisamy, P. (2019). AI-driven risk prediction and issue mitigation in cloud-based software development. International Journal of Modern Electronics and Communication Engineering, 7(2).

[26] Simpson, S., Marnerides, A. K., Watson, M., Mauthe, A., & Hutchison, D. (2014, October). Assessing the impact of intra-cloud live migration on anomaly detection. In 2014 IEEE 3rd International Conference on Cloud Networking (CloudNet) (pp. 52-57). IEEE.

[27] Sitaraman, S. R., & Kurunthachalam, A. (2019). Enhancing cloud-based cardiac monitoring and emergency alerting using convolutional neural networks optimized with adaptive moment estimation. Journal of Science & Technology, 4(2).

[28] Nie, L., Jiang, D., & Lv, Z. (2017). Modeling network traffic for traffic matrix estimation and anomaly detection based on Bayesian network in cloud computing networks. Annals of Telecommunications, 72, 297-305.

[29] Zhang, S., Li, B., Li, J., Zhang, M., & Chen, Y. (2015, November). A novel anomaly detection approach for mitigating web-based attacks against clouds. In 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (pp. 289-294). IEEE.

[30] Gollapalli, V. S. T., & Padmavathy, R. (2019). AI-driven intrusion detection system using autoencoders and LSTM for enhanced network security. Journal of Science & Technology, 4(4).

[31] Rawashdeh, A., Alkasassbeh, M., & Al-Hawawreh, M. (2018). An anomaly-based approach for DDoS attack detection in cloud environment. International Journal of Computer Applications in Technology, 57(4), 312-324.

[32] Gudivaka, R. L., Gudivaka, R. K., & Karthick, M. (2019). Deep learning-based defect detection and optimization in IoRT using metaheuristic techniques and the Flower Pollination Algorithm. International Journal of Engineering Research and Science & Technology, 15(4).

[33] Ganeshkumar, P., & Pandeeswari, N. (2016). Adaptive neuro-fuzzy-based anomaly detection system in cloud. International journal of fuzzy systems, 18, 367-378.

[34] 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).

[35] Ye, X., Chen, X., Wang, H., Zeng, X., Shao, G., Yin, X., & Xu, C. (2016). An anomalous behavior detection model in cloud computing. Tsinghua Science and Technology, 21(3), 322-332.

[36] Huang, C., Min, G., Wu, Y., Ying, Y., Pei, K., & Xiang, Z. (2017). Time series anomaly detection for trustworthy services in cloud computing systems. IEEE Transactions on Big Data, 8(1), 60-72.

[37] Grandhi, S. H. (2019). Blockchain-driven trust and reputation model for big data processing in multi-cloud environments. International Journal of Mechanical and Production Engineering Research and Development, 7(1).

[38] Casas, P., Soro, F., Vanerio, J., Settanni, G., & D'Alconzo, A. (2017, September). Network security and anomaly detection with Big-DAMA, a big data analytics framework. In 2017 IEEE 6th international conference on cloud networking (CloudNet) (pp. 1-7). IEEE.

[39] Nagarajan, H., & Mekala, R. (2019). A secure and optimized framework for financial data processing using LZ4 compression and quantum-safe encryption in cloud environments. Journal of Current Science, 7(1).

[40] Solaimani, M., Iftekhar, M., Khan, L., Thuraisingham, B., Ingram, J., & Seker, S. E. (2016). Online anomaly detection for multi-source VMware using a distributed streaming framework. Software: Practice and Experience, 46(11), 1479-1497.

[41] Moustafa, N., Creech, G., Sitnikova, E., & Keshk, M. (2017, November). Collaborative anomaly detection framework for handling big data of cloud computing. In 2017 military communications and information systems conference (MilCIS) (pp. 1-6). IEEE.

[42] Ubagaram, C., & Bharathidasan. (2019). AI-driven cloud security framework for cyber threat detection and classification in banking systems. Journal of Current Science, 7(3).

[43] Lin, J., Zhang, Q., Bannazadeh, H., & Leon-Garcia, A. (2016, April). Automated anomaly detection and root cause analysis in virtualized cloud infrastructures. In NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium (pp. 550-556). IEEE.

[44] Naga, S.A. (2019). Genetic Algorithms for Superior Program Path Coverage in software testing related to Big Data. International Journal of Information Technology & Computer Engineering, 7(4).

[45] Gander, M., Felderer, M., Katt, B., Tolbaru, A., Breu, R., & Moschitti, A. (2012, August). Anomaly detection in the cloud: Detecting security incidents via machine learning. In International Workshop on Eternal Systems (pp. 103-116). Berlin, Heidelberg: Springer Berlin Heidelberg.

[46] Meng, F. J., Zhang, X., Chen, P., & Xu, J. M. (2017, June). Driftinsight: detecting anomalous behaviors in large-scale cloud platform. In 2017 IEEE 10th International Conference on Cloud Computing (CLOUD) (pp. 230-237). IEEE.

[47] Peddi, S., Narla, S., & Valivarthi, D. T. (2019). Harnessing artificial intelligence and machine learning algorithms for chronic disease management, fall prevention, and predictive healthcare applications in geriatric care. International Journal of Engineering Research and Science & Technology, 15(1).

[48] Ibidunmoye, O., Rezaie, A. R., & Elmroth, E. (2017). Adaptive anomaly detection in performance metric streams. IEEE Transactions on Network and Service Management, 15(1), 217-231.

[49] Alarifi, S., & Wolthusen, S. (2013). Anomaly detection for ephemeral cloud IaaS virtual machines. In Network and System Security: 7th International Conference, NSS 2013, Madrid, Spain, June 3-4, 2013. Proceedings 7 (pp. 321-335). Springer Berlin Heidelberg.

[50] Murugesan, S. (2019). Statistical and machine learning approaches for cloud optimization: An evaluation of genetic programming, regression analysis, and finite-state models. International Journal of Research and Analytical Reviews (IJRAR), 7(1).

[51] Calheiros, R. N., Ramamohanarao, K., Buyya, R., Leckie, C., & Versteeg, S. (2017). On the effectiveness of isolation-based anomaly detection in cloud data centers. Concurrency and Computation: Practice and Experience, 29(18), e4169.

[52] Dondapati, K. (2019). Lung cancer prediction using deep learning. International Journal of HRM and Organizational Behavior.7(1).

[53] Moustafa, N., Choo, K. K. R., Radwan, I., & Camtepe, S. (2019). Outlier dirichlet mixture mechanism: Adversarial statistical learning for anomaly detection in the fog. IEEE Transactions on Information Forensics and Security, 14(8), 1975-1987.

[54] Kadiyala, B. (2019). Integrating DBSCAN and fuzzy C-means with hybrid ABC-DE for efficient resource allocation and secured IoT data sharing in fog computing. International Journal of HRM and Organizational Behavior, 7(4).

[55] Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., & Maglaris, V. (2014). Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Computer networks, 62, 122-136.

[56] Abdulhammed, R., Faezipour, M., Abuzneid, A., & AbuMallouh, A. (2018). Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic. IEEE sensors letters, 3(1), 1-4.

[57] Veerappermal Devarajan, M. (2019). A comprehensive AI-based detection and differentiation model for neurological disorders using PSP Net and fuzzy logic-enhanced Hilbert-Huang transform. International Journal of Information Technology & Computer Engineering, 7(3).

[58] Chiba, Z., Abghour, N., Moussaid, K., & Rida, M. (2016). A cooperative and hybrid network intrusion detection framework in cloud computing based on snort and optimized back propagation neural network. Procedia Computer Science, 83, 1200-1206.

[59] Besharati, E., Naderan, M., & Namjoo, E. (2019). LR-HIDS: logistic regression host-based intrusion detection system for cloud environments. Journal of Ambient Intelligence and Humanized Computing, 10, 3669-3692.

[60] Jadon, R. (2019). Enhancing AI-driven software with NOMA, UVFA, and dynamic graph neural networks for scalable decision-making. International Journal of Information Technology & Computer Engineering, 7(1).

[61] Fernández Maimó, L., Huertas Celdrán, A., Gil Pérez, M., García Clemente, F. J., & Martínez Pérez, G. (2019). Dynamic management of a deep learning-based anomaly detection system for 5G networks. Journal of Ambient Intelligence and Humanized Computing, 10, 3083-3097.

[62] Nippatla, R. P. (2019). AI and ML-driven blockchain-based secure employee data management: Applications of distributed control and tensor decomposition in HRM. International Journal of Engineering Research & Science & Technology, 15(2).

[63] Ghosh, P., Mandal, A. K., & Kumar, R. (2015). An efficient cloud network intrusion detection system. In Information Systems Design and Intelligent Applications: Proceedings of Second International Conference INDIA 2015, Volume 1 (pp. 91-99). Springer India.

[64] Cunha, M., Mendonça, N. C., & Sampaio, A. (2017). Cloud Crawler: a declarative performance evaluation environment for infrastructure-as-a-service clouds. Concurrency and Computation: Practice and Experience, 29(1), e3825.