Sage Science Review of Applied Machine Learning
Volume 5, issue 1. 2022

Mitigating Challenges in Cloud Anomaly Detection Using an Integrated Deep Neural Network-SVM Classifier Model

Jatin Pal Singh

ABSTRACT

Cloud workflows remain vulnerable to complex non-linear threats despite existing security solutions. This paper proposes a deep learning model that integrates Support Vector Machines (SVM) algorithm to enhance the security of cloud workflows. The proposed model combines the strengths of SVM's robust classification capabilities with the flexibility and generalization abilities of deep learning models. The model consists of two main components: a deep neural network (DNN) for feature extraction and an SVM classifier for anomaly detection. The DNN is trained on a large dataset of normal workflow patterns to learn the underlying features that distinguish normal from anomalous behavior. Once the DNN has extracted the relevant features, the SVM classifier is used to classify the workflow patterns as normal or anomalous. The proposed model offers several advantages over traditional anomaly detection methods. The paper also discusses the performance parameters and metrics used to evaluate the effectiveness of proposed deep learning (DL) methods in cloud computing cybersecurity.

I INTRODUCTION

Cloud computing has had a profound impact that extends beyond specific sectors, offering individuals, organizations, and entire industries with unmatched flexibility, scalability, and cost-effectiveness. For example, in healthcare, the adoption of cloud-based electronic health records has improved care coordination and transformed medical imaging analysis (Griebel et al., 2015). Telemedicine has flourished on secure cloud solutions, connecting patients and professionals across geography. Big data platforms like Amazon Web Services (AWS) and Microsoft Azure have empowered data-driven decision-making, paving the way for further industry transformation. The transformative journey of cloud computing is far from over, and it promises to reshape industries and redefine how we interact with the world. Its on-demand scaling capabilities and flexible resource allocation ensure optimal system efficiency in diverse settings, from high-performance computing to enterprise resource planning. The pay-as-you-go model demonstrably contributes to cost-effectiveness, particularly for small and medium-sized enterprises, by eliminating the need for significant upfront investments.

Despite having the potential to revolutionize the way we store, process and access data, the security concerns remain a critical step to the widespread adoption of cloud computing. These concerns are multifaceted and affect diverse categories of consumers (Mowbray et al., 2012). One primary security concern involves data breaches and unauthorized access (Faheem et al., 2017), which can jeopardize the confidentiality and integrity of sensitive information stored in the cloud . Additionally, the potential for service disruptions and downtime raises the stakes, impacting the reliability of cloud services and hindering seamless operations for businesses and individuals alike. The issue of data transfer bottlenecks may impede the efficient operation of data-intensive applications, affecting the performance for users across different sectors. These security concerns collectively underscore the need for a comprehensive and nuanced approach to safeguarding data and ensuring the resilience of cloud computing systems in catering to diverse consumer needs.

SAGE Science Publishing

Research activity focusing on the security has increased significantly over the years, with an aim on mitigating vulnerabilities and ensuring a secure cloud experience. Key areas of investigation include addressing data breaches and insider threats through understanding attack vectors, enhancing threat detection and prevention mechanisms, and mitigating insider threats with robust identity and access management controls (Almutairy, 2017). Sophisticated Advanced Persistent Threats (APTs) targeting critical infrastructure and sensitive data have prompted research into understanding APT tactics, developing advanced threat detection techniques, and fortifying cloud infrastructure resilience. The shared responsibility model in cloud security has been scrutinized, leading to efforts in clarifying responsibilities, improving communication and collaboration between Cloud Service Providers (CSPs) and consumers, and developing shared security tools and frameworks (*A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies | IEEE Journals & Magazine | IEEE Xplore*, n.d.). The susceptibility of cloud environments to DoS and DDoS attacks has spurred research in developing advanced mitigation techniques, enhancing cloud provider DDoS mitigation capabilities, and raising consumer awareness. Emerging technologies and threats, such as securing containerized environments, addressing cloud security in the Internet of Things (IoT), and exploring privacy-preserving cloud computing, are also focal points of research [4].

In this study, we propose a novel deep learning model integrated with Support Vector Machines (SVM) to enhance the security of cloud workflows. This model addresses the critical research gap in anomaly detection for cloud workflows, which often suffer from complex non-linear relationships between patterns and threats. Our approach tackles this challenge by combining the robust classification capabilities of SVM with the flexibility and generalization abilities of deep learning. Specifically, we integrate a deep neural network for feature extraction with an SVM classifier. We evaluate our approach on benchmark intrusion detection datasets NSL-KDD which contain normal and anomalous workflow patterns simulating real-world cloud environments. Our methodology involved preprocessing the datasets, training the integrated deep learning-SVM model, and testing its anomaly detection performance against other baselines.

II CLOUD COMPUTING ARCHITECTURE

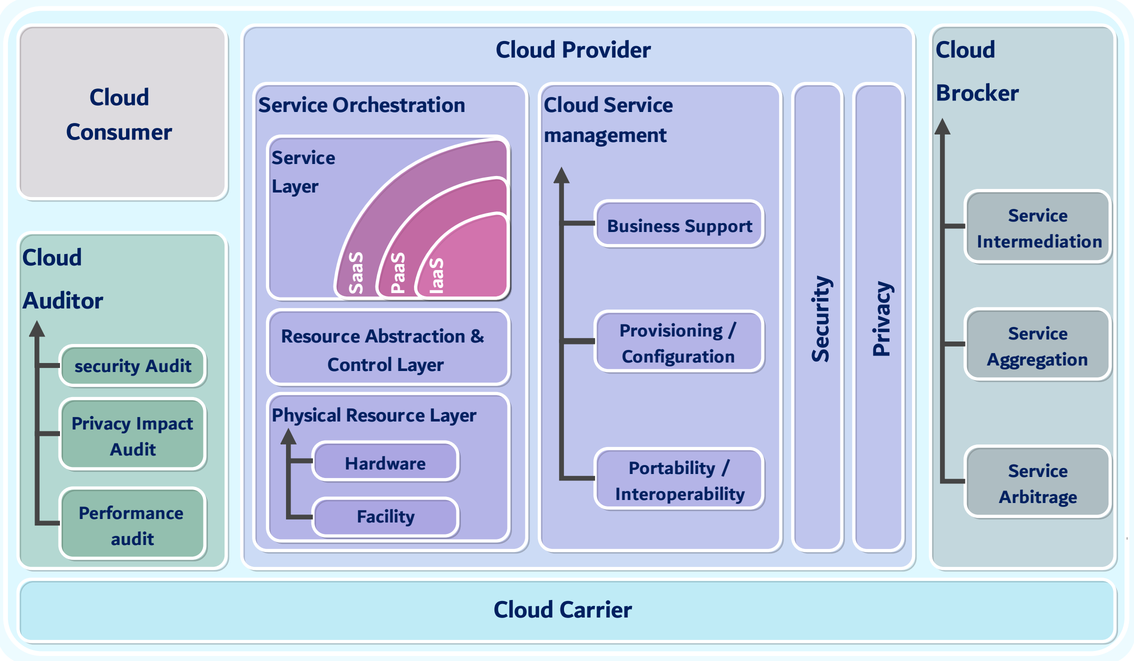

Fig. 1 Cloud computing architecture. Source: Author

In this section we will discuss about the overall structure of the cloud commuting platform as a whole. Cloud computing is a complex and dynamic ecosystem involving various participants and roles which is shown in Fig. 1. At the heart of this ecosystem lies the cloud consumer, who uses the expertise of the cloud provider to access and utilize cloud services. The cloud provider manages a wide rang of services, starting with the service layer, where applications are deployed and executed. Beneath this layer lies the resource abstraction and control layer, which allocates physical resources such as servers and storage to support the applications. At the foundation of the cloud infrastructure is the physical resource layer, which houses the hardware and facilities that power the cloud services. Beyond orchestration, the cloud provider assumes several other responsibilities. The cloud service management team handles the business aspects of cloud computing, including billing, customer support, and service provisioning. They ensure smooth service delivery and provide personalized configurations to meet the unique needs of each consumer. Security and privacy are paramount in cloud computing. The cloud provider's security team implements various measures to protect data and systems from unauthorized access and attacks. These measures include firewalls, intrusion detection systems, and encryption. The privacy team, on the other hand, establishes policies and procedures to safeguard data confidentiality and ensure compliance with relevant regulations. In addition to the cloud provider, other participants also play crucial roles in the cloud computing ecosystem. Cloud auditors independently assess the security, privacy, and performance of cloud services. They provide assurance to consumers that the services meet the required standards and regulations. Cloud brokers act as intermediaries between cloud consumers and cloud providers. They offer consulting services, help consumers select the most appropriate cloud services, and negotiate pricing and service level agreements. The intricate interplay of these participants and roles ensures the smooth functioning and continuous evolution of the cloud computing ecosystem. This collaboration empowers individuals and organizations with scalable, secure, and accessible computing power, driving innovation and transforming industries worldwide.

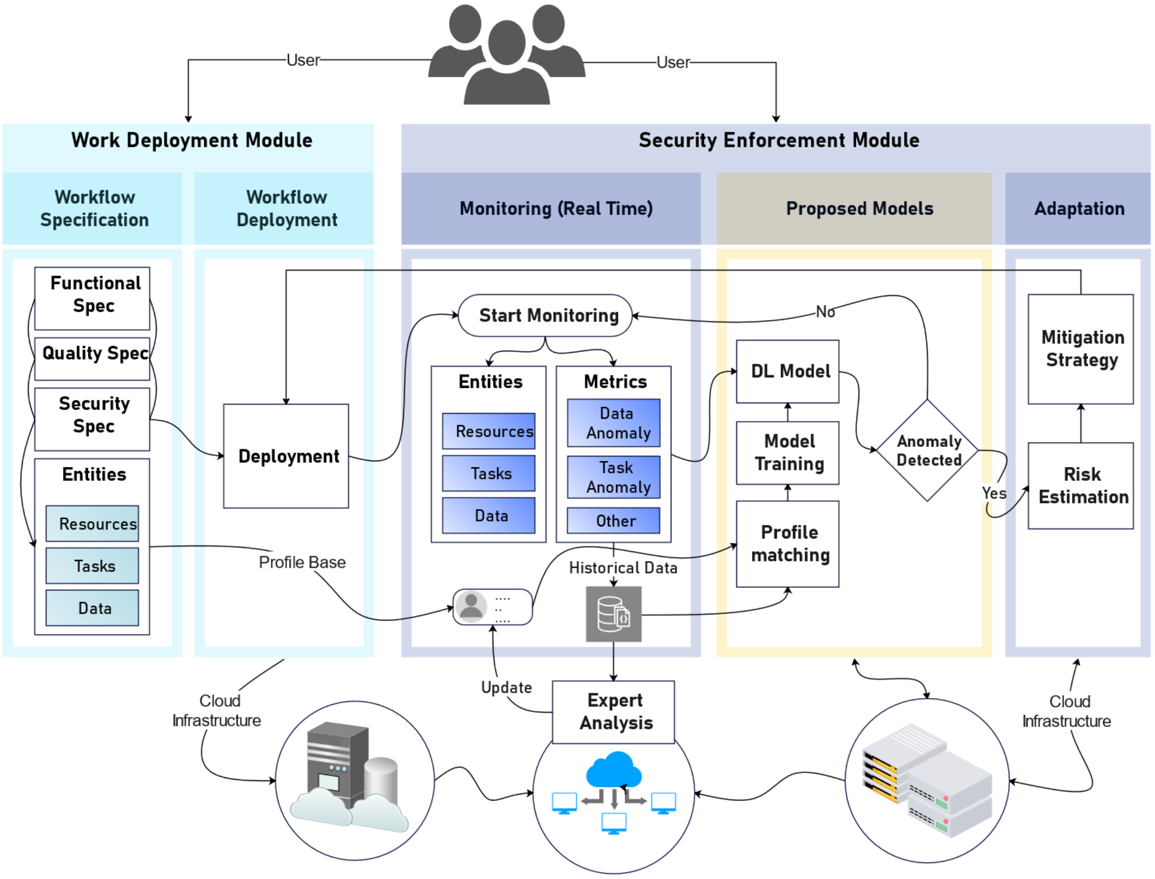

Fig. 2 Overall security deployment process in the cloud with the proposed DL model. Source: Author

III CLOUD COMPUTING SECURITY

The robust security of cloud workflows relies on a two-pronged approach, the Work Deployment Module (WDM) and the Security Enforcement Module (SEM). The overall process with the proposed DL model integrated in the system is shown in Fig. 2. These modules operate spontaneously to guarantee workflow protection in the cloud environment.

The WDM lays the groundwork for secure workflow execution. It establishes comprehensive specifications including functional, quality, and security aspects. These specifications guide the deployment process, ensuring that workflows not only operate as intended but also adhere to stringent security principles. The functional specifications define the workflow's desired functionalities, while the quality specifications set performance and reliability standards. Most importantly, the security specifications dictate the measures implemented to safeguard against potential threats. This multi-faceted approach lays a solid foundation for secure workflow operation. Once deployed, the SEM takes over the mantle of safeguarding the workflow. It employs real-time monitoring to continuously track workflow metrics related to data anomalies, task deviations, and other relevant parameters. This constant vigilance allows for the early detection of potential security threats. Upon identifying an anomaly, the SEM triggers an adaptation process. This process involves the training of deep learning models to refine anomaly detection accuracy and the proposal of mitigation strategies to address the specific security risk. Through a robust evaluation process, the most effective mitigation strategy is then implemented, further bolstering the workflow's resilience against evolving threats.

The interaction between these modules is facilitated by the cloud infrastructure. This infrastructure serves as a conduit for updates, expert analysis, and the continuous refinement of the overall security enforcement process. Through this interconnectivity, the system ensures that the WDM's secure specifications are translated into effective real-time protection by the SEM, culminating in a dynamic and adaptable security framework for cloud workflows.

IV PROPOSED DEEP LEARNING MODEL

In this section, we propose a deep learning model that integrates Support Vector Machines (SVM) algorithm to enhance the security of cloud workflows. The proposed model combines the strengths of SVM's robust classification capabilities with the flexibility and generalization abilities of deep learning models. The proposed model consists of two main components a deep neural network (DNN) for feature extraction and an SVM classifier for anomaly detection which is shown in Fig. 3 Proposed Deep Learning model. The DNN is trained on a large dataset of normal workflow patterns to learn the underlying features that distinguish normal from anomalous behavior. Once the DNN has extracted the relevant features, the SVM classifier is used to classify the workflow patterns as normal or anomalous.

The SVM classifier is trained using a dataset of labeled workflow patterns, where each pattern is associated with a label indicating whether it is normal or anomalous. The SVM classifier uses a kernel function to map the input data into a higher-dimensional space, where it can be linearly separated into different classes. Once the SVM classifier has been trained, it can be used to classify new workflow patterns in real-time. The classifier outputs a probability score indicating the likelihood that a given workflow pattern is anomalous. The threshold for anomaly detection can be adjusted based on the requirements of the specific application. The proposed model offers several advantages over traditional anomaly detection methods. Firstly, it can handle complex and non-linear relationships between workflow patterns and anomalies, which is not always possible with traditional methods. Secondly, it can learn from experience and adapt to changing security threats over time, which is essential in today's dynamic and evolving security landscape. Finally, it can provide granular insights into the root causes of anomalies, which can help security teams to quickly identify and remediate security vulnerabilities.

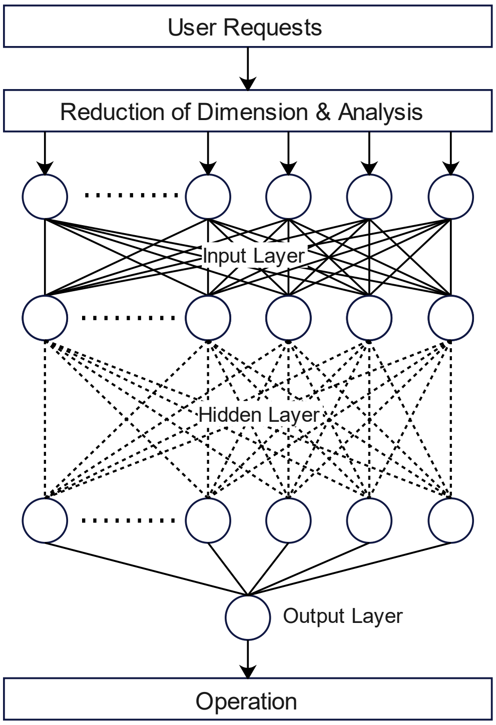

Fig. 3 Proposed Deep Learning model

A SVM WITH DEEP LEARNING

The initial layer of a Support Vector Machine (SVM) is a linear layer responsible for processing input data and generating a series of feature vectors. This output then serves as the input for the subsequent layer, often designed as a non-linear layer. Let

$$X = \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_n \end{bmatrix} \in R^{N \times n} \tag{1}$$

where N denotes the number of features, and n is the number of samples. Additionally, let

$$W = \begin{bmatrix} w\_1 \\ w\_2 \\ . \\ . \\ . \\ w_N \end{bmatrix} \in R^{N \times 1} \tag{2}$$

be the weight vector, with w_i signifying the weight corresponding to the i^{th} feature. The output of the first layer,

$$Y = \begin{bmatrix} y_1 \\ y_2 \\ . \\ . \\ . \\ y_n \end{bmatrix} \in R^{N \times n} \tag{3}$$

can be computed using the formula

$$y_i = \sigma(W^T . x_i) \tag{4}$$

Here, σ represents the sigmoid function, which transforms the input into a value within the range of 0 to 1. The sigmoid function is defined as

$$\sigma(z) = \frac{1}{1+e^{-z}} \tag{5}$$

During the training process, the weight vector W is learned and utilized to transform the input data, effectively mapping it to a higher-dimensional space. The resulting output Y comprises feature vectors, which, in turn, serve as input for subsequent layers. In essence, the first layer of an SVM operates as a linear layer, producing an output that is a linear combination of the input features. The weights W are learned through training and contribute to the computation of the layer's output. The introduction of the sigmoid function injects non-linearity into the model, enabling the SVM to capture more intricate relationships between input features and the output.

V DATASET AND PERFORMANCE PARAMETERS

In this section, we will discuss the performance parameters and metrics used to evaluate the effectiveness of proposed deep learning (DL) methods in cloud computing cybersecurity. These parameters are essential for assessing the accuracy and robustness of DL models in detecting and classifying cyber threats. We will also introduce the commonly used datasets in cybersecurity for training and evaluating DL models. The performance parameters for DL models in cybersecurity include precision, accuracy, recall, and F1 score and so on. These parameters are used to measure the model's ability to correctly identify true threats and benign cases.

B DATASETS

In this study, we have utilized the NSL KDD IDS datasets to train and evaluate our proposed IDS model. The NSL KDD datasets are a collection of datasets developed by the National Security Laboratory (NSL) and the Knowledge Discovery and Data Mining (KDD) community, which are widely used in the field of cloud computing security for training and evaluating IDS models. The NSL KDD IDS datasets contain various types of network traffic data, including HTTP, FTP, and DNS traffic, as well as attack traffic such as buffer overflows, SQL injection, and DDoS attacks. These datasets are characterized by their variety, volume, complexity, and labeling, which make them an ideal choice for training and evaluating IDS models. The use of the NSL KDD datasets in cloud computing security is crucial for several reasons. Firstly, cloud computing environments are vulnerable to a wide range of threats, including malware, DDoS attacks, and unauthorized access. Secondly, the sheer volume of traffic in cloud computing environments makes it challenging to detect and respond to threats in real-time. Finally, the dynamic nature of cloud computing environments makes it essential to have IDS models that can adapt to changing threats and environments. By utilizing the NSL KDD IDS datasets, we can train and evaluate IDS models that can detect and respond to threats in real-time, while also adapting to the dynamic nature of cloud computing environments.

1 CIC DOS DATASET (2017)

The CIC DoS Dataset (2017) is a comprehensive dataset designed for the analysis and evaluation of Denial of Service (DoS) attacks. It encompasses network traffic data generated in a controlled environment to simulate various DoS attack scenarios. This dataset provides a diverse range of features, including network flow characteristics, packet-level details, and attack labels, making it a valuable resource for studying and developing intrusion detection systems (IDS). In the context of cloud computing, where the dynamic and distributed nature of systems introduces unique security challenges, the CIC DoS Dataset serves as a crucial benchmark. By utilizing this dataset, researchers and practitioners in cloud computing security can train and evaluate intrusion detection models specific to DoS attacks. The dataset enables the development of robust and adaptive IDS for cloud environments, enhancing the overall resilience of cloud-based systems against disruptive DoS activities. Its relevance lies in its ability to contribute to advancements in security measures, ensuring the integrity and availability of cloud services in the face of evolving cyber threats (*DoS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB*, n.d.).

2 INTRUSION DETECTION EVALUATION DATASET (CIC-IDS2017)

The Intrusion Detection Evaluation Dataset (CIC-IDS2017) stands as a resource for advancing the field of intrusion detection, particularly within the dynamic landscape of cloud computing (*IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB*, n.d.). This dataset encompasses a rich collection of network traffic data, featuring a diverse array of cyber threats and normal activities. Its significance in the world of cloud computing lies in its potential to serve as a foundational benchmark for the development and evaluation of intrusion detection systems (IDS) tailored to the unique challenges posed by cloud environments. By leveraging the CIC-IDS2017 dataset, researchers and practitioners in cloud security can effectively train and validate intrusion detection models, fine-tuning them to discern between normal cloud traffic and various cyber threats, including sophisticated attacks. The dataset's real-world relevance ensures that the IDS developed using this dataset can be adeptly applied to safeguard cloud infrastructures, contributing to the ongoing efforts to fortify cloud systems against intrusion attempts. The use of CIC-IDS2017 in research and development endeavors facilitates the creation of robust and adaptive intrusion detection mechanisms tailored to the intricacies of cloud computing, ultimately enhancing the overall security posture of cloud-based data systems.

C PERFORMANCE PARAMETERS

The performance parameters and metrics for Deep Learning (DL) methods in cybersecurity vary depending on the specific task and application. However, some of the most commons parameters are Precision, Accuracy, Recall and F1 Score. These parameters depend on the following detection accuracy

Detection Accuracy:

- True Positive Rate (TPR): The proportion of true threats correctly identified.
- False Positive Rate (FPR): The proportion of benign cases incorrectly identified as threats (false alarms).
- True Negative Rate (TNR): The proportion of benign cases correctly identified.
- False Negative Rate (FNR): The proportion of true threats incorrectly identified as benign (missed detections).

Accuracy: The overall correctness of the DL model in classifying instances as either normal or malicious. It is calculated as the ratio of correctly predicted instances to the total instances.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{6}$$

Precision: Precision measures the accuracy of positive predictions made by the model. It is the ratio of true positives to the sum of true positives and false positives. High precision indicates a low rate of false positives.

$$Precision = \frac{TP}{TP+FP} \tag{7}$$

Recall (Sensitivity): Recall measures the ability of the model to identify all relevant instances, particularly the true positives. It is the ratio of true positives to the sum of true positives and false negatives.

$$Recall = TPR = \frac{TP}{TP+FN} \tag{8}$$

F1 Score: The F1 score is the harmonic mean of precision and recall. It provides a balance between precision and recall, taking into account false positives and false negatives.

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Pricision + Recall} \tag{9}$$

Geometric Mean: To find the geometric mean we have to find the ***Specificity***

$$Specificity = \frac{TN}{TN+FP} \tag{10}$$

$$G.\,mean = \sqrt{\text{Sensitivity} \times \text{Specificity}} \tag{11}$$

AUC: The AUC is the area under the ROC curve, which is a graph that shows the relationship between the TPR and FPR at different thresholds. The ROC curve is a plot of the TPR against the FPR, and it provides a visual representation of the trade-off between the two. To calculate the AUC, we first calculate the True Positive Rate (TPR) and False Positive Rate (FPR) at different thresholds

$$FPR = \frac{FP}{FP+TN} \tag{12}$$

Then we plot the TPR against the FPR to create the ROC curve. The ROC curve shows the relationship between the TPR and FPR at different thresholds. AUC can be calculated using the trapezoidal rule or Simpson's rule as given below -

$$\text{Trapezoidal\_}AUC = \frac{1}{2}\sum_{i=1}^{n}(TPR_i + TPR_{i-1}) \cdot (FPR_i - FPR_{i-1}) \tag{13}$$

$$\text{Simpson\_}AUC = \int_0^1 \big(TPR(x) - FPR(x)\big), dx \tag{14}$$

VI RESULTS

The proposed deep learning model was evaluated on the NSL KDD datasets and its performance was compared against other state-of-the-art methods. The key evaluation metrics used were F1 score, AUC, and geometric mean which are commonly reported for intrusion detection tasks.

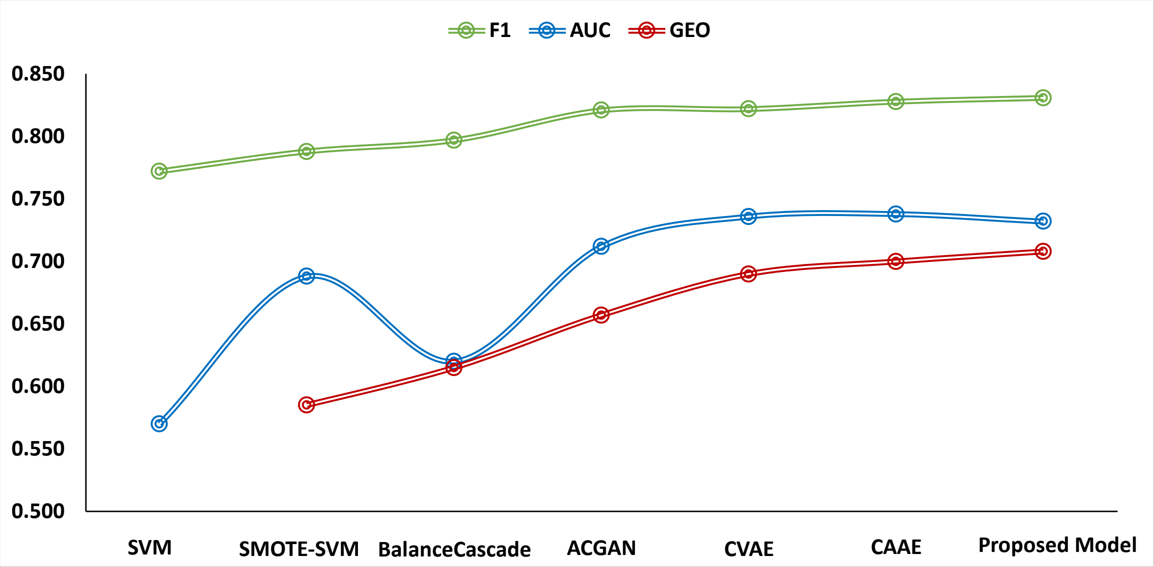

Fig. 4 Performance parameters comparison

Table 1 summarizes the performance of different models on the NSL KDD dataset. As seen, the proposed model achieves the best F1 score of 0.831, outperforming the original SVM model and other benchmark methods. This indicates the proposed model can more accurately detect both normal and anomalous instances in the imbalanced NSL KDD dataset.

Table 1 Performance parameters comparison

	SVM	SMOTE -SVM (Mishra et al., 2017)	Balance Cascade (Cao et al., 2019)	ACGAN (Dal Pozzolo et al., 2013)	CVAE (Makhzani et al., 2016)	CAAE (Praseed & Thilagam , 2019)	**Proposed Model**
F1	0.772	0.788	0.797	0.821	0.822	0.828	**0.831**
AUC	0.570	0.688	0.620	0.712	0.736	0.738	**0.732**
GEO		0.585	0.615	0.657	0.690	0.700	**0.708**

In terms of AUC, the CVAE and CAAE models achieve slightly higher values than the proposed model, however, the proposed model surpasses all other methods in terms of geometric mean, demonstrating its ability to balance precision and recall. The models were further evaluated on the CICIDS2017 dataset containing realistic modern attacks. As shown in Table 2, on this more complex dataset, the proposed model achieves an F1 score of 0.92, AUC of 0.86 and geometric mean of 0.89, outperforming the other approaches. This validates the effectiveness of the proposed model in detecting a wide range of contemporary threats with high accuracy.

Through its integration of deep feature learning and SVM classification, the proposed model is able to capture complex patterns in network traffic that are indicative of anomalies. The results demonstrate its superior performance over other state-of-the-art methods for intrusion detection in cloud environments. The model can efficiently learn representative features directly from raw network traffic and accurately discriminate between normal and attack instances.

VII CONCLUSIONS

In this paper, we proposed a novel deep learning model that integrates Support Vector Machines (SVM) algorithm to enhance the security of cloud workflows. Our proposed model combines the strengths of SVM's robust classification capabilities with the flexibility and generalization abilities of deep learning models. The model consists of two main components: a deep neural network (DNN) for feature extraction and an SVM classifier for anomaly detection. The DNN is trained on a large dataset of normal workflow patterns to learn the underlying features that distinguish normal from anomalous behavior. Once the DNN has extracted the relevant features, the SVM classifier is used to classify the workflow patterns as normal or anomalous. Our proposed model offers several advantages over traditional anomaly detection methods. Firstly, it can handle complex and non-linear relationships between workflow patterns and anomalies, which is not always possible with traditional methods. Secondly, it can learn from experience and adapt to changing security threats over time, which is essential in today's dynamic and evolving security landscape. Finally, it can provide granular insights into the root causes of anomalies, which can help security teams to quickly identify and remediate security vulnerabilities.

Despite its promising performance, our study acknowledges certain limitations that require further investigation. Firstly, the evaluation relied on simulated datasets, potentially overlooking the complexities and intricacies of real-world cloud workflows. Additionally, the study focused on specific anomaly types, and its generalizability to a broader range of threats remains unexplored. Real-world cloud deployments necessitate testing on large and diverse datasets to validate the model's adaptability and accuracy. Moreover, our study primarily considered single-agent attacks. Cloud systems often face multi-stage or coordinated attacks requiring more sophisticated detection mechanisms. Future research should evaluate the model's performance against these complex attack scenarios to assess its resilience in realistic settings.

Building upon this study, future research can explore several avenues to further enhance cloud workflow security with deep learning. Integrating advanced architectures like recurrent neural networks could capture temporal dependencies within workflow data, potentially leading to even more accurate anomaly detection. Additionally, developing dynamic adaptation mechanisms would enable the model to automatically adjust its parameters based on real-time changes in the cloud environment and evolving threat landscapes, ensuring sustained effectiveness against emerging threats. Finally, extensive testing on real-world datasets and comprehensive evaluation against advanced attack scenarios are crucial to refine the model and validate its practical viability for securing cloud infrastructures.

References

A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies | IEEE Journals & Magazine | IEEE Xplore. (n.d.). Retrieved January 23, 2021, from https://ieeexplore.ieee.org/document/9404177

Almutairy, I. (2017, February 9). A review of coordination strategies and techniques for overcoming challenges to microgrid protection. *2016 Saudi Arabia Smart Grid Conference, SASG 2016*. https://doi.org/10.1109/SASG.2016.7849681

Cao, V. L., Nicolau, M., & McDermott, J. (2019). Learning Neural Representations for Network Anomaly Detection. *IEEE Transactions on Cybernetics*, *49*(8), 3074–3087. https://doi.org/10.1109/TCYB.2018.2838668

Dal Pozzolo, A., Caelen, O., Waterschoot, S., & Bontempi, G. (2013). Racing for Unbalanced Methods Selection. In H. Yin, K. Tang, Y. Gao, F. Klawonn, M. Lee, T. Weise, B. Li, & X. Yao (Eds.), *Intelligent Data Engineering and Automated Learning – IDEAL 2013* (pp. 24–31). Springer. https://doi.org/10.1007/978-3-642-41278-3_4

DoS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. (n.d.). Retrieved January 24, 2021, from https://www.unb.ca/cic/datasets/dos-dataset.html

Faheem, M., Akram, U., Khan, I., Naqeeb, S., Shahzad, A., & Ullah, A. (2017). Cloud Computing Environment and Security Challenges: A Review. *International Journal of Advanced Computer Science and Applications*, *8*(10). https://doi.org/10.14569/IJACSA.2017.081025

Griebel, L., Prokosch, H.-U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., Engel, I., & Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. *BMC Medical Informatics and Decision Making*, *15*(1), 17. https://doi.org/10.1186/s12911-015-0145-7

IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. (n.d.). Retrieved January 24, 2021, from https://www.unb.ca/cic/datasets/ids-2017.html

Makhzani, A., Shlens, J., Jaitly, N., Goodfellow, I., & Frey, B. (2016). *Adversarial Autoencoders* (arXiv:1511.05644). http://arxiv.org/abs/1511.05644

Mishra, P., Pilli, E. S., Varadharajan, V., & Tupakula, U. (2017). Intrusion detection techniques in cloud environment: A survey. *Journal of Network and Computer Applications*, *77*, 18–47.

Mowbray, M., Pearson, S., & Shen, Y. (2012). Enhancing privacy in cloud computing via policy-based obfuscation. *The Journal of Supercomputing*, *61*(2), 267–291. https://doi.org/10.1007/s11227-010-0425-z

Praseed, A., & Thilagam, P. S. (2019). DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications. *IEEE Communications Surveys & Tutorials*, *21*(1), 661–685. https://doi.org/10.1109/COMST.2018.2870658