iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67984

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

A Review on Deep Learning for Anomaly and Malicious Traffic Detection in Cloud Environments

Tilak Sharma[1], Unmukh Datta[2]
[1]*M.E Scholar*, [2]*Associate Professor, Department of Computer Science and Engineering, Maharana Pratap College of Technology, Gwalior, MP*

Abstract: ***This review paper explores the development of a deep learning-based framework aimed at improving the security of cloud computing environments by detecting anomalous and malicious traffic. The paper emphasises the requirement of real-time detection in view of the growing issues presented by sophisticated threats including distributed denial of service (DDoS) assaults, botnet traffic, and data exfiltration. Combining recurrent neural networks (RNNs) with convolutional neural networks (CNNs), models and detects traffic anomalies rather effectively. Here we derive important characteristics obtained from a large cloud traffic dataset—such as packet size, source IP, and traffic patterns—which the model subsequently employs. The study contrasts the performance of the deep learning model with traditional machine learning techniques such decision trees and support vector machines (SVMs) using evaluation metrics including accuracy, precision, recall, F1-score, and area under the curve (AUC). The deep learning-based model reveals to be superior to more conventional techniques with enhanced accuracy and recall. It is versatile enough to match shifting attack patterns with minimal training and quite sensitive to known and novel anomalies. Moreover, our method excels in identifying sometimes ignored subtle and nuanced negative behaviours by conventional models. At last, the findings suggest that deep learning offers a scalable, adaptable, and effective solution to enhance negative traffic identification in cloud systems, therefore providing a strong means of managing evolving security challenges.***

Keywords: Anomaly Detection, Malicious Traffic, Cloud Computing, Deep Learning, Cybersecurity Threats, Traffic Analysis.

I. INTRODUCTION

Cloud computing has transformed the digital world with low scalable, flexible, reasonably cost data storage and processing capability. Apart from the quick uptake of cloud technology, security issues include illegal access, data breaches, and Distributed Denial-of- Service (DDoS) attacks have become much more important. The dynamic and multi-tenant character of cloud systems aggravates these risks by making standard security solutions less effective. Within the most difficult parts of cloud security is aberrant and hostile traffic, which frequently hides itself within allowed data transfers and resists traditional detection methods[1]–[3]. To help to address this rising issue, researchers and business executives are looking more and more to new technologies—especially deep learning—which offers unparalleled chances for spotting complex trends in data. In cloud computing, an anomaly detection is the discovery of abnormalities from regular traffic patterns suggesting either system failures or cyberattacks. On the other hand, hostile traffic detection is more focused in spotting and lowering obviously harmful activities endangering data integrity, availability, and confidentiality. Although traditional methods like statistical analysis and rule-based systems have been widely applied for these goals, their enormous scope and variation sometimes make them inappropriate[4], [5]. Usually based on pre-defined rules, these traditional methods limit their flexibility to changing risks. Deep learning is useful here since it can learn complicated representations from big datasets, therefore allowing it to precisely detect subtle and expanding risks. Among deep learning models showing great potential in cloud traffic monitoring are auto encoders, CNNs, and recurrent neural networks (RNNs).

Fig.1 Anomaly and malicious Traffic Detection in Cloud Computing [6]

Since they shine in recognizing intricate temporal and spatial Network traffic patterns allow these models to be quite effective at identifying anomalies and malicious activity. RNNs could search data sequences for time-dependent anomalies; CNNs could evaluate multi-dimensional traffic data to spot harmful tendencies. Very good in anomaly detection tasks including unsupervised learning methods including auto encoders when a limited labelled dataset is involved. These methods improve their accuracy and durability by letting the models learn straight from raw traffic data, hence lowering reliance on human-defined characteristics. Applications of deep learning in cloud traffic management provide special difficulties. Particularly in real-time detection settings, the running deep learning model processing cost is a significant obstacle. Fast speed models must analyses and process data with lowest latency as massive volumes of data produced by cloud settings demand. Researchers are looking at light-weight architectures, distributed learning techniques, hardware accelerations like Graphics Processing Units (GPUs) and Tensor Processing Units (TPUs) to overcome this. Ensuring that deep learning models are interpretable presents still another really crucial difficulty. Sometimes the "black-box" character of these algorithms makes it challenging for security experts to grasp their decision-making process, therefore eroding confidence and adoption. Better openness and useful results are made possible by the growing momentum of attempts to include explainable artificial intelligence algorithms into anomaly and hostile traffic monitoring systems[7], [8]. Apart from technical hurdles, ethical and privacy issues define cloud security most importantly. Handling sensitive user data is a common component of network traffic monitoring that raises questions regarding data privacy and regulatory compliance that the Regulation on the Protection of Personal Data (GDPR) is addressing. Combining anonymizing technologies with privacy-protecting features like federated learning into deep learning-based detection systems helps to preserve ethical standards while nevertheless allowing exceptional detection accuracy in these systems[9]. These methods balance security and privacy by letting models be trained across scattered datasets without disclosing sensitive information. Deep learning included into cloud traffic monitoring could fundamentally alter the security environment and offer better tools to combat ever more sophisticated intrusions. Cloud service providers may improve their defensive systems and so guarantee a safer environment for users by using the capability of deep learning to identify anomalies and dangerous behaviors with remarkable accuracy. Advancements in hardware and software optimization along with the continuous development of deep learning architectures should assist to make these systems more accessible and efficient over time. Deep learning-based solutions will be absolutely essential in safeguarding digital ecosystems from growing hazards since cloud computing keeps getting more advanced and massive.

II. RELATED WORK

Zhao 2024 et al. investigates, with an emphasis on CNN-Focal model, the application of deep learning in network intrusion detection systems (IDs). It presents CNN-Focal, which uses threshold convolution and SoftMax multi-class classification to improve detection accuracy and efficiency, so highlighting the limits of conventional IDS in managing complex network traffic. Strong performance of the model on open datasets is confirmed by experimental data, therefore highlighting its relevance in practical network situations. shows the promise of deep learning to solve contemporary problems and opens the path for next study in this area, therefore providing a direction for increasing network security[10].

Sanjeev 2024 et al. Changing security issues and convoluted legal regulations challenge regulatory compliance for cloud computing. Machine learning (ML) provides answers when one automates compliance tasks, improves security, and raises reporting accuracy. Case studies such Microsoft Azure Sentinel and Google Cloud DLP API highlight the benefits of ML: efficiency, cost savings, better security, and more auditability. Among recently developed ML techniques with even more promise are deep and federated learning. Good compliance management requires constant monitoring, data governance programs, and model interpretability. This paper exhibits ML's transformational ability in enhancing compliance strategies and provides useful guidance on tackling evolving regulatory challenges in cloud platforms[11].

Elbakri 2024 et al. Platform for dynamic cloud computing expose data leakage, unlawful access, and evolving risk of infection. Strong adaptive cloud intrusion detection systems (CIDS) are required since the dynamic character of the cloud questions accepted security approaches. Support Vector Machine (SVM) and Pruned Exact Linear Time (PELT) approaches help ACIDs-PELT address these problems. It offers SVM classification for behavioral analysis, exact anomaly detection via PELT, and hybrid harmony search-based feature selection. By addressing imprecision in change point detection, ACIDS-PELT guarantees excellent threat detection in cloud environments by surpassing current algorithms in accuracy, precision, and recall evaluated on the NSL-KDD dataset[12].

Arjunan 2024 et al. Mass network data quantities and growing sophistication of cyberattacks make real-time network traffic anomaly detection absolutely essential. Inaccurate hand inspection drives the usage of deep learning models as LSTM and CNN for automated anomaly detection in big data systems.

Having been educated using benchmark or real-world data, these models show more accuracy and efficiency than more conventional approaches. Real-time detection in low latency large volume streaming data handling is made possible. By use of model compression and transfer learning, methods for optimization boost detection efficiency. highlights deep learning's efficiency, scalability, real-time network anomaly detecting power in demanding, high-traffic settings[13].

Mitropoulou 2024 et al. managing cloud computing systems is difficult in distributed, diverse, and dynamic character. Suggests a new approach to show cloud resources and apps using knowledge graphs, therefore facilitating efficient monitoring and administration. Graph SAGE provides vector-based representations evaluated by unsupervised machine learning methods CBLOF and Isolation Forest to identify overuse events; CBLOF performs better in this regard. Re-optimization systems ensure application performance even after discovered faults. Evaluated in a simulated environment, the method improves anomaly detection and infrastructure optimisation by means of data representation, machine learning, and proactive management techniques, therefore presenting a scalable, intelligent solution for modern cloud systems[14].

TABLE 1 LITERATURE SUMMARY

Authors/year	Model/method	Research gap	Findings
Thapa/2024 [4]	Machine learning enhances anomaly detection for cloud cybersecurity and resilience.	Limited research on deploying machine learning for dynamic cloud security.	Machine learning improves anomaly detection, enhancing cloud cybersecurity and resilience.
Thillaivanan/2024 [15]	Automated DoS detection using MFO, XGBoost, and GWO techniques	Challenges in dynamic DoS detection within distributed cloud environments	DoSD-MFOML improves DoS detection performance using feature selection and optimization
Lin/2024 [8]	Deep learning enhances anomaly detection in cloud-driven Big Data environments.	Limited research on deep learning for scalable cloud network security.	Deep learning model improves anomaly detection with high accuracy and precision.
Saleh/2023 [16]	Portable healthcare system using IoT	Limited integration of IoT with portable healthcare systems for remote monitoring.	Portable healthcare system tracks health indicators and environmental conditions.
Parameswarappa/2023 [17]	Machine learning-based anomaly detection for secure cloud environments	Limited machine learning techniques for accurate anomaly detection in cloud	Machine learning improves anomaly detection accuracy in secure cloud environments.

III. THE ROLE OF DEEP LEARNING IN TRAFFIC ANALYSIS AND DETECTION

A kind of machine learning, deep learning automatically recognises intricate patterns, hence improving network traffic analysis. It changes to fit new challenges unlike more conventional approaches and discovers concealed dangers in real-time.[18]. Deep learning strengthens security in cloud systems by means of training on vast datasets improving anomaly detection.

A. Traffic Pattern Recognition Through Deep Learning

Deep learning is quite good in identifying intricate traffic patterns in network data. CNNs and other deep models let one look at raw network traffic and spot frequent trends and deviations. This awareness covers conventional traffic patterns including user behaviour, data transfers, or cycle of requests and responses. As traffic deviates to learnt patterns, deep learning techniques can detect behaviour as aberrant. Early identification of prospective hazards, such botnet assaults or attempts to exfiltration sensitive data, made feasible with this capacity to notice both subtle and major behavioural changes improves general network security[19].

B. Feature Extraction for Enhanced Detection

As observed from a network traffic analysis, the autonomous feature extracting capacity of deep learning has great advantages. Manual feature engineering—where experts select particular properties including packet size, flow rates, or protocols—allows conventional systems to find possible security issues. Professional understanding can limit this operation and increase the time-consuming process duration. Conversely, from raw network data, deep learning techniques—especially neural networks—can, automatically, select the most relevant properties without human participation. These systems identify advanced trends including unusual packet timings, traffic surges, or conflicting protocols implying illegal activity including data exfiltration or DDoS attacks[20]. Deep learning reduces need for human input by automating feature extraction, hence enhancing detection accuracy. The obtained characteristics then enable the intrusion detection system efficiency to be improved by helping to differentiate between trustworthy and dubious signals. Network security is much enhanced by this ability to adapt and expand from data in real-time by exactly identifying new threats.

C. Anomaly Detection in Network Traffic

Usually in network traffic analysis, deep learning depends on anomaly detection. Deep learning algorithms could thus identify deviations from this baseline because educated to identify trends of regular network operation. These deviations—such as surprising traffic surges, unpredictable access times, or unusual traffic volume—may indicate possible security concerns including botnet activity, data exfiltration activity, or Distributed Denial of Service (DDoS) assaults. Learning from vast volumes of traffic data helps these algorithms to identify hitherto undetectable anomalies and assaults missed by conventional rule-based systems. Their aptitude for lifetime learning from fresh data helps them to significantly defend against increasing threats in dynamic network environments. Deep learning is thus a required tool in contemporary cybersecurity systems for real-time detection and prevention[21].

D. Malicious Traffic Detection Using Deep Learning

Deep learning is critically necessary for the detection of malicious network traffic across a wide spectrum of assaults including phishing, malware dissemination, Distributed Denial of Service (DDoS), and more generally. Big amounts of network data let deep learning systems recognize the unique traits of both legitimate and malicious traffic, thereby facilitating their correct separation between the two. These models consider numerous factors, including packet sizes, time, source IP addresses, traffic volume, to spot unusual patterns indicating of risks including botnet activity and denial-of-service attacks[22]. As these models manage growing volumes of data, they become more accurate and enable their identification of both known and novel forms of assaults. Because of its versatility and learning from changing network activity, deep learning is rather successful in tackling new difficulties. This adaptability ensures that deep learning models are absolutely essential components of contemporary cybersecurity systems since they provide continual protection against ever more sophisticated and dynamic attacks.

E. Convolutional Neural Networks for Traffic Analysis

CNNs are somewhat well-known in traffic analysis since their great capacity to detect spatial patterns in network data. CNNs can detect hierarchical patterns, hence they are highly helpful for structured traffic data analysis even if they have long been utilised for image processing chores. By means of convolutional layers, CNNs may identify many anomalies such aberrant packet distributions, anomalous traffic bursts, or atypical protocol usage, therefore implying possible security issues including DDoS attacks, malware, or botnet activity. First, the network detects low-level characteristics as packet sizes and timings first; next, it gradually combines these elements into higher-level insights revealing more intricate hierarchically ordered patterns[23].

This method helps CNNs to more precisely recognize both expected and known risks. CNNs are also appropriate for real-time traffic monitoring and the improvement of network security by recognizing recently discovered, previously undetectable attack pathways since they can effectively manage big volumes of data.

IV. TYPES OF TRAFFIC ANOMALIES AND MALICIOUS ATTACKS IN CLOUD ENVIRONMENTS

Cloud systems vary in their variations in network traffic anomalies and hostile assaults, which can damage data, disturb operations, and jeopardise security[24]. Usually observed are many basic types of traffic anomalies and hostile attacks:

A. Distributed Denial of Service (DDoS) Attacks:

DDoS (Distributed Denial of Service) attacks compromise the usual operating of services since they produce too much traffic to overwhelm a network. Attackers use the scalable and elastic character of cloud resources in cloud settings to improve the scope of their actions. DDoS assaults can bypass conventional protection systems and result in catastrophic service failures, application slowdowns, and resource exhaustion by distributing the damaging traffic over many sites. For companies, this means major downtime, lost money, and reputation harm; consequently, it is crucial to apply smart mitigating solutions in cloud systems[25].

B. Phishing Attacks:

Popular type of cybercrime is phishing, in which case sensitive data including login passwords, financial information, or personal information leaks by user or system deceit. Usually, phishing efforts in cloud systems take the shape of well-prepared emails or false websites closely matching dependable cloud services, such as email providers, cloud storage systems, or office applications. These phoney emails or websites might persuade consumers to click on dangerous links, download dangerous attachments, or update their account information. Encouragement of customers to interact with a reputable company will help them to enter sensitive information, which the aggressor then gathers for evil intent. By focussing on people who access their accounts from untested devices or networks, these assaults can also make use of cloud-based applications. It is still a major concern in cloud systems since phishing targets human weaknesses rather than technical defenses, so avoiding conventional security procedures[26].

C. Malware Propagation:

Malware—including viruses, worms, and ransomware—is a big threat in cloud systems, because it may quickly spread across linked clouds. Once malware finds its way into a cloud system, it can threaten data integrity by infecting virtual machines, programs, and databases, therefore disrupting services. Particularly dangerous are worms and viruses since they could copy and spread on their own, target various resources, and exploit holes in the cloud infrastructure. More precisely, ransomware is a type of virus that can encrypt critical data and demand a ransom for release, therefore disrupting corporate operations and maybe resulting in financial losses[27].

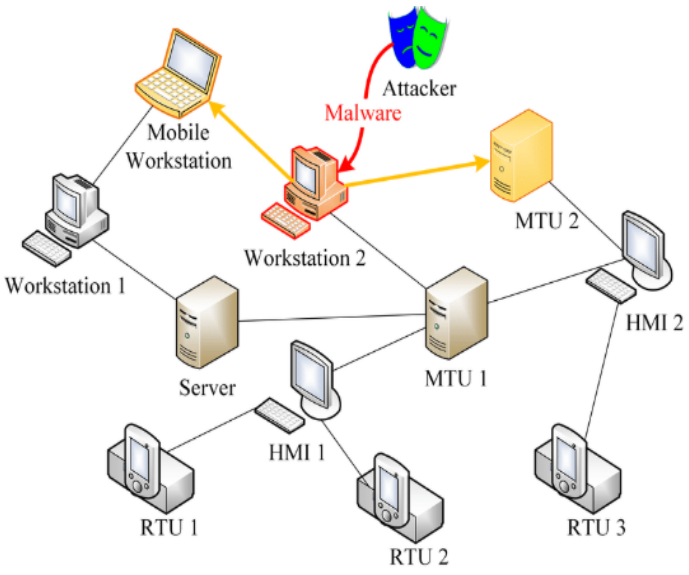


Fig. 2 Malware Propagation [28]

Malicious actors raise the potential damage by spreading malware across numerous targets using the scalability and distributed aspect of the cloud. Launching themselves via cloud services allows attackers to access many systems and individuals, thereby complicating identification and containment. Consequently, the result frequently emphasizes the need of robust cloud security defenses since it is usually notable data leakage, intellectual property theft, or full system penetration.

D. Man-in-the-Middle (MitM) Attacks:

Man-in-middle (MITM) attacks are ones whereby an adversary discreetly intercepts and maybe alters the communication between two parties, like a user and a cloud server. In cloud systems, these assaults substantially undermine the integrity and confidentiality of private data. An adversary might, for example, intercept data transferred between a user and a cloud service, therefore collecting login passwords, personal data, or business-critical information. They can also modify the sent data, therefore allowing system entry of harmful codes, unlawful access, or manipulation of cloud resources. Poor SSL/TLS installations or insecure communication channels or by way of encryption protocol flaws can all be used for MitM attacks. A successful MitM attack compromises data security, financial losses, and reputation damage since it causes data leaks, identity theft, and unlawful activities inside the cloud environment. Strong encryption, safe means of communication, and continuous monitoring are absolutely essential in preventing MitM attacks[29].

E. Data Exfiltration:

Data exfiltration is the illicit, generally hostile actor movement of private or sensitive data from cloud-based systems to outside places. Attackers routinely use advanced techniques such malware or exploit weaknesses in cloud systems, misconfigurations, or inadequate access limits to get unauthorized access to priceless data in cloud environments. Once on the system, they can silently access data—such as intellectual property, bank details, or personal information—without triggering any signals. Usually covert, the transfer can go undetectable for lengthy stretches of time and make it difficult for businesses to respond before significant damage emerges. The exfiltrated data can be sold, applied for another attack, or used for financial gain. Effective data exfiltration leads to major data leaks, intellectual property theft, compliance rule violations, financial losses, and brand damage for a company. Strong security policies are definitely required to stop such assaults and protect private data since cloud systems are getting more complex.

F. SQL Injection:

SQL injection attacks pose a serious threat to cloud-based databases since they exploit flaws in online apps interacting with databases. In a SQL injection attack, harmful SQL code is inserted into web application input fields—such as search bars or login forms. Should the application fail to properly sanitise or validate user inputs, the attacker can manipulate the SQL query given to the database, therefore providing unlawful access to confidential data. Attackers might thereby view, change, or destroy valuable information maintained in the database. SQL injections circumventing authentication mechanisms, raising access, or running arbitrary commands on the database server might cause more breach and hence compromise security. Since it can undermine data integrity, interfere with business operations, expose private client data, or let attackers access other network segments, a SQL injection attack can adversely impact a cloud environment. Prevention techniques including parameterized searches and input validation help to protect cloud databases against SQL injection risks[30].

V. DEEP LEARNING TECHNIQUES FOR ANOMALY DETECTION IN NETWORK TRAFFIC

In network traffic, anomaly detection helps to identify whether anomalies and associated hazards exist inside cloud and network settings. Since deep learning techniques can automatically extract features and identify intricate patterns in vast-scale network data, they have been ever more popular for anomaly detection[31]–[34]. There are some fundamental deep learning methods used in network traffic anomaly detection listed below:

A. Autoencoders for Anomaly Detection

Auto encoders, a form of unsupervised neural network, have great application in network traffic anomaly identification. An autoencoder picks up compression and rebuilding of input data. Applied to network traffic, it can learn a model of "normal" traffic patterns. When fresh, invisible traffic deviates from this learnt representation, reconstruction error increases signalling an anomaly. Especially effective in spotting new dangers and reducing the need for tagged data in training are auto encoders[35].

B. Convolutional Neural Networks (CNNs)

Originally meant for image processing, convolutional neural In traffic anomaly detection, networks—CNNs—have shown quite remarkable performance. CNNs are quite good in spotting spatial patterns, so they qualified to find anomalies in network traffic data. Applied to unprocessed packet data, CNNs can identify odd protocol use, aberrant packet distribution, or unexpected traffic surges. CNNs could find known and undiscovered abnormalities by knowing the spatial connections between packets and traffic patterns. This ability helps the model to recognise various likely security risks, therefore providing a strong instrument for real-time anomaly detection and network traffic analysis enhancement[36].

C. Recurrent Neural Networks (RNNs)

Especially Long Short-Term Memory (LSTM) networks, recurrent neural networks (RNNs) are rather successful for time-series data analysis including network traffic. Perfect for predicting and forecasting traffic patterns over great distances, LSTMs are especially designed to preserve long-term associations in sequential data. In traditional neural networks, LSTMs can recall data from prior time steps—a necessary capacity for temporal anomaly detection in network traffic. Understanding data flow helps RNNs identify abnormalities including odd packet sequences, abrupt traffic spikes, or changes in communication behaviour.

These anomalies could point to more severe security issues like malware spread or more odd behaviour including distributed denial of service (DDoS) assaults. Since their ability to replicate and forecast time-dependent correlations in traffic data increases their power to detect and react to growing hazards in dynamic network environments, LSTMs are a required tool in network security.

D. Generative Adversarial Networks (GANs)

By creating reasonable statistics capable of revealing Generative adversarial networks (GANs) have demonstrated to be a helpful method for anomaly detection in network traffic when straying from normal activity. Taken together, the generator and discriminator form a GAN two-Neural network. The generator generates synthetic network traffic; the discriminator finds true from false data. Under the context of network traffic, the generator learns to create traffic patterns that closely reflect every day while the discriminator finds anomalies by recognizing traffic deviating from the normal pattern. GANs have particularly useful ability to identify hitherto unidentified irregularities. The discriminator gets better at identifying anomalies that might indicate security breaches, such malware distribution or invasions as the generator adjusts to various traffic patterns[37]. In dynamic and evolving network situations where their adaptability might be sufficient instead of traditional techniques, GANs are very helpful.

E. One-Class Support Vector Machines (SVMs) with Deep Learning

A common approach for unsupervised anomaly detection particularly in cases when labelled data is limited is one-class support vector machines (SVMs). One-class SVMs provide a strong method for identifying network traffic anomalies when coupled with deep learning systems. Using deep learning networks—such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs)—this hybrid approach automatically extracts relevant features from unprocessed network traffic data. These features might mirror variations in packet size, flow rate, or communication method applied. The one-class SVM detects these features as either "normal" or "anomalous" once the deep learning model controls the raw data. The SVM is motivated by knowledge of the border separating feature space anomalies from regular traffic[38]. The capacity of deep learning to recognise intricate patterns or One-Class SVM's high anomaly detection powers together improve the accuracy and efficiency of the model in spotting fresh or past unmet network traffic irregularities.

VI. CONCLUSION

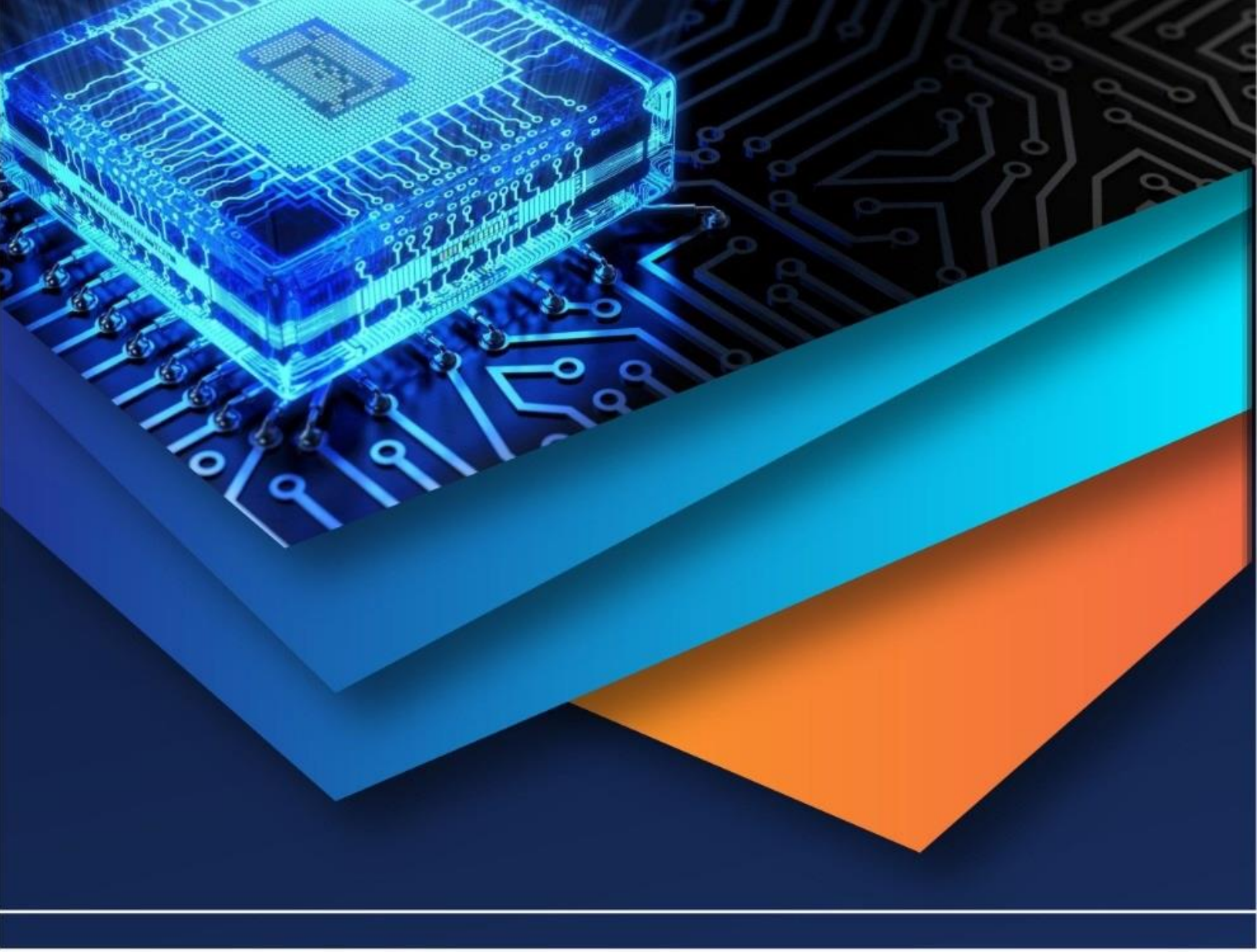
In conclusion, Deep learning for anomaly and malicious traffic identification is a significant advance in cloud computing system security. Large volumes of dynamic and changing traffic are part of conventional methods, which sometimes find it challenging to meet the scale and complexity of modern cloud setups. Deep learning models including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and auto encoders have shown incredible capacity in spotting complex patterns of destructive activity including data exfiltration, botnet activity, and distributed denial of service (DDoS) attack[39], [40]. These methods learn and adapt from large datasets without depending on hand-made feature extraction, hence they are really good in spotting heretofore unknown hazards. By learning from fresh data, deep learning methods may adapt with the cloud environment and remain current with developing cyberthreats. This is especially crucial considering the dynamic and often changing character of cloud-based systems, where attack strategies are always changing[41]. Though problems including computational costs, model interpretability, and data privacy still remain, deep learning offers tremendous benefits for cloud security.

But explainable artificial intelligence, distributed learning, and hardware acceleration are gradually fixing these issues. Including privacy-preserving methods like federated learning moving forward will assist to increase the scalability and compliance of deep learning-based detection systems even further[42]–[44]. Deep learning offers a robust and adaptable defence mechanism to protect private information and to preserve the integrity of cloud-based systems against ever more advanced cyber threats. It presents a promising future for enhancing anomaly and malicious traffic detection in cloud environments.

REFERENCES

[1] A. D. Vibhute and V. Nakum, "Deep learning-based network anomaly detection and classification in an imbalanced cloud environment," *Procedia Comput. Sci.*, vol. 232, no. 2023, pp. 1636–1645, 2024, doi: 10.1016/j.procs.2024.01.161.
[2] S. E. H. Hassan and N. Duong-Trung, "Machine Learning in Cybersecurity: Advanced Detection and Classification Techniques for Network Traffic Environments," *EAI Endorsed Trans. Ind. Networks Intell. Syst.*, vol. 11, no. 3, pp. 1–22, 2024, doi: 10.4108/eetinis.v11i3.5237.
[3] A. Abdullah and M. A. Bouke, "Towards Image-Based Network Traffic Pattern Detection for DDoS Attacks in Cloud Computing Environments: A Comparative Study," *Int. Conf. Cloud Comput. Serv. Sci. CLOSER - Proc.*, no. Closer, pp. 287–294, 2024, doi: 10.5220/0012725600003711.
[4] P. Thapa and T. Arjunan, "AI-Enhanced Cybersecurity: Machine Learning for Anomaly Detection in Cloud Computing," *Q. J. Emerg. Technol. Innov.*, vol. 9, no. 1, pp. 25–37, 2024, [Online]. Available: https://vectoral.org/index.php/QJETI/article/view/64
[5] W. H. Aljuaid and S. S. Alshamrani, "A Deep Learning Approach for Intrusion Detection Systems in Cloud Computing Environments," *Appl. Sci.*, vol. 14, no. 13, 2024, doi: 10.3390/app14135381.
[6] "Anomaly and malicious Traffic Detection in Cloud Computing - - Image Search results." https://in.images.search.yahoo.com/yhs/search;_ylt=Awr1WSy8sW9nYGEDKFjnHgx.;_ylu=Y29sbwMEcG9zAzEEdnRpZAMEc2VjA3BpdnM-?p=Anomaly+and+malicious+Traffic+Detection+in+Cloud+Computing&vm=r&type=fc_AC934C13286_s58_g_e_d022424_n9998_c999&param1=7&param2=eJwtj8lugzAQhl%2FFx0QKMB4bb9wS6ANUPTXKwRCHWKwCKqo%2Bfe20msv3LyPNtP5%2BLW7vJQVABeJ6uo1Ba61VwBgBIkceRPPnB%2FJzQORADdcARilkJlcNM5hTaqytqaklPAyTioV666bQ92PALxtomH5839ssT4Ecdj%2Fep30l40YopFCQYAhekG%2FBj8TOc%2B92V3d%2By3ImUybIoXtuQ38ive8caV3TTUfSPJdpcBllNIU4ZLUPu%2Fj%2FlXjw%2BvoyHrC65cUXgZKdS0hKASyhtKqSM1eR6NtFhFTrKvabWEZAngAmqD5AGCZMrlOU8vMXl3FZkw%3D%3D&hsimp=yhs-2461&hspart=fc&ei=UTF-8&fr=yhs-fc-2461#id=4&iurl=https%3A%2F%2Fwww.researchgate.net%2Fpublication%2F340704062%2Ffigure%2Ffig4%2FAS%3A1095915934887936%401631829812 8182%2FAnomaly-detection-process-of-cloud-computing-network.png&action=click (accessed Dec. 28, 2024).
[7] D. Sakthivel and B. Radha, "Network Traffic Analysis of Anomaly Detected Attacks Using Random Forest Algorithm in Cloud Environment," *Nat. Camp.*, vol. 28, no. 1, pp. 1–11, 2024, [Online]. Available: https://museonaturalistico.it
[8] Y. Lin, "Enhanced Detection of Anomalous Network Behavior in Cloud - Driven Big Data Systems Using Deep Learning Models," vol. 4, no. 8, pp. 1–11, 2024.
[9] Mahesh Kumar Bagwani, Anshu Gangwar, Karuna Vishwakarma, and Virendra Kumar Tiwari, "Real-time signature-based detection and prevention of DDOS attacks in cloud environments," *Int. J. Sci. Res. Arch.*, vol. 12, no. 2, pp. 2929–2935, 2024, doi: 10.30574/ijsra.2024.12.2.1608.
[10] F. Zhao, H. Li, K. Niu, J. Shi, and R. Song, "Application of deep learning-based Intrusion Detection System (IDS) in network anomaly traffic detection," *Appl. Comput. Eng.*, vol. 86, no. 1, pp. 250–256, 2024, doi: 10.54254/2755-2721/86/20241604.
[11] S. P. -, J. N. A. M. -, K. T. -, and M. D. -, "Achieving Regulatory Compliance in Cloud Computing through ML," *Adv. Int. J. Multidiscip. Res.*, vol. 2, no. 2, pp. 1–15, 2024, doi: 10.62127/aijmr.2024.v02i02.1038.
[12] W. Elbakri, M. M. Siraj, B. A. S. Al-Rimy, S. N. Qasem, and T. Al-Hadhrami, "Adaptive Cloud Intrusion Detection System Based on Pruned Exact Linear Time Technique," *Comput. Mater. Contin.*, vol. 79, no. 3, pp. 3725–3756, 2024, doi: 10.32604/cmc.2024.048105.
[13] T. Arjunan, "Real-Time Detection of Network Traffic Anomalies in Big Data Environments Using Deep Learning Models," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 12, no. 3, pp. 844–850, 2024, doi: 10.22214/ijraset.2024.58946.
[14] K. Mitropoulou, P. Kokkinos, P. Soumplis, and E. Varvarigos, "Anomaly Detection in Cloud Computing using Knowledge Graph Embedding and Machine Learning Mechanisms," *J. Grid Comput.*, vol. 22, no. 1, 2024, doi: 10.1007/s10723-023-09727-1.
[15] A. Thillaivanan, S. R. Wategaonkar, S. Duraisamy, R. Mishra, S. Nagaraj, and K. Singh, "Automated Denial of Service Detection Using Moth Flame Optimization With Machine Learning in Cloud Environment," *2023 2nd Int. Conf. Smart Technol. Syst. Next Gener. Comput. ICSTSN 2023*, no. June, pp. 1–6, 2023, doi: 10.1109/ICSTSN57873.2023.10151478.
[16] S. Saleh, B. Cherradi, O. El Gannour, N. Gouiza, and O. Bouattane, "Healthcare monitoring system for automatic database management using mobile application in IoT environment," *Bull. Electr. Eng. Informatics*, vol. 12, no. 2, pp. 1055–1068, 2023, doi: 10.11591/eei.v12i2.4282.
[17] P. Parameswarappa, T. Shah, and G. R. Lanke, "A Machine Learning-Based Approach for Anomaly Detection for Secure Cloud Computing Environments," *IDCIoT 2023 - Int. Conf. Intell. Data Commun. Technol. Internet Things, Proc.*, no. January, pp. 931–940, 2023, doi: 10.1109/IDCIoT56793.2023.10053518.
[18] K. Wang, Y. Fu, X. Duan, T. Liu, and J. Xu, "Abnormal traffic detection system in SDN based on deep learning hybrid models," *Comput. Commun.*, vol. 216, pp. 183–194, 2024, doi: 10.1016/j.comcom.2023.12.041.
[19] P. Zhong, Y. Liu, H. Zheng, and J. Zhao, "Detection of Urban Flood Inundation from Traffic Images Using Deep Learning Methods," *Water Resour. Manag.*, vol. 38, no. 1, pp. 287–301, 2024, doi: 10.1007/s11269-023-03669-9.
[20] E. Batalov *et al.*, "Ransomware Detection via Network Traffic Analysis Using Isolation Forest and LSTM Neural Networks Ransomware Detection via Network Traffic Analysis Using Isolation Forest and LSTM Neural Networks," 2024.
[21] M. Akibis *et al.*, "Measuring Ransomware Propagation Patterns via Network Tra c Analysis : An Automated Approach," 2024.
[22] F. Rustam and A. D. Jurcut, "Malicious traffic detection in multi-environment networks using novel S-DATE and PSO-D-SEM approaches," *Comput. Secur.*, vol. 136, no. August 2023, p. 103564, 2024, doi: 10.1016/j.cose.2023.103564.
[23] F. Alzonem *et al.*, "Ransomware Detection Using Convolutional Neural Networks and Isolation Forests in Network Tra c Patterns Network Tra ffi c Patterns," 2024.

[24] U. B. Clinton, N. Hoque, and K. Robindro Singh, "Classification of DDoS attack traffic on SDN network environment using deep learning," *Cybersecurity*, vol. 7, no. 1, 2024, doi: 10.1186/s42400-024-00219-7.
[25] Y. A. Abid, J. Wu, G. Xu, S. Fu, and M. Waqas, "Multilevel Deep Neural Network Approach for Enhanced Distributed Denial-of-Service Attack Detection and Classification in Software-Defined Internet of Things Networks," *IEEE Internet Things J.*, vol. 11, no. 14, pp. 24715–24725, 2024, doi: 10.1109/JIOT.2024.3376578.
[26] I. Naseer, "The role of artificial intelligence in detecting and preventing cyber and phishing attacks The role of artificial intelligence in detecting and preventing cyber and phishing attacks," no. October, 2024.
[27] A. M. Sayed Ahmed, H. M. Ahmed, T. A. Nofal, A. Darwish, and O. A. M. Omar, "Hilfer-Katugampola fractional epidemic model for malware propagation with optimal control," *Ain Shams Eng. J.*, vol. 15, no. 10, p. 102945, 2024, doi: 10.1016/j.asej.2024.102945.
[28] "Malware Propagation - - Image Search results." https://in.images.search.yahoo.com/yhs/search;_ylt=Awr1WSwAsW9nWtEBSwTnHgx.;_ylu=Y29sbwMEcG9zAzEEdnRpZAMEc2VjA3BpdnM-?p=Malware+Propagation&vm=r&type=fc_AC934C13286_s58_g_e_d022424_n9998_c999&param1=7&param2=eJwtj8lugzAQhl%2FFx0QKMB4bb9wS6ANUPTXKwRCHWKwCKqo%2Bfe20msv3LyPNtP5%2BLW7vJQVABeJ6uo1Ba61VwBgBIkceRPPnB%2FJzQORADdcARilkJlcNM5hTaqytqaklPAyTioV666bQ92PALxtomH5839ssT4Ecdj%2Fep30l40YopFCQYAhekG%2FBj8TOc%2B92V3d%2By3ImUybIoXtuQ38ive8caV3TTUfSPJdpcBllNIU4ZLUPu%2Fj%2FlXjw%2BvoyHrC65cUXgZKdS0hKASyhtKqSM1eR6NtFhFTrKvabWEZAngAmqD5AGCZMrlOU8vMXl3FZkw%3D%3D&hsimp=yhs-2461&hspart=fc&ei=UTF-8&fr=yhs-fc-2461#id=0&iurl=https%3A%2F%2Fwww.researchgate.net%2Fprofile%2FKaiming-Xiao%2Fpublication%2F343693498%2Ffigure%2Ffig2%2FAS%3A926251116150784%401597846883066%2FAn-example-of-malware-propagation-in-cyber-physical-systems-CPS.ppm&action=click (accessed Dec. 28, 2024).
[29] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks," *Int. J. Inf. Secur.*, vol. 12, no. February, 2024, doi: 10.1007/s10207-024-00899-9.
[30] S. E. Prasetyo, H. Haeruddin, and K. Ariesryo, "Website Security System from Denial of Service attacks, SQL Injection, Cross Site Scripting using Web Application Firewall," *Antivirus J. Ilm. Tek. Inform.*, vol. 18, no. 1, pp. 27–36, 2024, doi: 10.35457/antivirus.v18i1.3339.
[31] F. Zhao, M. Zhang, S. Zhou, and Q. Lou, "Detection of Network Security Traffic Anomalies Based on Machine Learning KNN Method," *J. Artif. Intell. Gen. Sci. ISSN3006-4023*, vol. 1, no. 1, pp. 209–218, 2024, doi: 10.60087/jaigs.v1i1.213.
[32] G. Almahadin *et al.*, "VANET Network Traffic Anomaly Detection Using GRU-Based Deep Learning Model," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 4548–4555, 2024, doi: 10.1109/TCE.2023.3326384.
[33] T. Ali and P. Kostakos, "HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs)," 2023, [Online]. Available: http://arxiv.org/abs/2309.16021
[34] M. Vishwakarma and N. Kesswani, "A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection," *Decis. Anal. J.*, vol. 7, no. January, p. 100233, 2023, doi: 10.1016/j.dajour.2023.100233.
[35] H. Torabi, S. L. Mirtaheri, and S. Greco, "Practical autoencoder based anomaly detection by using vector reconstruction error," *Cybersecurity*, vol. 6, no. 1, pp. 1–13, 2023, doi: 10.1186/s42400-022-00134-9.
[36] H. Liu and H. Wang, "Real-Time Anomaly Detection of Network Traffic Based on CNN," *Symmetry (Basel).*, vol. 15, no. 6, 2023, doi: 10.3390/sym15061205.
[37] Yan Lei, "Smart Network Forensics with Generative Adversarial Networks Leveraging Blockchain for Anomaly Detection and Immutable Audit Trails," *Power Syst. Technol.*, vol. 48, no. 1, pp. 1625–1642, 2024, doi: 10.52783/pst.432.
[38] R. Ghiasi, M. A. Khan, D. Sorrentino, C. Diaine, and A. Malekjafarian, "An unsupervised anomaly detection framework for onboard monitoring of railway track geometrical defects using one-class support vector machine," *Eng. Appl. Artif. Intell.*, vol. 133, no. PB, p. 108167, 2024, doi: 10.1016/j.engappai.2024.108167.
[39] S. Chakraborty, S. K. Pandey, S. Maity, and L. Dey, "Detection and Classification of Novel Attacks and Anomaly in IoT Network using Rule based Deep Learning Model," vol. 2, pp. 1–11, 2022.
[40] A. Alshammari and A. Aldribi, "Apply machine learning techniques to detect malicious network traffic in cloud computing," *J. Big Data*, vol. 8, no. 1, pp. 1–24, 2021, doi: 10.1186/s40537-021-00475-1.
[41] R. H. Hwang, M. C. Peng, C. W. Huang, P. C. Lin, and V. L. Nguyen, "An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection," *IEEE Access*, vol. 8, pp. 30387–30399, 2020, doi: 10.1109/ACCESS.2020.2973023.
[42] S. Yaqoob, A. Hussain, F. Subhan, G. Pappalardo, and M. Awais, "Deep Learning Based Anomaly Detection for Fog-Assisted IoVs Network," *IEEE Access*, vol. 11, no. January, pp. 19024–19038, 2023, doi: 10.1109/ACCESS.2023.3246660.
[43] J. P. Singh, "Mitigating Challenges in Cloud Anomaly Detection Using an Integrated Deep Neural Network-SVM Classifier Model," vol. 5, no. 1, pp. 39–49, 2022.
[44] S. I. Imtiaz *et al.*, "Efficient Approach for Anomaly Detection in Internet of Things Traffic Using Deep Learning," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/8266347.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY