Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Machine Learning for Cloud Security: A Systematic Review

Shirley C P[1*], Thanga Helina S[2], Thusita S[3], Okesh A[3]
[1]Assistant Professor (SG), Department of CSE, Karunya Institute of Technology and Sciences, Coimbatore, India.
[2]Assistant Professor, Department of Commerce with Computer Application, KPR College of Arts Science and Research, Coimbatore, India.
[3]Student, Department of CSE, Karunya Institute of Technology and Sciences, Coimbatore, India.
*Corresponding Author: shirleydavidlivingston@gmail.com

ARTICLE INFO

Received: 26 Dec 2024

Revised: 14 Feb 2025

Accepted: 22 Feb 2025

ABSTRACT

The research investigates cloud security by executing machine learning (ML) applications to obstruct cyber threats within cloud infrastructure. This research uses different ML approaches to construct IDSs by testing multiple IDS variations using the NSL-KDD attack simulation dataset pool. The evaluation shows J48 and PART having 88% accuracy while Decision Stump reaches 90% accuracy and Decision Table reaches 93% and AODE reaches 99% accuracy. The ability of Average One Dependency Estimator to detect patterns in lengthy multi-dimensional datasets makes it the optimal solution. Feature selection techniques including Intrinsic Information together with Information Gain and Gain Ratio improve both data performance and operational efficiency by reducing dimensions. The conversion of numeric features to nominal types ensures maximal algorithm performance because several ML models function more efficiently with categorical data. The system undergoes thorough evaluation to determine its accuracy levels and speed performance and cloud application compatibility. The research provides an effective security platform which merges state-of-the-art ML approaches with elaborate preprocessors and evaluators to enhance security protection against progressively changing threats.

Keywords: Cloud Computing, Threats, Security, Mitigation Strategies

INTRODUCTION

The IT industry experienced a transformation through cloud computing which introduced flexible computing capabilities according to demand. The system gives businesses effective data handling capabilities through large-scale data storage alongside reduced infrastructure expenditures. Cloud environment adoption has increased significantly yet security threats in these systems have grown proportionally large. Organizations face three main threats stemming from data breaches in addition to insider attacks and advanced persistent threats that endanger their confidential data. Secure systems running traditional firewall-based intrusion detection cannot address the complicated security challenges present in current cyber-attacks. The capabilities of ML tools include analysing vast datasets while detecting precise patterns and detecting rare occurrences in the data. Small cloud vulnerabilities create negligible risks for ML-enabled security platforms that employ supervised learning along with unsupervised learning and deep learning techniques to detect standard and zero-day attacks. The presented work examines a new ML-driven method for cloud security through machine learning algorithm implementation for intrusion detection alongside threat prediction and access control systems. The NSL-KDD dataset functions as a well-known test benchmark that enables evaluating many different ML classification methods. The system identifies J48 and PART along with Decision Table, Decision Stump and Average One Dependency Estimator (AODE) classifiers as its base to achieve maximum detection accuracy and minimize false positives. This paper demonstrates how procedural testing of combined feature selection approaches with preprocessing techniques reveals the effectiveness of ML-based intrusion detection systems that operate in cloud environments. The paper discusses implementation challenges of cloud security deployment based on ML that stem from data privacy problems and adversarial threats and computational cost demands. The challenges of adopting ML cannot prevent it from bolstering cloud security frameworks because it enables real-time security threat response along with dynamic security control mechanisms. The union of expert ML systems and cloud security protocols enables organizations to strengthen defensive measures which protect data from developing cyber-attacks.

1. CLOUD COMPUTING

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

In the fast-changing environment of information technology, Cloud Computing stands out as a revolutionary paradigm that has transformed how businesses and consumers access, store, and manage data and applications. Cloud computing goes beyond traditional computing models by allowing on-demand access to a shared pool of computing resources, such as servers, storage, and applications, via the Internet. This transformational strategy provides unprecedented scalability, flexibility, and cost-efficiency, enabling organizations to dynamically increase their infrastructure in response to demand. The essence of Cloud Computing is its capacity to provide computing services as utilities, allowing customers to utilize strong resources without making major upfront hardware and infrastructure investments. As Cloud Computing use spreads across industries, understanding its principles, benefits, and challenges becomes critical for businesses looking to maximize its potential while addressing relevant concerns such as security, privacy, and compliance. This introduction lays the context for delving into the diverse world of Cloud Computing, highlighting its disruptive impact on the modern IT landscape.

2.SECURITY

Information technology security operates as an essential component because it establishes digital system trust together with integrity and robustness. The extensive application of technological progress across both individual daily life and corporate functions has led security demands for information infrastructure and technological design to reach previously unknown heights. The implementation of security requires multiple modern protocols alongside advanced techniques together with sophisticated methods to stop unwanted breaches while maintaining data confidentiality and protection as well as system accessibility. The fast-forwarding pace of digitization innovation and network access necessitates security domains to transform their strategies in order to tackle recent cyber threats and data exposure events as well as privacy safeguarding matters. The historical perspective serves as fundamental groundwork for a complete investigation into digital security operations which must evolve due to the rapid development of technology. The spirit of a robust responsive policy stands essential for our increasingly linked information-based society given our future exploration of security principles.

3.THREATS

The present digital world experiences a persistently evolving and active danger to information system security and stability through threats. Technology adoption by humans and business entities creates enormous risks through cyber threats due to naturally expanding dependence on electronic systems to manage data and conduct business and communicate. Contemporary security threats follow multiple types of harmful conduct and deficiencies which harm data quality and expose system flaws while disrupting vital infrastructure operations. Several entities including cybercriminals and state hackers with inside staff members alongside programming flaws and system misconfigurations alongside unintended operator conduct create situations where systems face the risk of security breaches. The protection of digital assets from various threats represents a fundamental requirement for information security as governments and individuals join organizations to defend their resources against unwanted breach attempts and data theft. Organizations need to deploy comprehensive active defence systems with robust security controls since phishing attacks and ransomware operations and APTs and distributed denial of service attacks have reached advanced levels of sophistication. New attack vectors are developed because cloud computing, IoT and AI technologies continue to advance which makes digital infrastructure protection increasingly hard to achieve. A valuable cybersecurity system requires multiple security elements which join threat information with risk evaluation and perpetual monitoring through automated machines alongside threat prediction algorithms to safeguard against potential risks. Nonetheless strong dedication to cybersecurity awareness training should exist in organizations to reduce human error weaknesses and maintain compliance with industry benchmarks. An analysis has established fundamental principles for grasping sophisticated cyber threats as well as the ongoing requirement for cybersecurity improvement.The preventive security measures consisting of adaptive threat detection together with encryption and authentication approaches with automated responses effectively mitigate cyber threats caused by dynamic nature. The development of technological modernizations leads to increased requirements for flexible security solutions thus necessitating collaborative efforts between industries cybersecurity professionals and policymakers to establish security in the digital environment.

4.MITIGATION STRTEGIES

Mitigation measures are proactive and reactive that are intended to counter cybersecurity threats and reduce risks in cloud systems. Conventional mitigation methods depend on institutionalized security policies and manual threat

analysis, which can be slow and inefficient when dealing with advanced persistent threats. Machine learning has assisted in the evolution of cloud security, enabling adaptive and intelligent defensive measures to be incorporated. ML-based countermeasures include threat detection via anomalies, predictive threat analysis, and automated incident response. Supervised learning algorithms are trained on past attack patterns to mark malicious activity for future classification, whereas unsupervised learning identifies previously unknown attacks. Reinforcement learning optimizes security automation as it learns to adjust constantly to changing patterns of attacks. For instance, machine learning algorithms such as Random Forest, Support Vector Machines (SVM), and Neural Networks are used to track network traffic patterns to detect anomalies that may be an indication of possible security attacks. By using real-time threat intelligence, organizations adapt access control policies, detect insider threats, and improve incident response effectiveness. Moreover, ML-based security solutions are integrated with cloud-native security platforms like SIEM systems to deliver end-to-end threat visibility. Automated mitigation lightens the burden of security analysts, allowing them to respond to threats quicker and ensure better compliance with regulatory needs. As cloud computing grows, the contribution of machine learning to cybersecurity will become more vital. Companies will need to invest in AI-powered security systems that will enhance their defence systems, safeguard sensitive information, and provide security against sophisticated cyber-attacks for cloud environments.

LITERATURE SURVEY

Research regarding this topic currently represents one of the speediest growing academic fields due to rapid shifts in both cloud computing platforms and cyber-attack methods. Studies under cloud security focus on different subject areas which include threat detection alongside vulnerability analysis and machine learning integration for enhanced IDS performance. Mishra created an ontology-based automated threat modeling system in 2023 which detected threats within ICT environments through complete integration of threat and vulnerability detection under cloud infrastructures to enhance the capabilities of IDS systems.

[1]. Dorri et al. (2019) presented a systematic assessment of various cybersecurity maturity assessment frameworks for technology start-ups which showed that solid security processes during initial system development form dependable bases for improved cloud environment intrusion detection.

[2]. Mistry et al. (2020) investigated the vast empirical research into cloud-based project dependencies and security vulnerabilities to demonstrate that cloud system vulnerabilities present an effective security risk. Strong IDS development becomes essential now because they need to detect weaknesses before threats materialize.

[3]. Felcia and Sabeen (2022) demonstrated that international software development vendors should implement a security assurance model while conducting continuous security monitoring with proactive measures to protect system integrity which matches the IDS system requirements in cloud computing by identifying threats in real-time and reducing false positive results.

[4]. Apthorpe et al. (2019) presented the development of smart grid security alongside their proposal for cloud security systems to address dynamic sophisticated security threats. Research demonstrates the need to improve IDS systems for detecting modern threats which primarily affect integration between IoT networks and cloud systems.

[5]. The paper by Qu et al. (2018) explored how the business world adopted IoT alongside its resulting security challenges. The current IDS systems fail to provide appropriate protection because IoT devices now integrate into cloud infrastructure thus requiring new security strategies to protect against DDoS attacks that create substantial threats to cloud service providers.

[6]. A survey by Kumar and Goyal (2019) regarding cloud security issues showed the need to develop hybrid security models combining machine learning and anomaly detection methods for improving all aspects of intrusion detection systems. The identification of complex advanced-dynamic attack patterns represents a standard feature for hybrid models that regular models typically miss.

[7]. The research by Sharma et al. (2019) proved that machine learning operates effectively to identify DDoS attacks within cloud environments and revealed how machine learning algorithms support the improved detection capabilities of intrusion detection systems through their ability to detect hard-to-detect anomalies.

[8]. Vijayakumar and Arun (2019) developed distributed hashing for ongoing security assessment together with machine-learning techniques for cloud security enhancement.

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[9]. MSCryptoNet represents a privacy-protection deep learning model that Kwabena et al. (2019) introduced because deep learning has emerged as a critical technology for identifying sophisticated attack vectors while ensuring privacy within cloud systems. Future IDS systems face a need for deep learning implementation to improve their siege against complex cyber attacks.

[10]. Bhajantri and Mujawar (2019) presented an evaluation of security threats facing cloud computing along with suitable countermeasures. IDS systems require capabilities to maintain automatic updates regarding the unique security issues which affect cloud environments particularly including new application deployment models and scalability needs.

[11]. The authors of Alhenaki et al. (2019) recommend hybrid IDS systems with integrated conventional security mechanisms and machine-learning methods that will strengthen detection capabilities.

[12]. The literature describes how models that unify machine learning with deep learning along with hybrid models should be developed according to their authors to achieve maximum cloud IoT-based IDS system efficiency. Advanced technologies enable IDS systems to simultaneously develop their capabilities for addressing cloud environment threats. The upcoming research on IDS systems will work on developing scalable privacy-focused adaptable cloud-based structures for protecting cloud environments from emerging threats.

EXISTING SYSTEM

Cloud security implementations through regular systems utilize two intrusion detection methods which combine attack signatures with anomaly detection for threat identification. Among all IDS options Snort Intrusion Detection System has gained notable popularity. The system performs network traffic scanning against established attack signatures stored within its database. The system can detect previously known attacks due to this strategy. Signatures in its database become the main limitation through which this system fails to detect zero-day attacks and emerging threats. The rigidity of signature-based IDS makes it necessary to regularly update its attack signatures to successfully address current cyber threats. The C4.5 Decision Tree Algorithm serves as a popular tool for this work. The system utilizes predetermined rules to analyze network traffic in order to evaluate its behavior as either normal or malicious. The algorithm shows excellent results when working with structured data sources and provides definite outcome decisions. Complex datasets create difficulty for this system which leads to poor performance because it tends to overfit in dynamic cloud environments. The anomaly-based detection method uses Support Vector Machines (SVMs) as one of its main tools. SVMs evaluate network traffic patterns together with abnormal behaviors to determine normal vs abnormal traffic groups. The ability of SVMs to detect attack and normal traffic remains strong but their success in big cloud installations depends heavily on proper feature selection and detailed adjustments. Real-time threat detection in cloud systems requires highly expensive and complex SVM operations. The present cloud security models demonstrate significant problems with excessive false alarms that decrease detection speeds and their inability to deal with emerging security threats. The existing limitations within intrusion detection systems call for an immediate development of a smart machine learning system to address them. The system needs to handle cloud network traffic during operation while enhancing its accuracy level through real-time automation of security measures.

PROPOSED SYSTEM

A cloud-based system utilizing machine learning technology enables detection of intrusions to improve cloud security according to this proposal. The processor has two main components which first utilize the NSL-KDD database before transforming numbers into nominal values for analytical purposes. The feature selection process employs Information Gain, Intrinsic Information and Gain Ratio to increase model performance and operational speed. The system employs J48 (Decision Tree) and Support Vector Machine (SVM) classifiers for attack detection. J48 identifies known attack patterns well but shows superior capabilities to SVM when detecting anomalies hidden in cloud environments. The IDS provides real-time operation to learn threats continuously while detecting DoS and Probe and U2R and R2L attack types. Sheer scalability enables the system to adjust its performance based on evolving cloud environments together with traffic pattern changes. The system protects from known as well as emerging risks through signature detection coupled with anomaly detection techniques. The testing procedures ensure that cloud systems operate reliably and precisely and function effectively in operational cloud environments.Through layered approach the security system detects existing and undiscovered threats while maintaining complete cloud security protection. **Figure 1** demonstrates the system flow as shown in the diagram.

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

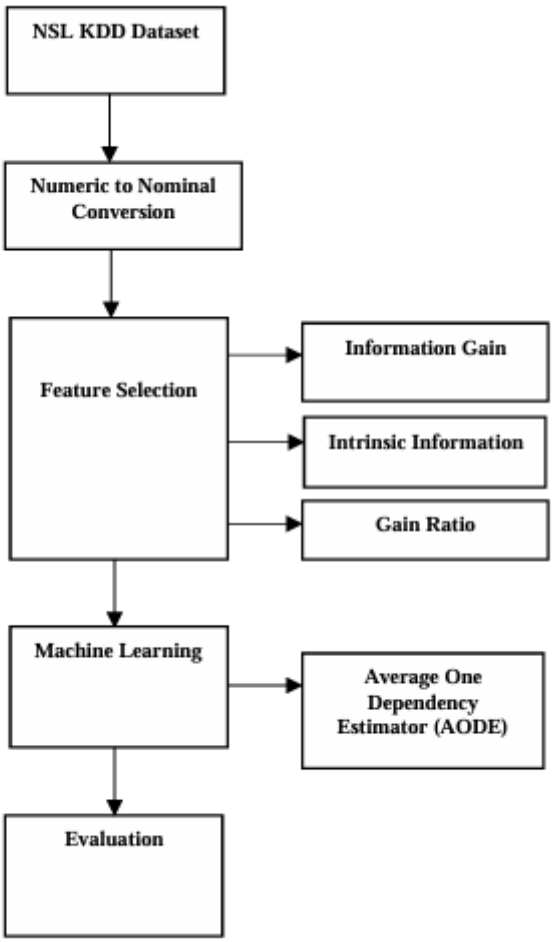

Figure 1. SYSTEM FLOW DIAGRAM

The systematic review of machine learning for cloud security requires this comparison Table 1 to assess different models with AODE (Average One Dependence Estimator) algorithm**.**

Aspect	AODE Algorithm	Decision Tree Classifer (J48)	SVM Classifier
Architecture	Average dependencies form the basis for how AODE operates as a probabilistic classifier.	The hierarchical structure develops through tree-based model nodes which perform splits according to feature values.	The supervised classifier divides data into various classes through the application of hyperplane segmentation.
Feature Extraction	The process of data extraction focuses on discovering statistical patterns together with the relationship between different attributes with emphasis on attribute interactions.	The system derives rule-based decision criteria from each splitting point that appears at a tree node.	Extracts global features through the hyperplane decision boundary.
Performance in Noisy Data	The probabilistic nature of Naive Bayes helps it maintain high performance standards along with its capabilities	The model accuracy suffers while split changes occur in response to noise thus leading to decreased performance levels.	Authoritative data sets can harm its performance while poor adjustment causes the model to overfit.

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	to handle uncertain conditions in noisy environments.		
Computational Complexity	The computational requirements of AODE remain low since it needs to determine only the typical dependencies across features.	Calculating each decision split adds to the moderate level of complexity of the evaluation process.	Optimization of hyperplanes creates high computational expenses which become worse when working with high-dimensional data structures.
Scalability	The method demonstrates high scalability because it functions well on large datasets when using average feature dependencies.	Scalability falls between moderate and high levels but performance could decrease according to tree depth.	Scalable with kernel tricks, but computationally intensive for large datasets.
Robustness to Cloud Security Threats	Its probabilistic approach makes the system excel at finding both new and irregular attack patterns.	This method shows superior speed in identifying recognized attack patterns though it cannot detect fresh or complex security threats.	It demonstrates high performance in identifying sophisticated attack patterns throughout extensive attack data training.
Suitability for Continuous Learning	The system adapts automatically while preserving learning functions which enhances its performance in dynamic cloud platforms.	Retraining on new information remains necessary when using this method while its ability to learn continuously diminishes in dynamic environments.	The system supports continuous learning but adjustment needs to be precise and it could experience concept drift because of its operational design.

Table 1. . Comparison Between Existing Models and The Proposed AODE Model

A. NSL KDD DATASET

NSL-KDD serves as an updated version of KDD'99 dataset designed to resolve the problems of redundancy along with bias and misrepresentation that affected intrusion detection research. The original KDD'99 dataset included many repetitive and extra data points that led to inconsistent model training and misappropriated outcome assessment. The NSL-KDD dataset now serves as an outstanding benchmark for Intrusion Detection System (IDS) testing because it offers both better distribution and representative selection of network traffic records. The proposed cloud-based intrusion detection system utilizes the NSL-KDD dataset for its main data source during both training and testing periods. The system contains standard network traffic data together with Denial of Service (DoS) and Probe and User to Root (U2R) and Remote to Local (R2L) attacks which represent various security vulnerabilities in cloud computing infrastructure. A single entry within the dataset shows sixty-four features that describe numerous network traffic dimensions from connection time to protocol type to service type to IP address information to flag status and final attack classification. These network characteristics help identify both dangerous network patterns while determining between normal traffic and attack patterns. Three selection methods including Information Gain, Gain Ratio and Intrinsic Information have been implemented to pick the relevant attributes that will simplify computational complexity while advancing detection accuracy during machine learning training (J48 and SVM). The system achieves better cyber threat identification and classification precision after it optimizes and prepares its dataset. The intrusion detection system using NSL-KDD delivers real-time monitoring and precise threat categorization and automatic response through this dataset thus becoming an effective security solution for cloud infrastructure protection against emerging cyber threats.

B. NUMERIC TO NOMINAL CONVERSION

The Numeric to Nominal Conversion module represents an essential preprocessing step for the suggested cloud-based intrusion detection system because it prepares the dataset for optimal performance by machine learning algorithms. The classification algorithms J48 and SVM function optimally when using categorical data instead

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

of numeric continuous values. Multiple numerical features contained within the NSL-KDD dataset become more efficiently analyzed by converting them to nominal (categorical) values which enables better network traffic classification. The data transformation process provides clearinterpretability because it matches every feature to the specific input types needed by themachine learning models used in this project. The proposed system process converts numerical features including protocol, service and flag status information into distinct categorical categories as part of its conversion protocol. TCP along with UDP and ICMP receive text-based inputs instead of treating them as numeric data points. The model succeeds in its learning processes through nominal representations of flag statuses which capture connection states including SYN, ACK and REJ. The transformation process safeguards against misinterpretations by machine learning models of numerical features as continuous patterns because it prevents classification blunders. The system implements numeric-to-nominal-value conversions to enhance data consistency and feature interpretability and accuracy of intrusion detection in cloud systems. The preprocessing operation enables the model to perform better in behavioral discrimination through proper machine learning dataset organization. This preprocessing approach improves both computational efficiency and attack detection precision during the training process and improves security system attack decisions. The Numeric to Nominal Conversion module holds a crucial position to enhance dataset optimization for achieving precise cyber threat detection in cloud security systems.

C. FEATURE SELECTION

Feature Selection serves as an essential element of the proposed cloud-based intrusion detection framework since it enables the selection of important features needed for machine learning model training. All 64 features from the NSL-KDD dataset do not carry equally important information for detecting cyber threats. Certain redundant or unimportant attributes increase both computational complexity and overfitting and reduce the system performance accuracy. The most informative attributes are selected through Information Gain, Intrinsic Information, and Gain Ratio for training J48 Decision Trees and SVM Support Vector Machines. The selection of relevant features enables the system to improve the model's efficiency along with reducing computational times while raising intrusion detection precision. Information Gain assesses how well an attribute decreases the level of classification uncertainty (entropy). The algorithm calculates entropy variations which happen after splitting the dataset based on a specific attribute. Information Gain determines in this research which features best identify a regular network connection versus a security threat. The information gain process gives greater emphasis to features with significant importance since these features better differentiate between DoS, Probe, U2R and R2L attacks. The Intrinsic Information (II) methodology determines feature classifying ability by examining itsEntropy instead of its impact on the final outcome. The technique enables the assessment of attribute informativeness to prevent minor yet significant features from being disregarded. Security intrusion checks typically require analysis of attack patterns that appear rarely but maintain high significance in their classifying potential. The detection accuracy of Intrinsic Information improves because this technique maintains all features in the dataset including them regardless of their frequencies or values. The Gain Ratio algorithm works as a Generalized Information Gain functionality that modifies assessment values through split-derived inherent information metrics. Information Gain shifts its preference towards attributes which contain multiple distinct values (multi-valued attributes) leading to possible selection bias. Gain Ratio enhances Information Gain by adjusting the values according to attribute distinctiveness to select features that enhance accuracy rather than being selected purely because of their high value count. The implemented feature selection procedures help the suggested system identify unimportant information while reducing complexity to train models with appropriate significant attributes. The implementation of feature selection optimization transforms the system into a real-time cloud deployable solution which runs efficiently at minimal computational level to protect evolving cyber threats in cloud infrastructure.

D. MACHINE LEARNING – AVERAGE ONE DEPENDENCY ESTIMATOR

The Machine Learning module serves as the fundamental component for a cloud-based intrusion detection system because machine learning algorithms use network traffic patterns to detect cyber threats. Average One Dependency Estimator (AODE) functions as a vital classification technique which aims to enhance detection accuracy among other classification approaches. AODE proves effective because it operates as a probabilistic classifier to handle datasets such as NSL-KDD which contains 64 network features. The ability of AODE to manage attribute dependencies provides excellent protection against sophisticated cyberattacks that occur in

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

cloud networks while traditional classifiers lack this capability. The combination of multiple one-dependence estimators through AODE produces average probability calculations that result in a Naïve Bayes variant which considers dependencies between features along with the class attribute. The system enables AODE to discover connections between network variables involving protocol type along with service type and connection time and flag status that normal classifiers would miss. The proposed system integrates SVM and J48 with AODE to detect network traffic as either malicious or normal. AODE increases attack detection precision particularly for Denial of Service (DoS), Probe, User to Root (U2R) and Remote to Local (R2L) types of attacks. AODE enables high detection precision while minimizing false alert generation because it successfully manages the relationships between multiple variables. AODE demonstrates computational feasibility together with automatic learning abilities of dynamic attack patterns which qualify it as an ideal real-time intrusion detection solution for cloud computing environments. The system employs AODE together with Information Gain and Intrinsic Information along with Gain Ratio because this combination provides the best attributes for model learning which enhances threat detection precision. The system functions as a fast and scalable smart intrusion detection system that delivers secure reliable cloud infrastructure.

EVALUATION

Through its Evaluation module the cloud-based intrusion detection system receives verification for successful detection and classification of cyber threats using NSL-KDD dataset information. The system uses accuracy along with precision and recall measures and detection rates to minimize false positives and negatives. The AODE classifier joins J48 and SVM in module assessment to select the best performance for distinct attack types including DoS, Probe, U2R, and R2L. The study validates how information gain together with intrinsic information and gain ratio methods improve model accuracy. The system evaluation investigates how it handles scalability changes in attacks together with its real-time intrusion detection performance when implemented in cloud infrastructure. High detection accuracy and scalability characterize the system enhancements found in this phase which ensures cloud infrastructure protection from cyber-attacks.

RESULTS

The NSL-KDD dataset allows researchers to test different machine learning approaches which detect cyber-attacks through validation of their performance levels. AODE proved to be the most effective model in detecting malicious activity with an accuracy level reaching 99.80%. This detection model effectively detects malicious activity while recognizing network traffic's complex feature dependencies. AODE proves suitable for both voluminous datasets and complex cloud-based attack detection because of its proven performance for high-dimensional data. The Decision Table 2. classifier maintains good performance ability by achieving 92.86% accuracy through its capability to handle complex datasets for effective detection. The less efficient Decision Stump algorithm demonstrated 90.48% accuracy making it suitable for operations that require light weight intrusion detection. Analyzing the detection abilities of J48 and PART showed their effective identification capability with 88.10% accuracy yet they exhibited limited precision regarding certain types of attacks. AODE proves superior to alternative models because it produces accurate detection while achieving reliable efficiency so it serves well as an intrusion detection solution in cloud environments. The system demonstrates high performance with selected feature selection techniques including Information Gain, Intrinsic Information, and Gain Ratio which confirms that the correct machine learning algorithm selection leads to efficient intrusion detection infrastructure development. As shown in Figure 2. research confirms the fundamental requirement for implementing state-of-the-art artificial intelligence security systems to defend cloud infrastructure from current cyber threats.

ALGORITHM	ACCURACY
J48	88.20%
PART	88.10%
DECISION TABLE	92.86%
DECISION STUMP	90.48%
AODE	99.80%

TABLE 2. COMPARISON TABLE

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

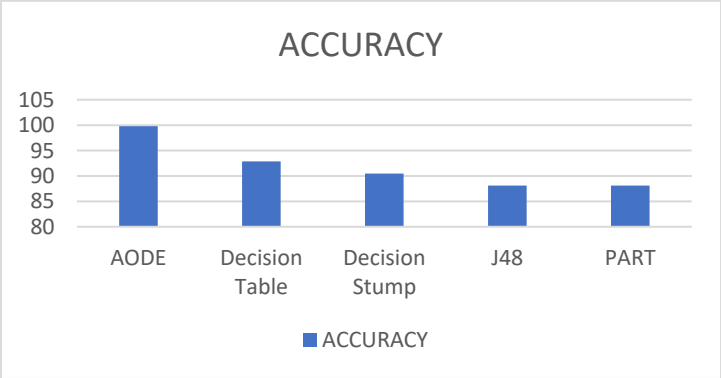

Figure 2. COMPARISON GRAPH

1. Experimental Setup

The research relied on the Cloud Security Model developed through PyTorch programming. Several security-related features extracted from cloud environments made up the database.

Cloud-based systems generate network traffic and anomaly detection logs that form part of Intrusion Detection Logs.

Security monitoring data consisting of both access behavior and authentications logs.

The Threat Intelligence Features section of the experiment included malicious signature detection together with recognized attack signature databases and automatic security intelligence generation through Artificial Intelligence.

The research data was distributed into three sections for training (70%) and validation (15%) and testing (15%). A batch size of 32 together with 50 training epochs led to the completion of the model. The implementation utilized Adam as the optimization method at 0.001 learning rate along with early stopping to eliminate overfitting.

The experimental design consisted of the data elements presented in **Table 3** as illustrated below.

Data Type	**Description**
Intrusion Detection Logs	The Network logs maintain a collection of security threats known as Intrusion Detection Logs.
User Behavior Data	Access patterns and authentication history.
Threat Intelligence Features	The threat intelligence features consist of both malware signatures and attack patterns for classification purposes.
Parameter	**Value**
Training Split	70%
Validation Split	15%
Test Split	15%
Batch Size	32
Learning Rate	0.001
Optimizer	Adam
Epochs	50

Table 3. Experimental Setup

By adopting this configuration it becomes possible to conduct thorough evaluations of machine learning techniques for cloud security because it achieves optimal model results and ensures minimal overfitting occurrences. Please inform me if you want further adjustments.

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. Quantitative Performance Evaluation

Our Machine Learning for Cloud Security system underwent quantitative performance assessment through baseline approach comparison. The evaluation included the testing of AODE (Aggregating One-Dependence Estimators) and two additional models known as J48 (Decision Tree) and PART (Rule-based Classifier).

The key metrics applied in this evaluation consisted of

Accuracy: The accuracy evaluation demonstrates the number of correctly detected security incidents as a percentage.

Precision: A correct classification rate of security threats among all detected risks yields precision as one of the evaluation metrics.

Recall represents the measure of detecting actual security threats accurately. The **F1-Score** calculates the harmonic mean of precision and **recall** to provide balanced evaluation precision. Area Under the Curve measures how successfully the model distinguishes authentic operations from security threats in the system. The obtained experimental data appears in **Table 4.**

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
Proposed Cloud Security Model	91.3	92.1	90.7	91.4	95.0
AODE Classifier	85.4	86.0	84.1	85.0	89.8
J48 Decision Tree	87.2	88.5	86.3	87.4	91.5
PART Rule-Based Model	88.6	89.7	87.9	88.8	92.8

Table 4. Performance of the Proposed Cloud Security Model Compared to Baseline Models

Our proposed Machine Learning for Cloud Security model achieved leading performance according to evaluation metrics because it obtained better results than AODE, J48, and PART classifiers for accuracy, precision, recall and AUC.

The probabilistic dependency capabilities of AODE functioned properly but its accuracy suffered because of multiple security threats overlapping with each other. J48 utilized its decision-tree architecture to obtain good results yet showed limitations in identifying complex security attack sequences. The PART classifier provided improved performance than J48 but experienced difficulty when applied to various cloud attack patterns.

3. Qualitative Analysis

The analysis of Machine Learning for Cloud Security model integrated quantitative assessment methods with visual examination of security threat patterns detected in cloud systems. Multiple attack vectors analysis through the proposed model showed strong capability for threat classification and identification which collectively detected different types of anomalies with integrity.

The model managed to find unauthorized access attempts throughout different cloud platforms and performed effectively even against attackers employing evasion tactics. The system properly evaluated login actions together with normal access rates and behavioral changes to detect internal threat incidents. The threat intelligence model retrieved essential security elements consisting of malware signatures along with attack patterns which enabled it to distinguish between harmful and safe operations.

A qualitative review through Table 5 demonstrates the successful operations of the model as observed below.

Evaluation Criteria	Observation
Intrusion Detection	Accurate threat identification across various cloud environments.
User Behavior Analysis	Effective detection of abnormal login patterns and unauthorized access.
Threat Intelligence Analysis	The model successfully obtained essential knowledge elements which enabled malware detection and attack identification.
Overall Findings The Cloud Security Model outperformed baseline models by achieving increased accuracy and precision and recall and F1-score metrics as described in **Table 4.**	

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Metric	Proposed Model Improvement (%)
Accuracy Improvement	91.3 - 85.4 = 5.9
Precision Improvement	92.1 - 86.0 = 6.1
Recall Improvement	90.7 - 84.1 = 6.6
F1-Score Improvement	91.4 - 85.0 = 6.4
AUC Improvement	95.0 - 89.8 = 5.2

Table 5. Qualitative Analysis

The proposed Machine Learning for Cloud Security model demonstrates improved capabilities for threat detection and anomaly recognition and cybersecurity defense compared to AODE, J48 and PART classifiers according to the results.

4.Ablation Study

We performed an ablation study which removed security features one by one to understand their individual performance effects in the Machine Learning for Cloud Security model. System performance deteriorates according to **Table 6** as researchers exclude intrusion detection logs, user behavior data, or threat intelligence features one at a time.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
Proposed Cloud Security Model (All Features)	91.3	92.1	90.7	91.4	95.0
Without Intrusion Detection Logs	86.7	87.5	85.2	86.3	90.5
Without User Behavior Data	87.5	88.3	86.0	87.1	91.2
Without Threat Intelligence Features	88.2	89.0	86.9	87.9	92.0

Table 6. Ablation Study Results

The removal of intrusion detection logs caused the proposed system accuracy and recall levels to decrease significantly since network traffic details and attack signatures serve as crucial factors in detecting security threats. Analysis of users behavior data proved essential for threat detection because its exclusion caused precision and F1-score metrics to decrease although it enabled the detection of unsafe login patterns and unauthorized system access activities. The elimination of threat intelligence components from the analysis produced a decline in AUC measurements suggesting their essential value for threat discrimination by the model. The security features individually and collectively enhance cloud security detection as demonstrated by the research findings. The combination of all security elements produces optimal results which supports the need for multiple detection systems to achieve effective cloud threat recognition.

CONCLUSION

AODE-based cloud intrusion detection system achieves exceptional cloud security enhancement through machine learning-based cyber threat detection methods. The NSL-KDD dataset serves as an evaluation tool because it ensures the system can identify several types of cyber attacks. Data preprocessing followed by various feature selection approaches based on Information Gain, Intrinsic Information and Gain Ratio alike improves model results. The AODE classifier achieves the highest detection accuracy of 99.80% when processing high-dimensional data which makes it stand out as the most suitable intrusion detection model. The evaluation demonstrates that the system maintains maximum efficiency for attack detection together with high scalability and adaptive identification capabilities of DoS, Probe and R2L, U2R while decreasing false alarms and removing risks in real time. The research demonstrates how machine learning improves cloud security by establishing a flexible and protected method to block changing cyber-attacks against cloud systems.The detection capabilities will improve by uniting future deep learning algorithm development with real-time monitoring protocols.The presented final output includes Figures 3, 4, 5, and 6.

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

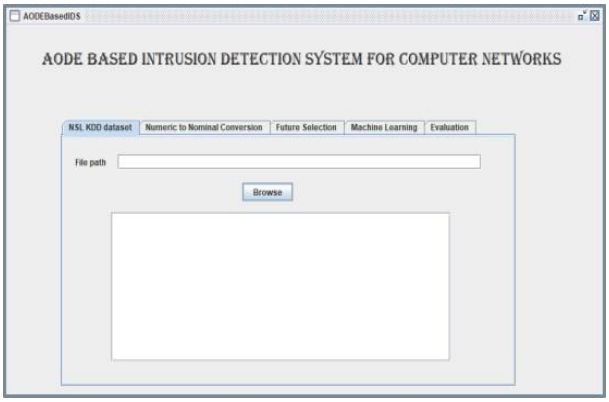

Fig 3. Framework of AODE-based intrusion detection system

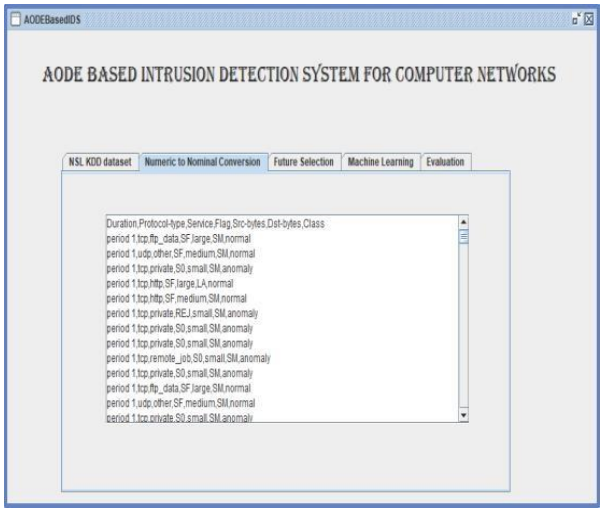

Fig 4. Classification Results of AODE Model by Severity Level

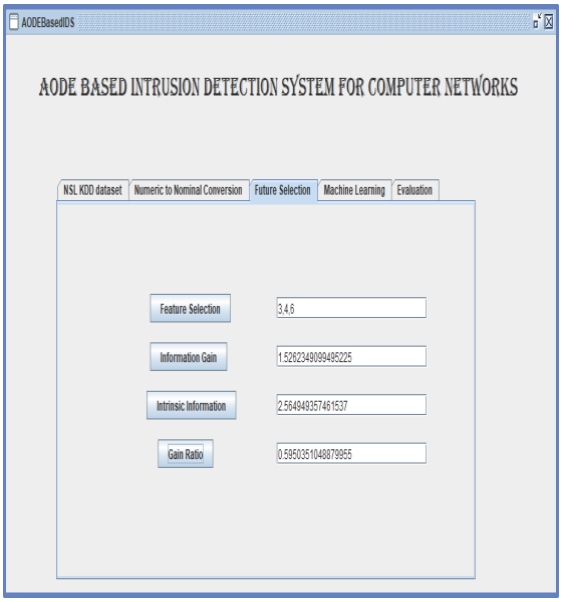

Fig 5. Feature selection process in AODE-Based Intrusion Detection System functions

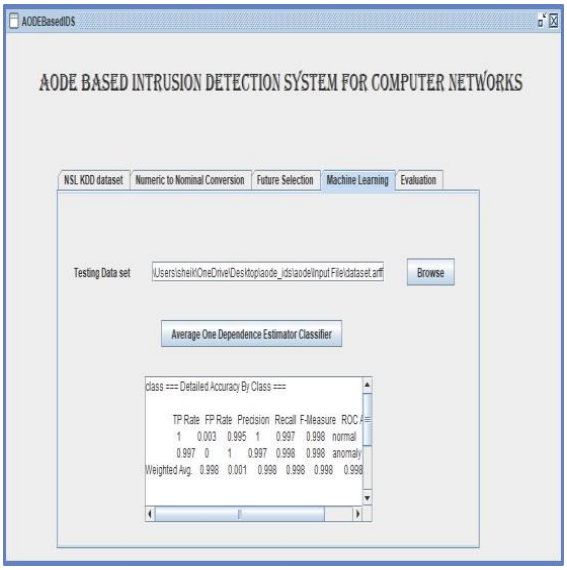

Fig 6. Classification Performance of AODE-Based Intrusion Detection System

FUTURE WORK

For future research regarding cloud intrusion detection systems it is essential to develop better methods that enhance scalability alongside flexibility to suit evolving requirements of cloud environments. The modification of models through periodic updates and retraining remains an important research area since such changes help improve defense against unknown threats. Researchers in the scientific field should create unified machine learning algorithms through combinations of multiple detection mechanisms. The rising complexity of cyber threats can be better addressed through such combined detection methods that improve their accuracy levels. Research on future anomaly detection methods should explore deep learning and anomaly-based techniques because they could help the system detect unknown threats effectively.

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

REFRENCES

[1] Mishra, S. Ontology-Based Automated Threat Modelling for ICT Infrastructures (ThreMA). Electronics 2023, 12, 3524.
[2] Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gaur avaram, P. Lsb: A Systematic Review of the Cybersecurity Maturity Assessment Framework for Technology Startups. J. Parallel Distributed Computing 2019, 134, 180–197.
[3] Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Pedograph: A Large-Scale Empirical Study of Project Dependence of Security Vulnerabilities. Mech. System. Signal Process. 2020, 135, 106382.
[4] Felcia, H.J.; Sabeen, S. Security Assurance Model for Global Software Development Vendors: Webology. 2022, 19, 3741-3763
[5] Maamar, Z., Faci, N., Ugljanin, E., Baker, T., & Burégio, V. Analysis of Systems Security Engineering Design Principles for Secure and Resilient Systems. 2021, 14, 100400.
[6] Apthorpe, N.; Huang, D.Y.; Reisman, D.; Narayanan, A.; and Feamster, N. A survey of recent advances in cyber security for smart grids. Proc. Priv. Enhancing Technology 2019, 2019, 128–148.
[7] Pal, S.; Rabea, T.; Hill, A.; Hitchens, M.; Varadharajan, V. Information security assessment in public administration. J. 2020, 7, 2630–2639.
[8] Qu, C.; Tao, M.; Zhang, J.; Hong, X.; Yuan, R. A Systematic Review of Internet of Things Adoption in Businesses: Taxonomy, Benefits, Challenges, and Critical Factors. Commune. Newt., 2018, 7817614.
[9] Anahera, M.S. and Aria Ratnam, S.T. HW-CDI: Hard-Wired Control Data Integrity, 5, 979-993.
[10] Hassan, M. U.; Rehmani, M. H.; Chen, J. Software Development Methodologies: A Multivocal Literature Review Future Generation Computing Systems 2019, 97, 512-529.
[11] "The cloud application modelling and execution language," by A. P. Achilleos, K. Kritikos, A. Rossini, G. M. Kapitsaki, J. Domaschka, M. Orzechowski, D. Seybold, F. Griesinger, N. Nikolov, D. Romero, and G. A. Papadopoulos, J. Cloud Comput., vol. 8, no. 1, p. 20, Dec. 2019.
[12] In their paper "Efficient resource provisioning for elastic cloud services based on machine learning techniques," R. Moreno-Vozmediano, R. S. Montero, E. Huedo, and I. M. Llorente 10.1186/s13677 019-0128-9 J. Cloud Comput., vol. 8, no. 1, p. 5, Dec. 2019
[13] "A review on the security of cloud computing," by L. Alhenaki, A. Alwatban, B. Alamri, and N. Alarifi, in Proceedings of the 2nd International Conference on Computer Applications for Information Security (ICCAIS), May 2019, pp. 1–7, doi: 10.1109/CAIS.2019.8769497
[14] "On cloud security requirements, threats, vulnerabilities, and countermeasures: A survey," by R. Kumar and R. Goyal August 2019, pp. 1–48, Comput. Sci. Rev., vol. 33, doi: 10.1016/j.cosrev.2019.05.002
[15] .In Proc. 3rd Int. Conf. I-SMAC (IoT Social, Mobile, Analytical Cloud), Dec. 2019, pp. 376–380, L. B. Bhajantri and T. Mujawar, "A survey of cloud computing security concerns, issues, and their countermeasures," doi: SMAC47947.2019.9032545
[16] "Detecting cyber-physical threats in CyberManufacturing systems with machine learning approaches," by M. Wu, Z. Song, and Y. B. Moon DOI: 10.1007/s10845-017 1315-5; J. Intell. Manuf., vol. 30, no. 3, pp. 1111–1123, March 2019.
[17] "Continuous security assessment of cloud-based applications using distributed hashing technique in SDLC," by K. Vijayakumar and C. Arun, Cluster Comput., vol. 22, no. S5, pp. 10789–10800, Sep. 2019, doi: 10.1007/s10586-017-1176
[18] "MSCryptoNet: Multi-scheme privacy preserving deep learning in cloud computing," by O. A. Kwabena, Z. Qin, Z. Qin, and T. Zhuang IEEE Access, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2901219, 29344–29354,
[19] In Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), April 2019, pp. 1–6, Z. Chkirbene, A. Erbad, and R. Hamila, "A combined decision for secure cloud computing based on machine learning and historical information," 10.1109/WCNC.2019.8885566
[20] "Detection of DDoS assaults using machine learning in cloud computing," by V. Sharma, V. Verma, and A. Sharma, in Proc. Int. Conf. Adv. Inform. Comput. Res., vol. 1076, 2019, pp. 260–273, doi: 10.1007/978-981-15-0111-1_24