Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.jistm.com

INTELLIGENT MODELS FOR INTRUSION DETECTION OVER CLOUD INFRASTRUCTURE: A LITERATURE REVIEW

Mansir Abubakar[1*], Alwatben Batoul Rashed[2], Mohamad Yusof Darus[3], Armayau Z. Umar[4]

[1] Department of Computer Science, College of Computing, Informatics and Mathematics, Universiti Teknologi Mara (UiTM), Shah Alam, 40000 Selangor, Malaysia
Email: mansir@uitm.edu.my
[2] Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia
Email: batool.alwtban@gmail.com
[3] Department of Computer Science, College of Computing, Informatics and Mathematics, Universiti Teknologi Mara (UiTM), Shah Alam, 40000 Selangor, Malaysia
Email: yusof_darus@uitm.edu.my
[4] College of Computing and Information Science, Al-Qalam University Katsina, Nigeria
Email: azuamar@auk.edu.ng
[*] Corresponding Author

Article Info:

Article history:
Received date: 14.01.2025
Revised date: 23.01.2025
Accepted date: 27.02.2025
Published date: 20.03.2025

To cite this document:

Abubakar, M., Rashed, A. B., Darus, M. Y., & Umar, A. Z. (2025). Intelligent Models For Intrusion Detection Over Cloud Infrastructure: A Literature Review. *Journal of Information System and Technology Management, 10* (38), 162-180.

DOI: 10.35631/JISTM.1038011

Abstract:

Cloud Computing has revolutionized the information technology (IT) landscape, enabling scalable and on-demand access to resources. However, its reliance on shared infrastructure introduces vulnerabilities, necessitating advanced security measures. Traditional intrusion detection systems (IDSs) struggle to cope with the complexity and scale of cloud environments. Machine Learning (ML) has emerged as a promising approach, offering automation, adaptability, and enhanced detection capabilities, thus, ensuring intelligence in intrusion detection systems. With the increasing reliance on cloud infrastructure for critical applications, ensuring robust security measures has become paramount. This paper reviews existing works that employ Machine Learning (ML) techniques for intrusion detection in cloud environments. By analyzing the strengths and weaknesses of these models, we identify gaps in current approaches and propose potential research directions. Furthermore, we recommend advanced ML techniques to enhance the security and reliability of cloud-based systems. The existing literature revealed that the transition from conventional methods to advanced learning approaches signals a critical shift in the landscape of cloud-based security, although

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

the literature disclosed that further research is necessary to refine these models and enhance their effectiveness across diverse attack vectors.

Keywords:

Cloud Computing, Intelligent Models, Intrusion Detection System, Machine Learning

Introduction

Cloud infrastructure refers to the set of hardware, software, networks, storage systems, and services that work together to support computing in a cloud environment. It forms the backbone of cloud computing, enabling users to store data, run applications, and leverage computing resources remotely over the internet. Key components of cloud infrastructure include physical data centers equipped with servers, storage devices, and networking equipment, as well as virtual resources like virtual machines (VMs) and containers, which ensure flexibility and scalability. Cloud infrastructure can be deployed in various models, such as public, private, or hybrid clouds, and is managed through platforms that automate resource allocation, security, and monitoring. It supports a wide range of services, including Infrastructure as a Service (IaaS), enabling businesses to reduce costs, enhance performance, and scale operations dynamically (Smith, 2020).

Intelligent models for intrusion detection on cloud infrastructure leverage advanced machine learning and deep learning techniques to enhance security against evolving cyber threats. These models are designed to monitor, analyze, and classify network traffic, effectively identifying both external and internal intrusions. The main objectives of this paper is to review studies that adopt ML techniques for detecting attacks on cloud systems, evaluate the strengths and limitations of existing approaches, and also recommend effective ML-based models to improve cloud security. To avoid reinventing the wheel in this review, we focus on the recent literature that based their findings on the previous literature in addressing the the issues of security on over the cloud infrastructure.

Security on Cloud Infrastructure

Cloud computing has transformed modern IT services by offering scalable, effective, and flexible resources. However, this reliance on cloud platforms introduces vulnerabilities, making them a prime target for cyber-attacks. Intrusion Detection Systems (IDS) are critical for identifying and mitigating threats, and recent advancements in ML have shown promise in improving their accuracy and adaptability. Cloud computing has revolutionized the IT landscape, enabling scalable and on-demand access to resources. However, its reliance on shared infrastructure introduces vulnerabilities, necessitating advanced security measures. Traditional intrusion detection systems (IDS) struggle to cope with the complexity and scale of cloud environments. Machine learning (ML) has emerged as a promising approach, offering automation, adaptability, and enhanced detection capabilities.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

The field of intrusion detection systems (IDS) has seen significant evolution in response to the increasing complexity of cyber threats, particularly within the context of cloud infrastructure and IoT environments. The literature highlights a shift from conventional machine learning techniques to more advanced methodologies, particularly deep learning, which are gaining traction due to their enhanced capabilities in processing vast and unstructured data. In a systematic literature review, (A. Alsoufi et al, 2021) argue that traditional machine learning approaches have limitations when applied to the unique challenges posed by IoT-generated data, which is characterized by its speed and volume. They underscore the necessity for deep learning techniques as they offer superior accuracy in feature extraction and anomaly detection compared to their conventional counterparts. Despite the promising nature of deep learning in this domain, the authors note that many existing IDS solutions are adaptations from traditional computer networks, which may not be suitable for the distinct characteristics of IoT applications. Their analysis reveals a gap in comprehensive reviews focusing on deep learning techniques specifically for IoT security, suggesting a need for further exploration into effective anomaly detection methods tailored to this environment.

Building upon this foundation, (Abu Al-Haija, 2022) presents a top-down machine learning-based architecture aimed at identifying and classifying cyberattacks within IoT communication networks. The author acknowledges the challenges posed by IoT heterogeneity and the limited resources of devices, which complicate the implementation of effective security measures. The study emphasizes the integration of conventional machine learning techniques with cybersecurity efforts, while also exploring the potential of deep neural networks. However, the research is critiqued for its narrow focus on a specific dataset that primarily addresses DDoS attacks, thus limiting its applicability to broader cybersecurity contexts. The findings highlight the effectiveness of certain machine learning classifiers, such as Random Forest and J48, in detecting malicious traffic, yet they also point to the labor-intensive nature of manual feature selection as a significant drawback.

Together, these articles illustrate the ongoing challenges and advancements in the development of intelligent models for intrusion detection on cloud infrastructure, particularly as they pertain to the unique demands of IoT environments. The transition from conventional methods to deep learning approaches signals a critical shift in the landscape of cybersecurity, although the literature reveals that further research is necessary to refine these models and enhance their effectiveness across diverse attack vectors. In contrast to the existing reviews, this paper focus on the evaluation of the strength and limitations of the intelligent intrusion detection models in order to suggest and recommend potential areas for refinement and enhancement of security in a cloud environment.

Intrusion Detection on Cloud Infrastructure

Intrusion detection involves monitoring network traffic and system activities for malicious behavior. Unlike traditional systems, cloud-based IDS must address challenges such as multi-tenancy, scalability, and diverse attack vectors. Intrusion detection involves identifying unauthorized access or malicious activities within systems or networks, often through specialized tools known as Intrusion Detection Systems (IDS). These systems are integral to

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011
modern cybersecurity frameworks, providing critical early warnings against threats. Intrusion Detection Systems can be categorized broadly into:

- Network-Based Intrusion Detection Systems (NIDS): These monitor and analyze network traffic to detect malicious activities (Scarfone & Mell, 2007).
- Host-Based Intrusion Detection Systems (HIDS): These operate on individual hosts, monitoring file access, logs, and processes (Singh & Silakari, 2009).
- Hybrid Systems: Combining NIDS and HIDS, these provide a comprehensive approach to threat detection (Alharbi et al, 2016).

Methods of Intrusion Detection

Intrusion detection with machine learning (ML) involves using algorithms to identify unauthorized or malicious activities within a network or system. Traditional intrusion detection systems (IDS) rely on predefined signatures or rules, making them less effective against novel or evolving threats. Machine learning methods address this limitation by analyzing patterns, anomalies, and behaviors in data to detect potential intrusions proactively. Generally, methods of intrusion detection are classified into:

Signature-Based Detection: This approach uses predefined patterns to detect known threats. While effective for familiar attacks, it struggles with new or evolving threats (Roesch, 1999).

Anomaly-Based Detection: By establishing a baseline for normal behavior, this method identifies deviations, making it useful for detecting novel attacks but prone to false positives (Sommer & Paxson, 2010).

Machine Learning-Based Detection: Leveraging advanced algorithms, this method can uncover complex attack patterns but requires substantial computational resources (Sculley et al, 2011). This paper focused more on the findings that leverages this method of intrusion detection.

Importance of Intrusion Detection System (IDS)

Intrusion detection is vital for Threat Detection; It is promising in detecting active attacks and reducing response times (Scarfone & Mell, 2007). It is also important in ensuring Regulatory Compliance via supporting standards such as GDPR and HIPAA that require system monitoring (Peltier, 2016). ID is can as well be used in Incident Response that requires providing forensic data to analyze the impact and scope of attacks (Casey, 2011). Intrusion detection is a cornerstone of cybersecurity, offering the ability to identify and mitigate threats proactively. When combined with other measures like firewalls and threat intelligence platforms, IDS can significantly enhance organizational security. Figure 1 shows a Cloud Computing Environment along with potential security vulnerabilities where application of Machine Learning Models should be a potential solution.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

Figure1: A Cloud Computing Environment Showing Potential Security Vulnerabilities

Role of Machine Learning in IDS

Machine learning (ML) algorithms significantly enhance intrusion detection systems (IDS) by leveraging their ability to learn patterns from historical and real-time data. Traditional IDS often rely on predefined rules or static signatures to identify threats, which can struggle to adapt to the ever-evolving nature of cyberattacks. ML algorithms, however, are dynamic and adaptive, capable of analyzing vast datasets to uncover subtle and complex attack patterns that might otherwise go undetected. By learning from both normal and anomalous behavior, these algorithms improve the system's ability to differentiate between benign activities and genuine threats (Kshetri, 2021; Latah & Toker, 2020).

The key benefits of ML-powered IDS include automation, real-time detection, and a marked reduction in false positives. Automation minimizes the need for continuous manual intervention, enabling the system to independently monitor, detect, and even respond to threats. This is crucial in environments with high volumes of network traffic, where manual oversight would be impractical (Cheng et al, 2020). Real-time detection ensures that threats are identified and mitigated swiftly, often before significant damage occurs (Kumar et al, 2021). Additionally, ML models can significantly reduce false positives by better understanding the nuances of normal system behavior, which prevents benign activities from being flagged unnecessarily and reduces the burden on security teams (Kshetri, 2021). Ultimately, the integration of ML into IDS represents a powerful evolution in cybersecurity, delivering faster, smarter, and more reliable protection against both known and emerging threats.

Machine Learning Based Intrusion Detection Models (IDMs)

This section reviews ML-based IDS in cloud environments, focusing on their application, performance metrics, and limitations. Intelligent models for intrusion detection in cloud infrastructure leverage advanced machine learning and deep learning techniques to enhance security against evolving cyber threats. These models are designed to monitor, analyze, and classify network traffic, effectively identifying both external and internal intrusions strategic points in a cloud environment as shown in figure 2.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

Figure 2: A Cloud Computing Environment Showing Where Intelligent Intrusion Detection Systems Can Operate

These systems are highlighted at critical junctures to monitor, detect, and prevent security breaches effectively. The key components depicted in the figure are briefly highlighted below alongside the security vulnerabilities at each Intelligent Intrusion Detection points with the key roles IIDM can play. Table 1 shows security vulnerabilities with IIDM roles on a key components of cloud infrastructure.

Table 1: Security Vulnerabilities with IIDM Roles

Key Component	Risk	IIDM Role
Client Endpoints Authentication	Weak credentials or phishing attacks.	Monitor login behaviors, detect unusual patterns, and flag unauthorized access attempts.
API Communications	Insecure APIs can be exploited for data breaches or unauthorized access.	Analyze API requests in real-time, identifying anomalous activity or malicious payloads.
Data Flow Between Components	Intercepted or tampered data during transmission.	Use traffic analysis to detect anomalies like packet injection or unexpected spikes in data flow.
Data Storage	Unauthorized access or data breaches.	Monitor access patterns to detect attempts to ex-filtrate or corrupt data.
Virtual Machine (VM) Operations	Virtual machine escapes, where malicious actors exploit VM vulnerabilities to access the host system.	Detect and respond to unusual system calls or behavior within VMs.
Insider Threats (Cloud Provider)	Employees with malicious intent or accidental mismanagement.	Monitor user activity logs and flag abnormal behaviors suggesting insider threats.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

Client Endpoints: Represent devices like desktops, mobile phones, and IoT devices connecting to the cloud; **Application Servers:** Handle requests and process data; **Data Storage:** Centralized databases where sensitive data is stored; **Virtual Machines (VMs):** Visualized resources running applications and services; **Cloud Provider:** Oversees infrastructure and operations, posing potential internal risks.

Figure 2 show how intelligent intrusion detection models can be strategically placed to safeguard critical points within the cloud infrastructure. It highlights the synergy between proactive monitoring and response systems in mitigating cloud-based security risks as presented in Table 1. The following sections outline key approaches and findings from recent researches that take in to consideration one or more of aforementioned strategic places.

Supervised Learning Models

Supervised models that applied Decision Trees (DT) are widely used due to their interpretability and low computational cost. However, they may struggle with high-dimensional data. A research highlights the application of various machine learning algorithms to address the challenges faced by traditional IDS. These algorithms are tailored to enhance the detection capabilities of the system (D.K. Sudha et al, 2023). The research compares the performance of the ODT with other machine learning algorithms, such as Naïve Bayes (NB), Logistic Regression (LR), Linear Discriminant Analysis (LDA), and K-Nearest Neighbor (KNN). This comparative analysis helps to demonstrate the effectiveness of the proposed method. In a similar work, a Decision Tree (DT) approach to create rules based on both anomalous and legitimate traffic, aiming to enhance detection capabilities while minimizing complexity (Coscia et al, 2024). Its introduction hints at the performance metrics that the proposed algorithm aims to achieve, indicating that it will be evaluated against existing machine learning classifiers and other state-of-the-art solutions in terms of detection rates and execution times.

Other studies employed Support Vector Machines (SVM) due to its Effectiveness in binary classification but proved to be computationally intensive for large datasets. An enhanced model combines these techniques to classify data packets, improving detection accuracy and efficiency in cloud environments (I.F. et al, 2024). The research presents an enhanced model for intrusion detection in cloud environments, utilizing machine learning techniques like Support Vector Machine and Bayesian Network to classify data packets, detect intrusions from both external and internal users, and improve network efficiency. Another work (R. Hari et al 2024) presents an Intrusion Detection System (IDS) tailored for cloud environments, utilizing Ensemble SVM models trained with bagging and boosting techniques on the UNSW_NB15 dataset, enhancing detection accuracy and robustness against network intrusions. This study introduces a specialized Intrusion Detection System (IDS) designed specifically for cloud computing environments. By leveraging the UNSW_NB15 dataset, it employs feature selection techniques such as Select KBest and ANOVA to extract relevant features, thereby improving the overall performance of the model.

Random Forests (RF) algorithm is another promising supervised family known for robustness and accuracy; however, prone to overfitting in certain cases. A recent study Cloud Computing Security via Intelligent Intrusion Detection Mechanisms (Hamza et al 2024), highlights the effectiveness of machine learning models, particularly the Random-Forest-Classifier, achieving a high test accuracy in intrusion detection. It emphasizes the advantages of intelligent systems

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011
over traditional rule-based and signature-based methods for cloud securityStudies also uses Auto-encoders have emerged as a powerful tool in intrusion detection systems (IDS) (Moukhafi et al, 2024), leveraging their ability to learn compressed representations of network traffic data. These models, particularly when combined with other deep learning techniques, demonstrate significant improvements in detecting anomalies and malicious activities across various network environments. LSTM-based Autoencoders also captured temporal dependencies in network traffic, achieving high accuracy in identifying intrusions, as shown in experiments with the NSL-KDD dataset (Elezmazy & Mostafa, 2024). In another development, Multiple-Input Auto-Encoder (MIAE) Designed for heterogeneous IoT data processes diverse inputs effectively, achieving a better accuracy in detecting sophisticated attacks (Dinh et al, 2024). Deep Auto-encoder with Stacked LSTM integrated approach enhances feature extraction and classification, yielding a promising accuracy on the UNSW-NB15 dataset (Moukhafi et al, 2024). Auto-encoders excel in scenarios with imbalanced data, improving classification accuracy by compressing majority samples and enhancing minority sample representation (Khan, 2024). The combination of auto-encoders with other models, such as Multi-Layer Perceptron (MLP), broadens the detection capabilities and improves performance across various attack types (Yashwanth et al, 2024).

While supervised methods show promise in enhancing IDS performance, challenges remain, such as managing false positives and ensuring privacy in data handling. Balancing detection accuracy with ethical considerations is crucial for the future of network security.

Unsupervised Learning Models

In this review, we reported the work of (Remah, Younisse., Qasem, Abu, Al-Haija, 2023) who draws several important conclusions regarding the use of online k-means clustering for intrusion detection systems (IDS). The study concludes that online k-means clustering is an effective method for intrusion detection, demonstrating performance levels comparable to traditional offline k-means clustering. This is particularly significant given the challenges posed by online data, which is often unbalanced and continuously generated in real-time environments. The results indicate that the online k-means algorithm can achieve high clustering purity rates, with 99% for normal packets and 93% for anomaly packets. This suggests that the algorithm is capable of accurately distinguishing between normal and malicious traffic, which is crucial for effective intrusion detection.

The study emphasizes the importance of data normalization in enhancing the performance of the online k-means clustering algorithm. Normalized data led to better clustering outcomes, highlighting that preprocessing steps can significantly impact the effectiveness of machine learning models in cybersecurity applications. It also demonstrates that the online k-means clustering method is robust when applied to diverse intrusion scenarios within an Internet of Things (IoT) network environment. This adaptability is essential for real-world applications where various types of intrusions may occur.

While the study provides promising results, it also suggests that further research is needed to explore the scalability of the online k-means clustering method in larger and more complex datasets. Additionally, investigating the integration of this method with other machine learning

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011
techniques could enhance its effectiveness in detecting sophisticated intrusions. The findings pave the way for future advancements in cybersecurity methodologies.

Hybrid Approaches

Hybrid models combine supervised and unsupervised methods to leverage their strengths. For example, combining RF with clustering has shown improvements in detection rates and scalability. A hybrid model utilizes DNNs for feature extraction and RF for classification, demonstrating superior performance in recognizing various intrusions (R. Hari et al, 2024). The research presents a novel DNN-RF model for intrusion detection in cloud environments, leveraging Deep Neural Networks for feature extraction and Random Forest for interpretability, enhancing security by accurately identifying and classifying various intrusions effectively. (R. Hari et al, 2024) presents a Hybrid Learning Model (HLM) that combines supervised and unsupervised learning techniques for intrusion detection in cloud environments, enhancing accuracy and reducing false positives through methods like Iterative Intrusion Detection System and Support Vector Machine with transfer learning.

An innovative *Biz-SCOP Model* integrates hybrid optimization and deep learning, achieving remarkable accuracy and effectively identifying various attack types (Menezes et al, 2024). The Biz-SCOP model integrates hybrid optimization techniques and an intelligent deep learning model, C2AE, to enhance intrusion detection in cloud environments, achieving high accuracy and performance in identifying various attack types, thus addressing security challenges effectively.

Deep Learning Models

Convolutional Neural Networks (CNN) based models demonstrates effectiveness for image-like data representations of traffic patterns but computationally expensive. CNN-based models have shown high accuracy in detecting cyber-attacks, effectively handling large-scale traffic in cloud networks (Aljuaid & Alshamrani, 2024). The research proposes a deep learning-based model utilizing convolutional neural networks (CNNs) for intrusion detection in cloud environments, achieving over 98% accuracy, precision, and recall, effectively addressing the challenges of detecting and classifying cyber attacks in cloud networks. Lightweight CNN with Particle Swarm Optimization is an approach that optimizes CNN parameters, achieving good accuracy and enhancing the model's adaptability to new threats (Rosline & Rani, 2024). The paper proposes a lightweight convolutional neural network (CNN) for intrusion detection in cloud environments, enhanced by particle swarm optimization (PSO) to optimize CNN parameters, thereby improving security against unauthorized access and data breaches.

A *novel Salp Swarm* Algorithm-Based Feature Selection with Deep Learning-Based Intrusion Detection *(SSAFS-DLID*) method for cloud infrastructure demonstrates promising potential in reinforcing the security environments of CC system (Durga, et al 2024). The study employs the Salp Swarm Algorithm for feature selection. This algorithm is designed to efficiently identify important features from large datasets, which helps in reducing computational complexity and dimensionality while ensuring that critical data is preserved for analysis.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

Strengths and Weaknesses of the Reviewed Models

Strengths

A model's strength lies in its ability to effectively learn patterns, relationships, and insights from data, enabling it to make accurate predictions or decisions. This strength is rooted in the quality of its architecture, such as the number and configuration of layers in neural networks or the choice of algorithms in machine learning approaches. Additionally, the strength is heavily influenced by the quality and quantity of the training data it is exposed to, as well as the fine-tuning of its hyper-parameters. Robust preprocessing techniques, adequate regularization to prevent overfitting, and scalability to handle diverse datasets further contribute to a model's resilience and reliability. Ultimately, a model's strength is reflected in its ability to generalize well to unseen data while maintaining efficiency and adaptability across different applications. Some notable strength are identified as follows:

Adaptability: Many ML models can learn new attack patterns. Adaptability in the context of machine learning refers to the ability of a model or algorithm to adjust and improve its performance in response to changing data or environments. This is crucial for real-world applications where data can be dynamic and unpredictable. Here are some key aspects of adaptability in machine learning:

a. Adaptive Algorithms: These algorithms can modify their internal parameters based on new data. For example, in supervised learning, models continuously refine their understanding of patterns and relationships as they encounter new labeled data.
b. Real-Time Learning: Adaptive machine learning systems can process and learn from data in real-time, making them suitable for applications like fraud detection, recommendation systems, and autonomous driving where conditions change rapidly.
c. Robustness and Efficiency: Adaptive models are designed to be more robust and efficient compared to traditional models. They can handle noise and variability in data better, leading to increased accuracy and sustainability.
d. Explainable AI (XAI): In educational contexts, for instance, adaptive models can be used to predict and explain student adaptability. Techniques like SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) help in understanding which features most influence the model's predictions.
e. Continuous Improvement: Adaptive machine learning involves continuous monitoring and updating of models to ensure they remain relevant and accurate over time. This is particularly important in environments where the underlying data distribution may change.

In general, adaptability enhances the practical utility of machine learning models by ensuring they remain effective in dynamic and evolving scenarios.

Scalability: Cloud-based implementations can scale ML models to handle large datasets. Scalability in machine learning refers to the ability of a model or system to handle increasing amounts of data, computational load, and user requests efficiently. Here are some key aspects of scalability in machine learning:

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

a. Data Handling: As datasets grow, scalable machine learning systems must efficiently process and store large volumes of data. This often involves distributed data storage and processing frameworks like Hadoop and Spark.
b. Model Training: Training machine learning models on large datasets can be computationally intensive. Scalable solutions often use distributed training techniques, where the workload is spread across multiple machines or GPUs. Frameworks like TensorFlow and PyTorch support distributed training.
c. Real-Time Processing: For applications requiring real-time predictions, such as recommendation systems or fraud detection, scalable systems must handle high throughput and low latency. This can be achieved using optimized data pipelines and serving architectures.
d. Resource Management: Efficiently managing computational resources is crucial for scalability. This includes using cloud services that offer auto-scaling capabilities, which automatically adjust resources based on demand.
e. Algorithm Efficiency: Scalable machine learning algorithms are designed to maintain performance as the size of the data and the complexity of the tasks increase. Techniques like mini-batch gradient descent and parallel processing help in achieving.
f. Monitoring and Maintenance: Scalable systems require continuous monitoring to ensure they perform well under varying loads. Tools for monitoring and logging help in identifying bottlenecks and optimizing performance.
g. Scalability is essential for deploying machine learning models in real-world applications where data and user demands can grow rapidly.

Improved Accuracy: Intrusion Detection models, in particular, have achieved high detection rates through the process of Data Quality and Preprocessing:

a. Data Cleaning: Remove or correct inaccurate records, handle missing values, and eliminate duplicates to ensure high-quality data.
b. Data Normalization and Scaling: Transform data to a common scale to ensure all features contribute equally to the model.
c. Creating New Features: Generate new features from existing data to capture more information and improve model performance.
d. Feature Selection: Identify and use the most relevant features to reduce noise and improve accuracy.
e. Choosing the Right Algorithm: Different algorithms have varying strengths. Evaluate multiple models to find the best fit for your data.
f. Cross-Validation: Use techniques like k-fold cross-validation to get a reliable estimate of model performance and avoid overfitting.
g. Hyper-parameter Tuning: Optimizing Parameters: Adjust the hyper-parameters of your model to find the best configuration for improved accuracy.
h. Combining Models: Use techniques like bagging, boosting, and stacking to combine multiple models and improve overall performance.
i. Regularization: Apply techniques like L1 and L2 regularization to prevent the model from fitting too closely to the training data.
j. Pruning: In decision trees, prune branches that have little importance to reduce complexity and improve generalization.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

k. Model Retraining: Regularly update the model with new data to maintain accuracy over time
l. By implementing these strategies, you can significantly enhance the accuracy of your machine learning models.

Weaknesses

Leveraging machine learning for intrusion detection offers transformative capabilities but also presents notable challenges. The primary concerns include:

Data Dependency: Supervised models require labeled data, which may not always be available. IDS models greatly rely on the availability of high quality, labeled data for their training. However, obtaining such data is challenging due to privacy concerns, and limited access to real-world attack scenarios. Employing techniques for data augmentation, synthetic data generation and federated learning is the way forward in mitigating such challenge.

High Computational Requirements: Deep models may be unsuitable for real-time detection in resource constrained environments. IDSs demand high computational resources like high-performance GPUs and significant memory capacities. This increases operational costs, particularly for small to medium-sized organizations when deploying cloud infrastructure. Leveraging cloud-native optimization techniques, model compression, and efficient training algorithms will drastically mitigate these challenges.

Generalization Challenges: Models trained on specific datasets may struggle with unseen attack patterns. Models trained on specific datasets may struggle to generalize to new and evolving attack patterns or diverse cloud environments. Techniques like meta-learning, which allows models to adapt to new attack scenarios with minimal training data, as described in Finn et al. (2017). Studies on transfer learning, such as the application to intrusion detection by Pan and Yang (2010). Adaptability and effectiveness in detecting unknown threats due to the fact that models trained on specific datasets may struggle to generalize to new and evolving attack patterns . The importance of continual learning frameworks, transfer learning, and ensemble approaches to improve the robustness and generalization capabilities of these models is essential.

Regulatory and Compliance Issues: Regulatory frameworks like HIPAA, GDPR, and CCPA can complicate the deployment of IDS on cloud infrastructure as well as the compliance to different regulatory issues (Abubakar et al., 2023) This challenge is critical as it has direct impact on how these regulations negatively affect data collection, processing, and storing and sharing across cloud environment.

Resistance to Technology Adoption: Stakeholders are the key component in technology adoption. Many organizations face resistance from stakeholders because of the concern about costs, the disruptions to existing workflows, and uncertainty on the reliability of AI-driven solutions. There is serious need for elaboration on the strategies to mitigate the consequences enforced by these concerns, this may be through gradual integration, demonstrating ROI, and comprehensive training.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

Data Privacy Concerns: Exploring the challenges of handling and maintaining data privacy when training ML-based models on sensitive cloud data is critical and the importance of employing techniques like federated learning and differential privacy is a way forward to addressing these challenges.

Overcoming these challenges is critical to fully realise the potential of machine learning in enhancing intrusion detection capabilities. Table 2 highlights how each machine learning technique aligns with a key challenge in relation to key concepts in different ways in terms of intrusion detection over cloud environment.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

Table 2: Relationships of Machine Learning Techniques with Key Challenges

Challenge / Technique	Adaptability	Scalability	Improved Accuracy	Computational Complexity	Data Dependency	Generalization Challenge
Supervised	Can adapt to new data if continuously retrained; however, it requires labeled data for effectiveness	Scales well with more labeled data, but training can become resource intensive with very large datasets.	Tends to achieve higher accuracy when provided with a quality and sufficient amount of labeled data.	Computation complexity depends on the model used; simple models are less complex than complex ones like ensemble methods.	Highly data dependent, as the quality and quantity of labeled data directly impact model performance.	Prone to overfitting if the model is too complex relative to the amount of training data, making generalization to unseen data challenging.
Unsupervised	Can identify new patterns in data without requiring labels, allowing flexibility in feature extraction.	Generally scalable; can handle large datasets effectively, especially with clustering methods that group data points.	Accuracy pertains more to the relevance of the discovered patterns; not as straightforward to measure as in supervised learning.	Varies with the algorithm; some methods, like k-means, are computationally less complex, while others like hierarchical clustering can be more intensive.	Still relies on data quality; irrelevant or noisy data can hinder meaningful pattern discovery.	May struggle to generalize since the model isn't trained with explicit labels; relevance to unseen data can be uncertain.
Hybrid Methods	Offers high adaptability by combining unsupervised preprocessing with supervised training to improve robustness.	Can be designed to scale by managing the complexity of handling both labeled and unlabeled data.	Often results in higher accuracy by leveraging strengths of both techniques, leading to better overall model performance.	Can be complex due to the combination of methods but can also be optimized for efficiency.	Balances the need for both labeled and unlabeled data, making it versatile in scenarios with limited labeled data.	May mitigate overfitting by using unsupervised methods to enhance the features captured before supervised training.
Deep Learning	Highly adaptable due to the ability to learn complex representations and features directly from raw data.	Extremely scalable, capable of processing large datasets efficiently using modern hardware (GPUs,TPs).	Often achieves state-of-the-art accuracy in various tasks, particularly in image and language processing, with sufficient data.	Generally high due to deep architectures requiring substantial computational resources for training.	Highly data dependent; requires large amounts of labeled data to achieve high performance.	Can face generalization challenges, particularly if not enough training data is provided; overfitting can be a risk unless proper regularization techniques are used.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

These relationships critically highlight how each machine learning technique aligns with or challenges these key concepts in different ways in terms of intrusion detection over cloud environment as presented in Table 2. These key challenges paves way to clear future research directions in ensuring maximum security on cloud infrastructure. The following section presents a synthetic summary of areas where security can be improved on cloud infrastructure with Intelligent Intrusion Detection method.

Future Research Directions

The future research to enhance security with Intelligent Intrusion Detection method should include the key directions highlighted as:

Addressing Scalability: Scalable frameworks like *Kubernetes*, which is widely used for orchestrating containerized applications, as highlighted in the work of (Burns et al. 2016). Server-less computing platforms, such as *AWS Lambda* and *Google Cloud* Functions, that enable dynamic resource allocation, will also be explored (Baldini et al., 2017). Lightweight algorithms like *TinyML*, which are designed for resource-constrained environments, and distributed machine learning frameworks like *Apache Spark MLlib* (Meng et al., 2016) will also be examined. Future models should focus on lightweight algorithms or distributed processing to reduce computational overhead while maintaining accuracy.

Handling Imbalanced Data: Synthetic data generation methods such as *Generative Adversarial Networks (GANs)* have been used to create diverse attack scenarios, as demonstrated in (Zhang et al., 2022). This method highlight the use of oversampling methods like *SMOTE* in handling class imbalance, as discussed in (Chawla et al. 2002). Techniques such as synthetic data generation or advanced sampling methods can help address the lack of labeled attack data.

Enhancing Real-time Detection: Online learning has been applied to intrusion detection in dynamic environments, such as the framework proposed in (Li et al. 2021). The use of federated learning for distributed real-time threat detection will be discussed, citing (Yang et al. 2019). Metrics like latency and resource management will be evaluated, referencing real-time benchmarks and case studies, such as the work by Tang et al. (2022). Real-time capabilities can be improved using online learning or federated learning approaches as presented in our recommendation section.

Robustness Against Evolving Threats: Techniques like meta-learning, which allows models to adapt to new attack scenarios with minimal training data, as described in (Finn et al. 2017). Studies on transfer learning, such as the application to intrusion detection (Pan and Yang 2010). These demonstrate how models can learn from one domain and generalize to another. We also highlight the role of continual learning in ensuring that models remain effective over time (Parisi et al. 2019). However, adopting reinforcement learning and adversarial training can make IDS more resilient to novel and adaptive attack strategies.

Recommended Methods for Performance Improvements

Ensemble Methods: Combining multiple models (e.g., RF + Auto-encoders) can leverage the strengths of different techniques for better accuracy and robustness.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

Transformer-based Architectures: Transformers, with their ability to process sequential data efficiently, are promising for cloud IDS applications.

Federated Learning Approaches: Distributed learning paradigms enable collaborative training of models across cloud nodes without compromising data privacy. Integrating this approach into existing ML models can enhance the performance of IDSs, specifically when handling privacy and ethical concerns.

Conclusion

This literature review examines the application of intelligent models, particularly machine learning (ML) and deep learning techniques, for intrusion detection in cloud infrastructure. The analysis reveals a significant shift from traditional signature-based intrusion detection systems (IDS) towards more advanced, adaptable ML-based approaches. While ML offers automation, enhanced detection capabilities, and real-time analysis, challenges remain, including scalability issues, handling imbalanced data, ensuring interpretability, and mitigating overfitting. The review highlights the strengths and weaknesses of various ML models (supervised, unsupervised, and hybrid), emphasizing the need for ongoing research to enhance robustness and efficiency, particularly regarding the adaptation to evolving attack vectors and the integration of advanced techniques such as ensemble methods, transformer-based architectures, and federated learning. Future research should focus on addressing scalability, data imbalance, real-time detection capabilities, and model robustness through integration of the recommended techniques, ultimately leading to more efficient, effective and reliable cloud security solutions.

Acknowledgment

The authors thank Universiti Teknologi MARA for supporting this work by providing a grant and the facilities needed to complete this review.

References

Alsoufi, M., Razak, S., Md. Siraj, M., Nafea, I., Abdulgaleel Abdoh Ghaleb, F., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in IoT using deep learning: a systematic literature review.

Abubakar, M. M., Armaya'u, Z. U., & Abubakar, M. (2023). Personal Data and Privacy Protection Regulations: State of compliance with Nigeria Data Protection Regulations (NDPR) in Ministries, Departments, and Agencies (MDAs), (pp. 1-6). IEEE. 10.1109/ITED56637.2022.10051182.

Abu Al-Haija, Q. (2022). Top-Down Machine Learning-Based Architecture for Cyberattacks Identification and Classification in IoT Communication Networks. https://doi.org/10.3389/fdata.2021.782902.

J., Dentamaro, V., Galantucci, S., Maci, A., & Pirlo, G. (2024). Automatic decision tree-based NIDPS ruleset generation for DoS/DDoS attacks.Journal of Information Security and Applications. https://doi.org/10.1016/j.jisa.2024.103736.

Alharbi, F., Aspinall, D., & Just, M. (2016). Challenges in intrusion detection systems. *Journal of Information Security*, *7*(2), 93–103.

Aljuaid, W. H., & Alshamrani, S. S. (2024). A Deep Learning Approach for Intrusion Detection Systems in Cloud Computing Environments. Applied Sciences. https://doi.org/10.3390/app14135381.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011
Baldini, I., Castro, P., Chang, K., Cheng, P., Fink, S., Ishakian, V., Mitchell, N., Muthusamy, V., Rabbah, R., Suter, P., & Tatbul, N. (2017). Serverless computing: Current trends and open problems. *Proceedings of the 8th ACM Symposium on Cloud Computing*, 281–293. https://doi.org/10.1145/3154862.

Burns, B., Grant, B., Oppenheimer, D., Brewer, E., & Wilkes, J. (2016). Borg, Omega, and Kubernetes: Lessons learned from three container-management systems over a decade. *Communications of the ACM, 59*(5), 50–57. https://doi.org/10.1145/2890784.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press, Coscia.

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic Minority Over-sampling Technique. *Journal of Artificial Intelligence Research, 16*, 321–357. https://doi.org/10.1613/jair.953.

Cheng, S., Xiao, Z., & Yang, J. (2020). Machine learning in intrusion detection systems: A survey. *IEEE Access,8,*182463–182486. https://doi.org/10.1109/ACCESS.2020.3029584

Durga, Prasada, Rao, Sanagana., Chaitanya, Kanth, Tummalachervu. (2024). Securing Cloud Computing Environment via Optimal Deep Learning-based Intrusion Detection Systems. doi: 10.1109/icdsis61070.2024.10594404.

Finn, C., Abbeel, P., & Levine, S. (2017). Model-agnostic meta-learning for fast adaptation of deep networks. *Proceedings of the 34th International Conference on Machine Learning*, 1126–1135. https://doi.org/10.5555/3305381.3305498.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, 169–178. https://doi.org/10.1145/1536414.1536440.

Hamza, Nasir., Azeem, Ayaz., Shahzmaan, Nizamani., Saima, Siraj., Shahid, Iqbal., M, Kamran, Abid. (2024). Cloud Computing Security via Intelligent Intrusion Detection Mechanisms. International Journal of Information Systems and Computer Technologies, doi: 10.58325/ijisct.003.01.0082.

I.F., Ogbomo, Okwudili, A. S., Nkiru, Anigbogu. G., & Sylvanus, A. K. (2024). An Enhanced Model for Intrusion Detection in a Cloud Computing Environment.Asian Journal of Research in Computer Science. https://doi.org/10.9734/ajrcos/2024/v17i7478.

K.Sudha, K. S., Devi, D., C.Balakrishnan, C. B. MegibaJasmine, R. T. Nithya, T. N., & Subramanian, R. S. (2023). A Effective Detection Method using Optimized Decision Tree Classification for Network based Intrusion. https://doi.org/10.1109/iceca58529.2023.10394812.

Kshetri, N. (2021). AI and ML for cybersecurity: The good, the bad, and the ugly. *Journal of Cybersecurity, 7*(1), 1–12. https://doi.org/10.1093/cybsec/tyab001.

Kumar, S., Jha, R., & Singh, A. (2021). Enhancing real-time cybersecurity with machine learning techniques. *Information Security Journal: A Global Perspective, 30*(2), 93–103. https://doi.org/10.1080/19393555.2021.1894043

Latah, M., & Toker, L. (2020). Integration of machine learning with intrusion detection systems: Challenges and future directions. *Computer Networks, 173*, 107276. https://doi.org/10.1016/j.comnet.2020.107276.

Li, Z., Chen, L., & Wang, W. (2021). Real-time intrusion detection in cloud-based systems using online learning. *IEEE Transactions on Emerging Topics in Computing, 9*(1), 150–163. https://doi.org/10.1109/TETC.2021.3052605

McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. Y. (2017). Communication-efficient learning of deep networks from decentralized data.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011

Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 1273–1282.

Meng, X., Bradley, J., Yavuz, B., Sparks, E., Venkataraman, S., Liu, D., Freeman, J., Tsai, D., Amde, M., Owen, S., Xin, D., Xin, R., Franklin, M. J., Zadeh, R., Zaharia, M., & Talwalkar, A. (2016). MLlib: Machine learning in Apache Spark. *The Journal of Machine Learning Research, 17*(1), 1235–1241. https://doi.org/10.5555/2946645.3058583.

Menezes, R. J., Jayarin, P. J., & Sekar, A. C. (2024). A bizarre synthesized cascaded optimized predictor (BizSCOP) model for enhancing security in cloud systems. https://doi.org/10.1186/s13677-024-00657-1.

Pan, S. J., & Yang, Q. (2010). A survey on transfer learning. *IEEE Transactions on Knowledge and Data Engineering, 22*(10), 1345–1359. https://doi.org/10.1109/TKDE.2009.191.

Parisi, G. I., Kemker, R., Part, J. L., Kanan, C., & Wermter, S. (2019). Continual lifelong learning with neural networks: A review. *Neural Networks, 113*, 54–71. https://doi.org/10.1016/j.neunet.2019.01.012

Peltier, T. R. (2016). *Information security policies, procedures, and standards: Guidelines for effective information security management* (2nd ed.). CRC Press.

R, A., Das, U., Ak, D., & Balachandar, N. (2024).Cloud-based Intrusion Detection System using Various Machine Learning Techniques. https://doi.org/10.1109/icicv62344.2024.00071.

Roesch, M. (1999). Snort - Lightweight intrusion detection for networks. *Proceedings of the 13th Systems Administration Conference (LISA '99)*, 229–238.

Rosline, G. J., & Rani, M. P. (2024). Intrusion detection system for cloud environment based on convolutional neural networks and PSO algorithm.Indonesian Journal of Electrical Engineering and Computer Science. https://doi.org/10.11591/ijeecs.v35.i3.pp1499-1506.

R. Hari, Krishna., Pallipamula, Vijaya, Bhaskar., Prasritha, Narahari., Meghana, Nalluri., Mohith, Ram, Mallapureddy. (2024). Intrusion Detection System on Cloud Computing using Ensemble SVM. International Journal For Multidisciplinary Research, http://doi.org/10.36948/ijfmr.2024.v06i02.17212.

Remah, Younisse., Qasem, Abu, Al-Haija. (2023). An empirical study on utilizing online k-means clustering for intrusion detection purposes. doi: 10.1109/smartnets58706.2023.10215737.

Ring, M., Wunderlich, S., Scheuring, D., & Landes, D. (2019). A survey of network-based intrusion detection data sets. *Computer & Security, 86*, 147–167. https://doi.org/10.1016/j.cose.2019.06.005.

Rudin, C. (2019). Stop explaining black box machine learning models for high-stakes decisions and use interpretable models instead. *Nature Machine Intelligence, 1*(5), 206–215. https://doi.org/10.1038/s42256-019-0048-x.

Sanagana, D. P. R., & Tummalachervu, C. K. (2024).Securing Cloud Computing Environment via Optimal Deep Learning-based Intrusion Detection Systems. https://doi.org/10.1109/icdsis61070.2024.10594404.

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)*. NIST Special Publication 800-94. National Institute of Standards and Technology.

Sculley, D., Holt, G., Golovin, D., & Wilkerson, J. (2011). Challenges in machine learning for intrusion detection. *ACM Transactions on Information and System Security, 14*(3), 1–27.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 162-180
DOI: 10.35631/JISTM.1038011
Singh, B., & Silakari, S. (2009). A survey of cyber attack detection systems. *International Journal of Computer Applications, 1*(7), 17–21.

Smith, J. (2020). Cloud infrastructure: The foundation of cloud computing. Tech Insights Journal, 15(3), 45-60. https://www.techinsightsjournal.com/cloud-infrastructure

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, 305–316.

Tang, M., Liu, Y., & Wei, W. (2022). Federated learning-based intrusion detection for real-time cyber defense. *Future Generation Computer Systems, 135*, 110–120. https://doi.org/10.1016/j.future.2022.05.018.

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology, 10*(2), 1–19. https://doi.org/10.1016/j.future.2019.02.007

Zhang, L., Wang, Y., & Huang, H. (2022). A novel intrusion detection system based on GAN and deep reinforcement learning in cloud computing. *Computers & Security, 117*, 102678. https://doi.org/10.1016/j.cose.2022.102678.