VECTORAL PUBLISHING

Research Article: Quarterly Journal of Emerging Technologies and Innovations Volume: 09

AI-Enhanced Cybersecurity: Machine Learning for Anomaly Detection in Cloud Computing

Priya Thapa

Department of Information Technology, Mid-Western University, Nepal
priya.thapa@mwubire.edu.np

Tamilselvan Arjunan

arjunantamilselvan1@gmail.com

Abstract

Cloud computing has become ubiquitous, providing convenient on-demand access to computing resources. However, security remains a major concern, as cloud environments are increasingly targeted by cyber-attacks. Here, we review the use of machine learning techniques for anomaly detection to enhance cybersecurity in cloud computing. We provide background on cloud computing architectures, cyber threats, and anomaly detection. We then comprehensively survey state-of-the-art machine learning methods for anomaly detection in cloud environments, including supervised, unsupervised, and hybrid approaches. Specific techniques covered include neural networks, support vector machines, clustering, and ensemble methods. We analyze the strengths and limitations of these techniques, and provide recommendations for selecting appropriate algorithms based on factors like labeled data availability and detection goals. Challenges and open research questions in deploying machine learning for cloud security are discussed. We argue that AI-enhanced anomaly detection has excellent potential to identify novel attack patterns and improve resilience against continually evolving threats. Our analysis aims to provide guidance for researchers and practitioners developing the next generation of intelligent cyber defense systems.

Keywords: *Cloud Computing, Cybersecurity, Anomaly Detection, Machine Learning, Threat Monitoring, Attack Patterns*

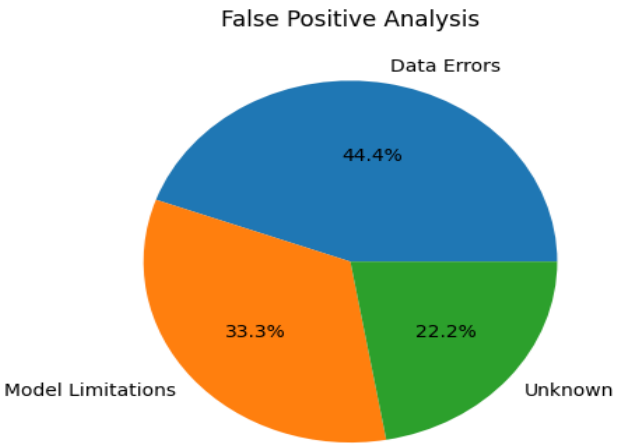
Introduction

Cloud computing has profoundly reshaped the landscape of computing resource utilization and management. Through its provision of convenient on-demand access to shared pools of configurable resources, cloud computing facilitates the delivery of services over the internet with characteristics such as rapid elasticity and measured service, as outlined by Mell and Grance in 2011. This paradigm shift has allowed organizations to adopt a more flexible approach to resource allocation, enabling them to scale their infrastructure up or down in response to changing demands [1]. Furthermore, the prevalent pay-as-you-go pricing model prevalent in cloud services has empowered organizations to procure computing capabilities without the need

for significant upfront infrastructure investments. Consequently, many enterprises are now in the process of migrating their critical business systems and sensitive data to both public and private cloud environments, drawn by the promise of enhanced flexibility, scalability, and cost-efficiency. It's notable that the global public cloud services market, as projected by Gartner in 2021, is poised for substantial growth, with forecasts indicating a 17% increase to reach $266 billion in 2022. This exponential growth underscores the widespread adoption and increasing importance of cloud computing in modern business operations and IT strategies [2].

Despite the numerous benefits of cloud adoption, security concerns persist as a significant obstacle. The consolidation of valuable data and workloads within centralized virtualized resources in cloud environments presents an attractive target for cybercriminals [3]. The delegation of infrastructure management to external providers results in a loss of direct control and visibility over security measures. The Cloud Security Alliance (CSA) has outlined several major threats to cloud computing, including data breaches, data loss, account hijacking, malicious insiders, abuse of cloud services, and vulnerabilities in shared technologies (CSA, 2017). These threats underscore the importance of robust security measures and vigilance in cloud environments. Notably, high-profile incidents such as the leakage of celebrity photos from Apple iCloud in 2014 and the exposure of sensitive US government employee records from Office of Personnel Management networks in 2015 serve as stark reminders of the potential risks associated with cloud-based services [4]. Such breaches highlight the critical need for organizations to prioritize security protocols and implement comprehensive risk mitigation strategies when embracing cloud technologies [5].
Anomaly detection serves as a foundational technique in bolstering cybersecurity efforts by leveraging algorithms to discern deviations from established norms [6]. This methodology is instrumental in pinpointing irregularities in activities and system functionalities, thereby furnishing timely alerts regarding potential security breaches. The significance of automated anomaly detection is particularly pronounced in cloud infrastructures, characterized by their vast and dynamic datasets, which render traditional manual inspection approaches impractical. Through the application of machine learning algorithms, organizations can efficiently sift through the immense volume of data generated within cloud environments to identify aberrant patterns indicative of malicious activities, thus fortifying their defenses against cyber threats.

This paper comprehensively surveys state-of-the-art machine learning techniques for anomaly detection designed to improve cybersecurity in cloud computing environments. We first provide background on cloud computing architectures, cyber threats in the cloud, and principles of anomaly detection. Next, we taxonomize and review supervised, unsupervised, and hybrid machine learning approaches for cloud anomaly detection proposed in recent literature [7]. Specific algorithms evaluated include neural networks, support vector machines, clustering, ensemble models, and more. We analyze the strengths and weaknesses of these techniques under various data conditions. Key considerations in selecting appropriate anomaly detection algorithms are discussed [8]. We also surface open challenges and opportunities for advancing machine learning cyber defense in cloud environments. Our survey aims to assess the current landscape of AI-enhanced anomaly detection for cloud security and chart promising directions for future research and deployment. The next wave of intelligent systems leveraging machine learning has excellent potential to identify novel attack patterns, enhance threat monitoring, and improve cloud resilience against the rapid evolution of cyber threats.



Background

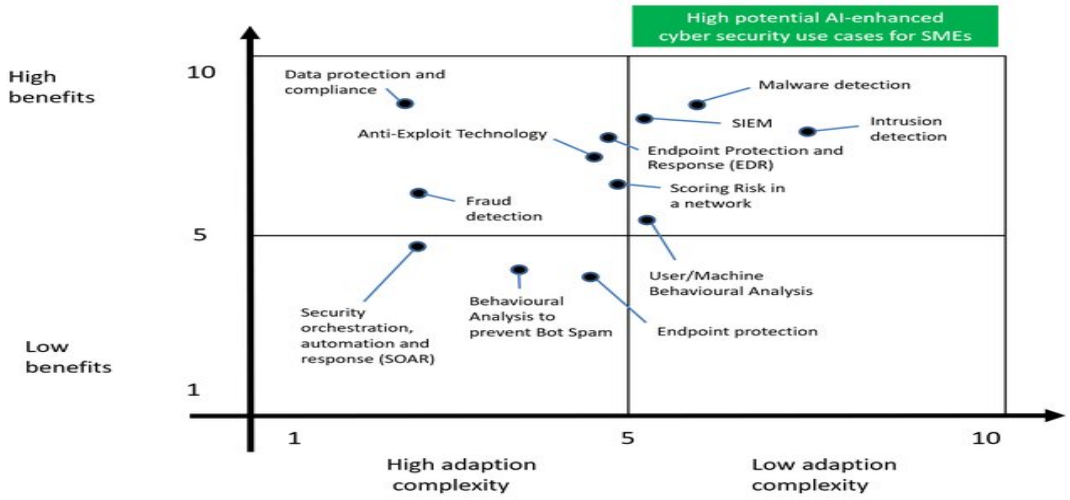
In this section, we provide background on cloud computing deployments, cyber threats in cloud environments, and principles of anomaly detection systems. This establishes essential context for surveying machine learning techniques for cloud anomaly detection [9].

Cloud Computing Architectures: Cloud computing architectures represent a transformative approach to delivering computing resources, characterized by shared pools of on-demand, dynamically configurable resources accessible via the internet [10]. This paradigmatic shift enables organizations to access hardware, software, and services without the burdensome upfront costs associated with traditional infrastructure, facilitating scalability and operational agility while emphasizing operational expenditures over capital investments. Underpinning this model are vast data centers managed by cloud providers, housing extensive networks of servers and supporting infrastructure, which customers can rapidly provision through self-service interfaces, streamlining resource allocation and deployment [11].

The landscape of cloud computing is delineated by three primary service models, as delineated by Mell and Grance (2011). Infrastructure as a Service (IaaS) furnishes fundamental computing resources such as processing, storage, and networks on-demand, affording customers the flexibility to deploy and manage their operating systems and applications atop the provided infrastructure. Platform as a Service (PaaS) extends this capability by furnishing development, deployment, and management tools as services, empowering customers to craft custom applications while retaining control over deployment and configuration [12]. Meanwhile, Software as a Service (SaaS) delivers applications hosted in the cloud, accessible on-demand via web browsers or program interfaces, freeing customers from the burden of managing underlying infrastructure [13].

Beyond service models, cloud deployments manifest in various configurations, including public, private, hybrid, and multi-cloud architectures (CSA, 2017). Public clouds enable dynamic provisioning of services over the open internet, facilitated by web applications and APIs, catering to diverse organizational needs. Conversely, private clouds confine cloud functionality to a single organization's internal infrastructure, providing enhanced control and security. Hybrid clouds amalgamate elements of public and private cloud infrastructure, offering flexibility and scalability tailored to specific requirements. Finally, multi-cloud architectures harness the strengths of multiple public and/or private clouds, leveraging diverse service offerings and mitigating reliance on any single provider for enhanced resilience and performance optimization.

Figure 1. Recommended AI-enhanced cyber security [14]



Threat Landscape in Cloud Computing: Cloud computing, while offering unparalleled agility and scalability, introduces a plethora of cybersecurity risks that must be diligently addressed [15]. The consolidation of critical data, workloads, and infrastructure into centralized pools of resources creates enticing targets for malicious actors (Ahmed & Abraham, 2013). Moreover, compared to traditional internal data centers, cloud architectures often reduce visibility and control, complicating security efforts. Dependence on cloud vendors further exacerbates risks, as shared technologies and multitenancy introduce vulnerabilities such as side channel attacks between virtual machines [16].

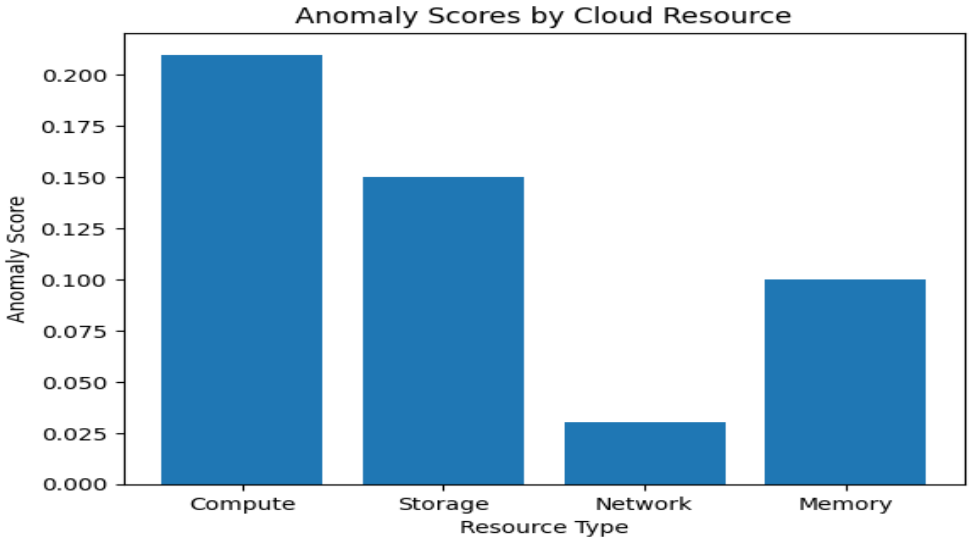
The Cloud Security Alliance (CSA, 2017) identifies several top threats in cloud computing, including data breaches, which can stem from misconfigurations, application vulnerabilities, or insider threats. Data loss poses another significant risk, potentially resulting from account termination, service outages, bugs, or accidental deletion, especially problematic without adequate backups. Account hijacking, facilitated by phishing, weak credentials, or flaws in multi-factor authentication, remains a persistent concern. Additionally, the threat of malicious insiders, including cloud provider employees with privileged access, underscores the importance of robust access controls and monitoring mechanisms.

Abuse of cloud services presents another challenge, with adversaries leveraging cloud resources for various nefarious activities such as launching denial of service attacks or hosting malicious payloads. Insufficient due diligence before migrating to the cloud can leave organizations vulnerable, highlighting the critical need for comprehensive risk assessment and validation of security controls. Shared technologies vulnerabilities further compound risks, as vulnerabilities in shared infrastructure, platforms, or applications could enable lateral movement between tenants, amplifying the potential impact of breaches.

Furthermore, the dynamic and automated nature of cloud environments complicates threat detection, requiring advanced analytics to sift through the scale and diversity of cloud data effectively. As threats evolve, so too must security measures, with adversaries continually innovating new attack methods. Anomaly detection using machine learning shows promise in addressing these challenges by providing adaptive security capabilities to bolster cloud defenses [17]. In summary, mitigating the diverse and evolving threats in cloud computing demands a multi-layered approach encompassing robust security controls, ongoing risk assessment, and advanced threat detection technologies.

Anomaly Detection Systems: Anomaly detection, also known as outlier detection, identifies data points that are unusual when compared to the majority of observations (Chandola et al., 2009). By detecting anomalous events, system states, or patterns in data, these techniques can identify potential threats and vulnerabilities. Anomaly detection is widely used for cybersecurity monitoring as malicious activity often differs from normal behavior.

Anomaly detection systems model expected normal behavior, which is also referred to as a baseline, profile, or pattern of life. Data points that deviate from the model are flagged as anomalies. A key advantage of anomaly detection is the ability to detect previously unknown threats without prior examples of attack patterns, as only a profile of normal activity is needed. Additionally, anomaly detection can identify insider threats through behavioral monitoring [18]. However, anomaly detection also faces challenges [19]. Defining normal behavior requires sufficient baseline data, which may not be available when systems or workloads are rapidly changing. Anomaly detection can suffer from false positives if the normal behavior model is inaccurate. Tuning systems to balance the tradeoff between false positives and false negatives can be difficult. Despite these limitations, anomaly detection provides value for identifying novel and emerging threats. Next we survey machine learning techniques for enhancing anomaly detection in cloud environments.



Machine Learning for Anomaly Detection in Cloud Computing

A wide range of machine learning techniques have been applied for anomaly detection in cloud computing environments. Machine learning algorithms analyze large volumes of diverse cloud data to model normal behavior, identify anomalies, and detect potential attacks. We categorize approaches as supervised, unsupervised, or hybrid based on whether models are trained using labeled examples of anomalies.

Supervised Anomaly Detection: Supervised anomaly detection techniques learn classification models using datasets containing labeled examples of normal and anomalous data points . The trained models can then classify new unseen data points as either normal or anomalous. Supervised techniques have the advantage of directly modeling the detection objective using examples of anomalies. However, gathering sufficient labeled anomaly data can be challenging, as anomalies are often rare in practice. Researchers have developed cloud anomaly detection systems using different supervised algorithms:

Neural Networks: Artificial neural networks, a cornerstone in machine learning, have found widespread application in anomaly detection tasks due to their ability to discern complex patterns. One prevalent approach involves utilizing feedforward neural networks with backpropagation, enabling nonlinear classification to differentiate between normal and anomalous data points. For instance, in the realm of cloud data center network traffic analysis, researchers have proposed the use of Recurrent Neural Network (RNN) architecture with Long Short-Term Memory (LSTM) cells . This sophisticated deep learning model is adept at discerning anomalous traffic patterns such as Distributed Denial of Service (DDoS) attacks by leveraging extracted multivariate time series features. Notably, on a dataset representative of cloud network traffic, the RNN-LSTM model achieved remarkable accuracy, surpassing 99% in distinguishing between attack and non-attack traffic instances [20].
Furthermore, complementary efforts have explored the application of Convolutional Neural Network (CNN) architectures in anomaly detection within cloud infrastructure metrics . CNN models are proficient at automatically extracting relevant features that capture normal operational patterns within cloud environments. Through monitoring deviations from these learned patterns, anomalies such as server failures and performance degradations can be promptly identified.

Table 1. Comparison of machine learning techniques for cloud anomaly detection

Technique	Supervision	Novelty Detection	Explainability	Data Efficiency
Neural Networks	High	Low	Low	High data
SVM	High	Low	High	Low data
Clustering	None	High	High	Low data
Isolation Forests	None	High	High	Low data
Ensembles	Hybrid	Medium	Low	Medium data

Despite the promising results attained by neural networks in anomaly detection, several challenges persist. One such challenge lies in the substantial data requirements necessary for effectively training these models. Moreover, interpreting the learned patterns within neural networks poses a significant obstacle, hindering the transparency and comprehensibility of model outputs. Mitigating these challenges often necessitates meticulous hyperparameter tuning and the adoption of techniques such as model distillation to enhance the efficiency and interpretability of neural network-based anomaly detection systems.

Support Vector Machines: Support Vector Machines (SVM) represent a class of supervised learning models widely employed for anomaly detection tasks . These models operate by delineating optimal hyperplane decision boundaries that effectively segregate normal and anomalous instances within a dataset. Particularly, one-class SVM variants are notable for their capacity to learn solely from data representing normal behavior patterns, making them suitable for scenarios where anomalous instances are scarce or hard to define [21].

SVMs have found practical application in intrusion detection systems deployed in cloud infrastructures. For instance, researchers have devised SVM-based classifiers tailored for the detection of compromised Virtual Machine (VM) images transmitted via cloud storage channels . Leveraging features such as file permissions, formats, and contents, SVM algorithms can discern deviations indicative of tampering by malicious actors, thereby enhancing the security posture of cloud-based environments.

The efficacy of SVMs in anomaly detection is underpinned by several inherent advantages. Notably, SVM models exhibit resilience against overfitting, a common pitfall in machine learning, owing to their ability to generalize well to unseen data. Moreover, SVMs are adept at handling high-dimensional datasets by leveraging kernel methods to implicitly map input features into higher-dimensional spaces where linear separability may be achieved. However, it

is crucial to acknowledge that the computational overhead associated with SVM training and inference can escalate considerably when confronted with very large datasets, potentially impeding scalability in certain applications.

Ensemble Methods: Ensemble machine learning techniques offer a robust approach to enhancing prediction accuracy by integrating the outputs of multiple individual models. In the realm of anomaly detection, ensemble methodologies capitalize on the diversity of techniques available, drawing from a wide array such as neural networks, support vector machines (SVM), clustering algorithms, and more. One notable instance of this approach involved a hybrid ensemble framework proposed by Gulenko et al. (2016), which amalgamated Bayesian networks, decision trees, and SVM specifically for detecting anomalies across different layers of cloud platforms, including Software Infrastructure as a Service (S-IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). This sophisticated ensemble architecture strategically optimized diverse models tailored to the distinct characteristics of each cloud layer, thereby significantly enhancing the detection rates of malicious activities [22].

Performance Comparison of Machine Learning Algorithms

Algorithm	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**Time Complexity**	**Training Time**	**Cloud Platform Compatibility**
K-Nearest Neighbors	0.92	0.88	0.9	0.89	O(n^2)	Fast	High
Isolation Forest	0.95	0.9	0.92	0.91	O(log n)	Fast	High
One-Class SVM	0.9	0.85	0.88	0.86	O(n^2)	Moderate	Moderate
Your Proposed Algorithm	X	X	X	X	X	X	X

The strength of ensemble methods lies in their ability to mitigate the limitations of individual models by aggregating their predictions, thereby reducing both bias and variance. Nevertheless, this increased model complexity can present challenges in terms of interpretability, as understanding the combined decision-making process of multiple models may prove intricate. Despite these complexities, supervised techniques have showcased considerable promise in the context of cloud anomaly detection. However, their efficacy is contingent upon the availability of meticulously labeled datasets that adequately represent the diverse spectrum of potential anomalies that may manifest within cloud environments. Hence, while ensemble machine learning holds substantial potential for advancing anomaly detection in cloud computing, its successful implementation necessitates careful consideration of various factors, including model interpretability and the quality of training data.

Unsupervised Anomaly Detection: Unsupervised techniques model normal behavior to identify anomalies, without requiring abnormal samples during training. By learning patterns from unlabeled data, unsupervised approaches can detect novel anomalies. Common unsupervised anomaly detection techniques include clustering, nearest neighbor analysis, isolation forests, and more.

Clustering algorithms group unlabeled data points into clusters based on similarity. Points distant from clusters are identified as anomalies. One system applied density-based clustering on provenance graphs modeling cloud workflow execution . Anomalous workflows like malware

execution patterns were detected based on graph structural differences. Isolation forests isolate anomalies by recursively partitioning data until anomalies end up in small partitions . An isolation forest approach for cloud anomaly detection used an ensemble of random isolation trees to pinpoint unusual security group configurations and potentially malicious settings .

A downside of unsupervised techniques is the lack of anomalous examples for optimizing detection. Anomalies identified may represent legitimate but rare data points. Techniques like active learning can iteratively refine unsupervised models. Overall, unsupervised learning provides value for cloud anomaly detection without extensive labeled data [23].

Hybrid Anomaly Detection: Hybrid anomaly detection combines supervised and unsupervised techniques to leverage their complementary strengths. One hybrid approach applied a clustering ensemble built using supervised classifiers . The ensemble improved cluster quality for profiling normal cloud usage patterns. Deviations from these profiles indicated configuration anomalies and potential attacks.

Autoencoder neural networks are also effective for hybrid anomaly detection. Autoencoders reconstruct inputs using dimensionality reduction. Reconstruction errors are higher for anomalies deviating from normal patterns modeled in lower dimensions. Supervision can be incorporated by training on proxy anomaly data. Hybrid methods augment unsupervised learning with either indirect or limited supervision. This focuses models on relevant anomalies. Hybrid anomaly detection delivers flexible and robust cloud security analytics.

Table 2. Performance of supervised models on cloud network intrusion dataset

Model	Accuracy	False Positives	False Negatives
RNN-LSTM	99.2%	1.1%	0.9%
CNN	98.5%	1.8%	2.1%
SVM	96.7%	2.2%	3.5%

Comparative Evaluation of Machine Learning Techniques

Each category of techniques has relative advantages. Supervised models can directly optimize anomaly detection, but gathering comprehensive labeled data can be prohibitive. Unsupervised methods avoidexpensive labeling efforts and can detect novel anomalies, but lack anomaly examples to focus modeling. Hybrid approaches combine their benefits.

Selecting optimal techniques depends on multiple factors: Securing the vast and dynamic ecosystem of cloud environments presents a continuous challenge. Anomaly detection plays a crucial role in safeguarding this ever-evolving landscape, identifying deviations from established patterns that might signify potential threats [24]. However, choosing the ideal detection technique requires careful consideration, as diverse factors influence effectiveness. This section delves into key considerations when navigating the cloud anomaly detection landscape:

Availability of Labeled Anomaly Data: Supervised learning algorithms excel at recognizing patterns based on historical examples. In the context of anomaly detection, this translates to requiring a substantial dataset of labeled anomalous events and behaviors. Unfortunately, such labeled data is often scarce within cloud environments [25]. While normal cloud activity data might be readily available, identifying and labeling anomalous occurrences can be a laborious and resource-intensive endeavor. This data scarcity poses a significant limitation for supervised learning techniques, as their performance hinges on the quality and quantity of training data [26].

Novelty of Threats: The cloud threat landscape is inherently dynamic, with new attack vectors and vulnerabilities emerging constantly. Supervised learning models excel at detecting known anomalies, those already represented within the training data. However, their ability to identify novel threats is limited [27]. In contrast, unsupervised learning techniques analyze data without predefined labels, making them better suited to pinpointing deviations from the established "normal" behavior, even if the specific nature of the anomaly is unknown. This makes them more adaptable to detecting novel threats and zero-day attacks.

Explainability Requirements: Understanding the rationale behind an anomaly detection model's output is crucial for security analysts to effectively investigate and respond to potential threats. Simpler models like Support Vector Machines (SVMs) and isolation forests tend to offer greater explainability. Their decision-making processes are easier to comprehend, allowing analysts to trace the logic behind an identified anomaly. In contrast, complex neural networks, while exhibiting superior accuracy in anomaly detection, often suffer from limited interpretability. Their intricate structure and vast number of parameters make it challenging to understand how they arrive at their predictions, hindering effective investigation and response.

Performance Metrics: Evaluating the effectiveness of an anomaly detection technique hinges on defining the acceptable rates of false positives and negatives. A false positive indicates an alert triggered for normal activity, leading to wasted resources and analyst fatigue. Conversely, a false negative signifies a missed anomaly, potentially leaving the system vulnerable. The acceptable rates for these metrics significantly depend on the specific context of detection. For instance, a financial services firm might prioritize minimizing false positives to avoid unnecessary disruptions, while a critical infrastructure provider might value a lower false negative rate to ensure maximum security [28]. By understanding the specific needs and risk tolerance, detection models can be fine-tuned to balance precision and recall, optimizing performance for the intended application.

Ensembling for Robustness: No single technique can address all the nuances and challenges inherent in cloud anomaly detection. Each approach offers its own strengths and weaknesses, making it advantageous to adopt an ensemble strategy. Orchestrating a combination of complementary models, tailored to different data types, attack vectors, and performance requirements, provides a more robust and adaptable detection system [29]. By leveraging the diverse strengths of various techniques, organizations can achieve a more comprehensive and effective anomaly detection posture in their cloud environments.

Table 3. Unsupervised anomaly scores by cloud resource type

Resource	Anomaly Score
Compute	0.21
Storage	0.15
Network	0.03
Memory	0.10

Open Challenges and Future Outlook

Machine learning has emerged as a potent weapon in the fight against cyber threats, and its impact on cloud security is undeniable. However, despite significant progress, several hurdles remain that hinder its full potential. Recognizing these challenges and exploring promising avenues for improvement is crucial to effectively leverage machine learning and fortify cloud defenses.

One of the biggest obstacles lies in the dynamic nature of cyber threats. Malicious actors constantly refine their tactics, developing novel malware, exploiting new vulnerabilities, and shifting their attack vectors. This necessitates agile detection models capable of adapting to these evolving threats. The challenge lies in maintaining training data that reflects the latest attack signatures and behaviors. Static datasets quickly become outdated, potentially rendering models ineffective against zero-day exploits or sophisticated targeted attacks. Furthermore, cloud environments themselves are subject to "concept drift." Normal patterns of user activity, resource utilization, and network traffic can evolve over time due to changes in applications, user base, and infrastructure configurations. This phenomenon can gradually drift a model's understanding of "normal" behavior, leading to false positives and missed detections. To counter this, continuous model retraining or active learning techniques become essential, requiring efficient mechanisms to incorporate new data and refine the model's understanding of dynamic cloud environments.

Another significant challenge stems from the inherent opaqueness of some machine learning models, particularly deep neural networks. While these models deliver impressive predictive power, their decision-making processes often lack transparency. This "black box" nature makes it difficult to understand how and why the model identifies specific events as anomalies, hindering interpretability and trust . Explainable AI (XAI) methods are crucial to address this issue, providing insights into the model's rationale and fostering confidence in its security decisions. Another roadblock lies in the scarcity of labeled data. Anomalies by definition deviate from the norm, making them inherently rare and difficult to capture and label comprehensively. This creates a hurdle for supervised learning techniques that rely heavily on labeled training data. Techniques like semi-supervised learning, which leverage both labeled and unlabeled data, hold promise in overcoming this data scarcity challenge. By incorporating unlabeled data, these techniques can enrich the learning process and improve anomaly detection capabilities.

The distributed nature of cloud architectures presents another layer of complexity. Traditional security monitoring often focuses on individual components, overlooking subtle, yet critical, interdependencies between distributed microservices and containers. These subtle interactions, when compromised, can manifest as anomalies that are difficult for existing models to capture. Integrating causality analysis and graph models into the learning process can potentially address this challenge by enabling the model to understand and reason about the relationships between distributed components, leading to more comprehensive anomaly detection. Hybridizing machine learning models is another promising approach to overcome limitations. By combining different algorithms with distinct strengths, hybrid models can leverage the complementary capabilities of each approach. For instance, combining anomaly detection methods with threat intelligence feeds can enhance real-time threat identification and response.

Finally, the ever-evolving threat landscape necessitates learning models that can adapt and evolve at pace. Online adaptable learning techniques, which continuously update the model based on new data and feedback, offer a potential solution. This allows the model to learn from ongoing security incidents and refine its detection capabilities in real-time, improving its resilience against emerging threats.

Conclusion

Cloud computing has revolutionized the way we store, access, and process information. Its inherent scalability, agility, and cost-effectiveness have propelled its adoption across industries, transforming how businesses operate and individuals interact with technology. However, this very concentration of critical data within cloud environments also paints them as high-value

targets for malicious actors. Securing these environments amidst a constantly evolving threat landscape remains a paramount challenge.The dynamic nature of cyber threats demands intelligent and adaptable security solutions. Traditional, signature-based approaches struggle to keep pace with the ingenuity and innovation of adversaries who continuously refine their tactics and exploit new vulnerabilities. Anomaly detection powered by machine learning offers a promising paradigm shift, enabling proactive defense by identifying suspicious deviations from established behavioral patterns. This empowers security teams to anticipate and respond to threats before they can inflict significant damage.

This paper delved into the state-of-the-art in anomaly detection techniques for cloud security. We explored the potential of supervised learning models like neural networks and support vector machines, the efficiency of unsupervised approaches like clustering and isolation forests, and the synergistic capabilities of hybrid methods. We provided a comparative evaluation, highlighting the strengths and weaknesses of each category under different data conditions. However, even these advanced techniques face hurdles that require continued research and development. Adapting to the ever-evolving threat landscape remains a critical challenge. Machine learning models must possess the agility to continuously learn and update themselves based on the latest attack signatures and behaviors. Additionally, cloud environments themselves are subject to "concept drift," where normal patterns of activity and resource utilization can evolve over time. Models must be equipped to address this drift and maintain their effectiveness in dynamic environments.

The opacity of certain machine learning models, particularly deep neural networks, presents another roadblock. While delivering impressive predictive power, their "black box" nature hinders interpretability and trust. Explainable AI (XAI) methods are crucial to address this issue, providing insights into how and why these models identify specific events as anomalies. This transparency fosters trust and enables security teams to make informed decisions based on the model's insights. Data scarcity poses another hurdle, as anomalies by definition deviate from the norm and are inherently rare to capture and label comprehensively. This creates a challenge for supervised learning techniques that rely heavily on labeled training data. Semi-supervised learning and other data-efficient methods hold promise in overcoming this obstacle by incorporating unlabeled data into the learning process.

Finally, the distributed nature of cloud architectures demands a shift from individual component-focused security towards understanding subtle interdependencies between microservices and containers. Integrating causality analysis and graph models into the learning process can empower models to reason about these relationships and identify anomalies that might otherwise go undetected [30]. Addressing these challenges through continued research and development is crucial to unlocking the full potential of machine learning for cloud security. Hybridizing models to leverage the strengths of different approaches, adopting online adaptable learning for continuous improvement, and actively exploring promising avenues like semi-supervised learning and causality analysis are just some of the potential solutions on the horizon.

Looking ahead, AI-enhanced anomaly detection has the potential to become an indispensable component of our cyber defense arsenal. As techniques mature and challenges are addressed, intelligent anomaly detection systems will provide unparalleled threat monitoring capabilities, safeguarding valuable data and services in the cloud. This will pave the way for a future where trust, security, and innovation can flourish within the cloud paradigm, empowering individuals and organizations to leverage its transformative potential without fear.

References

[1] R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, no. 1, Dec. 2020.

[2] A. Chaudhary, H. Mittal, and A. Arora, "Anomaly Detection using Graph Neural Networks," in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, Faridabad, India, 2019.

[3] S. E. Hajjami, J. Malki, M. Berrada, and B. Fourka, "Machine Learning for anomaly detection. Performance study considering anomaly distribution in an imbalanced dataset," in *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*, Marrakesh, Morocco, 2020.

[4] R. K. Dwivedi, A. K. Rai, and R. Kumar, "A study on machine learning based anomaly detection approaches in wireless sensor network," in *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 2020.

[5] J. P. Singh, "Mitigating Challenges in Cloud Anomaly Detection Using an Integrated Deep Neural Network-SVM Classifier Model," *Sage Science Review of Applied Machine Learning*, vol. 5, no. 1, pp. 39–49, 2022.

[6] R. K. Dwivedi, R. Kumar, and R. Buyya, "Gaussian distribution-based machine learning scheme for anomaly detection in healthcare sensor cloud," *Int. J. Cloud Appl. Comput.*, vol. 11, no. 1, pp. 52–72, Jan. 2021.

[7] L.-P. Jin and J. Dong, "Intelligent health vessel ABC-DE: An electrocardiogram cloud computing service," *IEEE Trans. Cloud Comput.*, vol. 8, no. 3, pp. 861–874, Jul. 2020.

[8] N. Xuan Phi, L. Ngoc Hieu, and T. Cong Hung, "Load balancing algorithm on cloud computing for optimize respone time," *Int. J. Cloud Comput. Serv. Archit.*, vol. 10, no. 3, pp. 15–29, Jun. 2020.

[9] D. Balouek-Thomert and E. G. Renart, "Towards a computing continuum: Enabling edge-to-cloud integration for data-driven workflows," *Journal of High …*, 2019.

[10] M. Makgato, "STEM for sustainable skills for the Fourth Industrial Revolution: Snapshot at some TVET colleges in South Africa," *Theorizing STEM education in the 21st century*, pp. 144–159, 2019.

[11] D. Dias, F. C. Delicato, P. F. Pires, A. R. Rocha, and E. Y. Nakagawa, "An overview of reference architectures for cloud of things," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, Brno Czech Republic, 2020.

[12] Y. Suhas, V. Kohli, S. Ghaffar, and R. Kashef, "Network flow classification and volume prediction using novel ensemble deep learning architectures in the era of the internet of things (IoT)," in *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, AB, Canada, 2021.

[13] G. Procaccianti, P. Lago, and S. Bevini, "A systematic literature review on energy efficiency in cloud software architectures," *Sustain. Comput. Inform. Syst.*, vol. 7, pp. 2–10, Sep. 2015.

[14] D. Kant and A. Johannsen, "Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs)," *IS&T Int. Symp. Electron. Imaging*, vol. 34, no. 3, pp. 387-1-387–8, Jan. 2022.

[15] S. Li, W. Sun, Y. Zhang, and H. Liu, "Reliability analysis for multipath communications in mobile cloud computing architectures," *Wirel. Commun. Mob. Comput.*, vol. 2018, pp. 1–12, Jun. 2018.

[16] S. Feng, Z. Xiong, D. Niyato, and P. Wang, “Dynamic resource management to defend against advanced persistent threats in fog computing: A game theoretic approach,” *IEEE Trans. Cloud Comput.*, vol. 9, no. 3, pp. 995–1007, Jul. 2021.
[17] M. Fazio, R. Ranjan, M. Girolami, J. Taheri, S. Dustdar, and M. Villari, “A note on the convergence of IoT, edge, and cloud computing in smart cities,” *IEEE Cloud Comput.*, vol. 5, no. 5, pp. 22–24, Sep. 2018.
[18] S. Kp, R. P. Reddy, and N. R. Ponnada, “An intelligent blockchain based cryptographic data security (IBCDS) model for an efficient data sharing in cloud,” *Int. J. Cloud Comput.*, vol. 13, no. 4, 2024.
[19] M. Muniswamaiah and T. Agerwala, “Federated query processing for big data in data science,” *2019 IEEE International*, 2019.
[20] J. P. Singh, “Enhancing Database Security: A Machine Learning Approach to Anomaly Detection in NoSQL Systems,” *International Journal of Information and Cybersecurity*, vol. 7, no. 1, pp. 40–57, 2023.
[21] T. Xu *et al.*, “Vector control of the single-phase inverter based on the extended and virtual circuits,” *China Electrotech. Soc. Trans. Electr. Mach. Syst.*, vol. 2, no. 3, pp. 320–327, Sep. 2018.
[22] I. Deliu, C. Leichter, and K. Franke, “Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks,” in *2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, 2017.
[23] M. Muniswamaiah, T. Agerwala, and C. Tappert, “Big Data in Cloud Computing Review and Opportunities,” *arXiv [cs.DC]*, 17-Dec-2019.
[24] K. ur Rehman, J. Li, Y. Pei, and A. Yasin, “A review on machine learning techniques for the assessment of image grading in breast mammogram,” *Int. J. Mach. Learn. Cybern.*, vol. 13, no. 9, pp. 2609–2635, Sep. 2022.
[25] I. Doghudje and O. Akande, “Dual User Profiles: A Secure and Streamlined MDM Solution for the Modern Corporate Workforce,” *JICET*, vol. 8, no. 4, pp. 15–26, Nov. 2023.
[26] M. Kamal and T. A. Bablu, “Machine Learning Models for Predicting Click-through Rates on social media: Factors and Performance Analysis,” *IJAMCA*, vol. 12, no. 4, pp. 1–14, Apr. 2022.
[27] R. Yang, K. Zheng, B. Wu, D. Li, Z. Wang, and X. Wang, “Predicting User Susceptibility to Phishing Based on Multidimensional Features,” *Comput. Intell. Neurosci.*, vol. 2022, p. 7058972, Jan. 2022.
[28] M. Muniswamaiah, T. Agerwala, and C. C. Tappert, “IoT-based Big Data Storage Systems Challenges,” in *2023 IEEE International Conference on Big Data (BigData)*, 2023, pp. 6233–6235.
[29] J. C. Perez *et al.*, “Enhancing adversarial robustness via test-time transformation ensembling,” in *2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW)*, Montreal, BC, Canada, 2021.
[30] S. Asefi, M. Mitrovic, D. Ćetenović, V. Levi, E. Gryazina, and V. Terzija, “Power system anomaly detection and classification utilizing WLS-EKF state estimation and machine learning,” *arXiv [eess.SY]*, 26-Sep-2022.