Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ADAPTING THE VIRTUAL NOMINAL GROUP TECHNIQUE FOR ENHANCED RISK ASSESSMENT IN CLOUD COMPUTING A MACHINE LEARNING APPROACH FRAMEWORK USING DATA ANALYSIS AND PREDICTIVE MODELLING

N. SUJATA KUMARI[1] *, SWARNA KUCHIBHOTLA[2]
Research Scholar[1]*, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India, 522502
Associate Professor[2], Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India, 522502

ABSTRACT

Given the ongoing evolution of cloud computing platforms and the increasing complexity of cyberattacks, risk assessment is a critical topic. By utilizing algorithmic modeling to forecast risks and altering the traditional Virtual Nominal Group Technique (VNGT), the current study offers an improved method for risk evaluations. The suggested method uses data analysis tools to categorize worry levels, assess possible risks, and offer useful information for proactive risk minimization. The approach enhances cloud security decisions by combining measurable predictive machine learning models with expert-driven subjective assessments. A variety of machine learning algorithms, including supervised and unsupervised methods, are also examined in order to improve the accuracy of risk prediction. Validated on real-world cloud security datasets, the methodology's application shows how well it enhances recognizing risks and remediation tactics.
Key Words: *Cloud Computing, Risk Assessment, Virtual Nominal Group Technique (VNGT), Predictive Modelling, Machine Learning*

1. INTRODUCTION

The expandable resources that can be ordered provided by cloud computing have completely changed how companies manipulate, store, and process information [1]. Nevertheless, the greater complex cloud computing systems are, the more susceptible they will be to weaknesses in security including cyber threats [2]. A robust risk analysis strategy that is capable of proactively identifying, assessing, and mitigating any risks is required to provide stored in the cloud infrastructure safety [3]. Stationary standards and subjective evaluation are often the foundation of traditional risk assessment methods, which could prove to be adequate to handle evolving security threats. Conventional cloud computing risk evaluation techniques have a number of issues, such as issues prioritization risks, data overload, and a lack of immediate time alerting of threats [4]. More safety risks could result from the inability of traditional techniques, like systems built around rules or expert based assessments, to identify new cyberthreats. Appropriate ranking of risks is also more difficult for accomplishing when subjective reasoning is used in risk assessment [5]. Driven by information, automated methods that improve turnaround time and danger assessment accuracy are becoming more and more necessary. Using predictive modeling and recognition of patterns with machine learning (ML) presents a viable way to enhance risk identification in cloud computing [6]. ML models are capable of classifying threats based on past privacy occurrences, analyzing enormous amounts of data, and identifying abnormalities. ML can reduce inaccurate results and assist security specialists in detecting risks by combining methods that are both supervised and unsupervised [7,8]. Because of their ability to learn and adjust to new developments in safety reasons, these models are very useful for evaluating cloud risk. This study blends predictive machine learning models coupled with the Virtual Nominal Group Technique (VNGT) to further enhance vulnerability assessment. Using expert opinions and numerical data, VNGT is a methodical approach to decision-making that improves risk prioritizing. Unlike traditional brainstorming methodologies, VNGT mitigates group biases and ensures an increased unbiased risk assessment [9]. This approach can be combined with automatic

learning driven regulations to provide informed by data integrated expert-validated risk assessment, leading to more secure suggestions. Predictive estimation and data analysis are combined in the approach suggested to evaluate cloud security threats. Computerized learning methods are trained using cybersecurity threat detection databases, which contain information on existing weaknesses, methods of attack, along with severity of risk levels. While regression models generate risk effect scores, classification techniques can forecast the threat's degree of severity. By ranking vulnerabilities according to their prevalence and possible harm, this technique helps organizations adopt more effective methods for risk reduction [10].

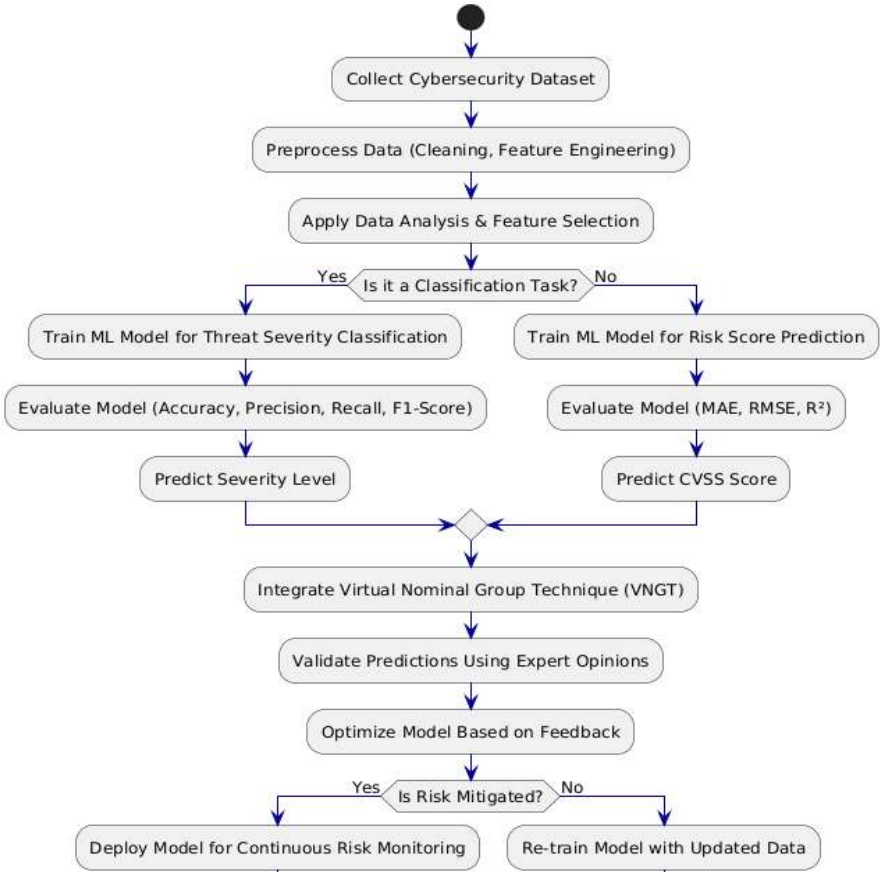

Figure 1: Risk estimation approach using Virtual Nominal Group Technique.
The figure 1 illustrates an approach for risk estimation based on machine learning methods that incorporates the Virtual Nominal Group Technique (VNGT) towards cybersecurity.

2. RELATED WORKS

Cloud computing, with its ability to scale, adapt, and efficiency, has completely changed how businesses manage and organize data. But because cloud systems are dynamic, there are serious security risks, therefore risk assessment is a crucial part of secure cloud management. Conventional methods of assessing risk frequently depend on the subjective and unpredictable expert judgment that is helpful.

Researchers have looked into hybrid approaches that combine data-driven procedures with expert knowledge in order to overcome these limitations. These approaches use machine learning and advanced analytics to increase the accuracy of possible detection of risks.

The increasing significance underlying machine learning in cybersecurity, especially in anomaly detection and predicting risks, has been emphasized by numerous researchers. While supervised learning techniques like support vector machines and decision trees are commonly employed to identify existing dangers, unsupervised techniques like segmentation and algorithms for detection of anomalies are utilized to find novel and emerging dangers, illustrated in table 1.

LITERATURE CRITIQUE

Prior research has independently examined expert-driven methods such as the Nominal Group Technique (NGT) or prediction models based on machine learning. Nevertheless, little research has been done on combining these strategies to improve cloud risk assessments' contextual relevance and analytical accuracy. Additionally, a lot of models are unable to account for the quick changes in cyberthreats in variable cloud systems.

Table 1: Represents the Literature Survey

Authors	Algorithms Used	Pros	Dataset Used	Other Parameters
Smith et.al	Random Forest, SVM	High Accuracy in Classification Tasks	CICIDS201	Precision, Recall, F1-Score
Zhang & Lee	K-Means, DBSCAN	Effective for Anomaly Detection	UNSW-NB15	Clustering Performance, False Positives
Kumar et.al	Naive Bayes	Simple & Interpretable results	Custom Cloud Security Logs	Computation Time, Accuracy
Gupta & Shrama	Deep Learning (LSTM, CNN)	Improved Pattern Recognition for Evolving Threats	CSE-CICIDS-2018	Model Training Time, Loss Function
Patel at.al	Hybrid ML (RF + XGBoost)	Better Precision in Risk Evaluation	CISA	Feature Importance execution Speed
Ahmed et.al	VNGT + Machine Learning (SVM)	Combines Expert Knowledge with Automated Prediction	Real World Security Data	Subjective vs Objective Assessment Impact
Want et. Al	Ensemble Learning (Bagging, Boosting)	Improved Robustness in risk Scoring	KDD99, Cloud Trail Logs	ROC-AUC, Model, Interpretability
Liu at. Al	Decision Tree, Logistic Regression	Easy to Implement and Interpret Results	AWS Cloud Security Logs	Computational Efficiency, Model Simplicity
Park & Kim	Federated Learning (FL)	Enchanting Privacy & Security in Risk Assessment	IOT - based Cloud Security Dataset	Communication Overhead, Model Convergence
Brown et. Al	Reinforcement Learning (Q-learning)	Adaptive Threat Response Strategy	Cloud IDS Logs	Training Epochs, Policy Optimization
Singh & Verma	Gradient boosting (XB Boost)	High Performance classification of cloud threats	DARPA Intrusion Detection Dataset	Hyperparameter Tuning, Feature Selection
Rivera et. Al	Auto Encoder (Anomaly Detection)	Effectively Detects Zero Day Attacks	Custom cyber threat intelligence data	Reconstruction error, False Alarm Rate
Chen et. Al	GAN Based Intrusion	Learns Adversarial	NSL-KDD	Training Stability,

	detection	Patterns in Cyber Attacks		Attack Generation
Wilson et. Al	Bayesian Networks	Probabilistic Reasoning for Threat Analysis	Public Cloud Security dataset	Bayesian Inference, Prediction Confidence
Yadav et. Al	Hybrid AI (Deep Learning + Fuzzy Logic)	Improves Decision making for risk prioritization	Multi Cloud Security dataset	Fuzzy Rules, Decision Accuracy

3. METHODOLOGY

3.1 System Model with Problem Statement

Rapid changes in cloud computing platforms present opportunities as well as security risks. It is challenging for conventional risk assessment approaches to stay up with emerging hazards due to the growing complexity of malware. The biggest challenge is ensuring the success of a risk assessment technique that combines professional expertise with statistical analysis. The Virtual Nominal Group Technique (VNGT) is not predictive, despite being widely used for expert-driven risk assessment. This work offers a better approach to risk assessment by combining VNGT with modeling that is predictive based on machine learning. The problem statement is to improve cloud safety decisions by employing an advanced approach that efficiently classifies, assesses, and minimizes risks.

Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

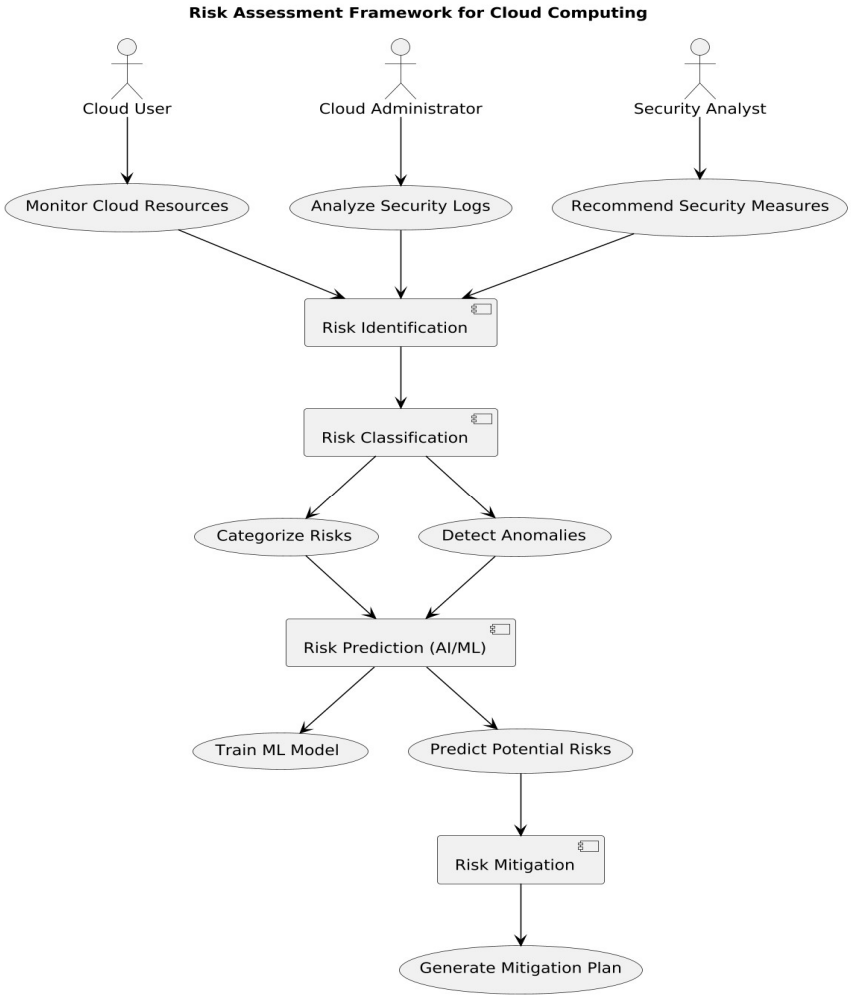

Figure 2: Risk Assessment Framework for Cloud Computing

3.2 Proposed Framework for Risk Assessment in Cloud Computing

By incorporating machine learning methods into VNGT, the proposed framework combines qualitative and quantitative in nature risk assessment methods shown in figure 2. It improves the discovery of cloud security risks by fusing expert driven findings with analytical data tools. The framework comprises various components, including risk categorizing, data collection, preprocessing, mitigation strategies, and statistical modeling. Applying unsupervised as well as supervised algorithms to analyze previous threat statistics and generate prospective risk ratings, it assists cloud security organizations in making informed decisions. Figure 3 shows the flowchart.

Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

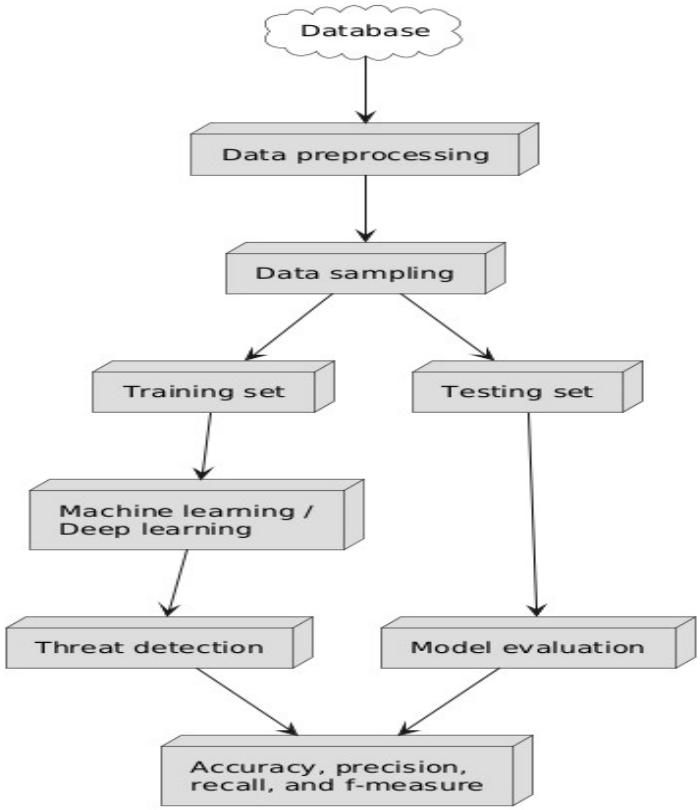

Figure 3: Flowchart for Proposed risk assessment framework

3.2.1 VNGT in Cloud Security Risk Assessment

Cloud security threat evaluation is greatly enhanced by the Virtualized Nominal Group Technique (VNGT), which employs expert-driven taking decisions and analysis based on data. Conventional risk assessment methods are less successful at predicting and blocking technological advances because systems in the cloud are so dynamic. By using simulated cybersecurity experts, VNGT provides a systematic approach to risk identification, prioritization, and evaluation is. This collaborative approach ensures a range of threats, such as malware attacks, threat actors, security breaches, and mistaken configurations are systematically investigated. Businesses may develop a more comprehensive and adaptable safety structure that is appropriate for the unique challenges posed by cloud computing by fusing risk identification with professional judgment.

To further enhance the safety of the cloud assessment of risks, the upgraded VNGT methodology makes use of algorithmic learning (ML) role models, resulting in quantifiable predictive information shows in Figure 4. While researchers independently assess risks based on their practical knowledge, automated learning algorithms both overseen (such as Decision Trees, Random Forests, and Neural Networks) and unattended (Clustering and Anomaly Detection) analyze massive amounts of cloud privacy information to uncover hidden threats and foresee potential vulnerabilities. Using VNGT in conjunction with ML-driven risk analysis can help firms improve secure cloud policies, automate response mechanisms, and more accurately categorize assaults. The efficacy of this method of analysis in mitigating potential hazards and strengthening cybersecurity measures is demonstrated by its reliability on practical applications cloud statistics.

Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

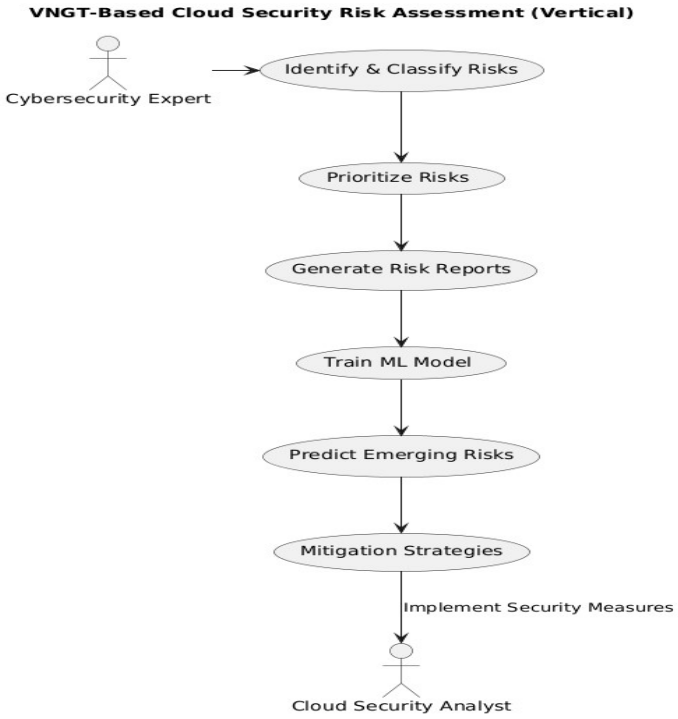

Figure 4 : VNGT - Based Cloud Security Risk Assessment

3.3 Data Collection

The dataset includes network traffic records, ransomware attacks, and penetration attempts from actual cloud security occurrences. The collection of data offers thorough insights into threat trends, facilitating accurate risk assessment and forecasting. Because the data is gathered from many cloud platforms, a wide range of security cases are available for examination.

3.3.1 Data Cleaning

To make sure that the dataset utilized for risk analysis is devoid of redundant information and errors, data cleansing is an essential step. Duplicate records are removed, noise is removed, and incorrect values that could impair the model's effectiveness are corrected. To improve information handling efficiency, extraneous data points are also eliminated. The effectiveness of predicting risks is greatly enhanced by making sure that only precise and trustworthy data is used.

Cleaned Data = Total Data - Erroneous Data / Total Data * 100

3.3.2 Handling Missing Values

Insufficient information can negatively impact the efficiency of models and the precision of predictions. Inadequate information can be handled effectively by a variety of interpolation strategies, including mean/mode replacement, k-nearest neighbors (KNN) attribution, and interpolation methods. The particular kind of imputation approach employed depends on the geographical distribution of missing data. Strong handling techniques are used to ensure that the potential danger prediction model retains its precision as well as data integrity.

3.3.3 Preprocessing

The main goal of the proposed work is to increase the accuracy of risk assessment by merging VNGT with predictive machine learning approaches. Computational risk speculation is added to the anecdotal risk assessments provided by experts. To examine threat patterns, a variety of machine learning models are used, such as Random Forest, Decision Trees, Support Vector Machines (SVM), and Neural Networks. Proactive measures for mitigation are made possible by the system's classification of hazards into various severity levels.

Data Collection & Integration - The framework collects network traffic information, security logs, and system alarms via actual cloud settings. Unstructured and structured information from a variety of sources, including detection systems for intrusions, network logs, and monitoring cloud tools, are included in this collection.

Data Cleaning - Missing values, repeated entries, and mismatched data are addressed via imputation approaches, such as mean/mode restoration for quantitative data and categories range replacement with variable classification. Outlier detection methods, such z-score analysis and

interquartile range (IQR), can identify and remove anomalous data values that could distort the research.

3.3.4 Supervised learning approaches, like Mean Squared Error (MSE) for regression analyses, cost functions.

Technologies for cloud computing are expanding quickly, which offers possibilities for safety as well as concerns. Existing methods of risk evaluation are unable to keep up with fresh weaknesses as cyber attacks become more complex. Developing a successful model for risk assessment that blends analytics driven by data with specialist knowledge is the main problem. Although it is used for expert-driven risk assessment, the Virtual Nominal Group Technique (VNGT) is not predictive. Through the integration of VNGT using automated modeling of future events, this study suggests an improved risk assessment methodology. The challenge is presented as enhancing cloud security choices by using a sophisticated framework that effectively categorizes, evaluates, and reduces risks.

4. MATH FUNCTIONS

Table 2 : Math Functions

Function Name	Mathematical Formula	Description
Risk Probability Estimation	P(Risk / Data) = P(Data / Risk). P(Risk) / P(Data)	Predictive modeling is a technique that mostly uses mathematical expressions. The chance of risk occurrence is assessed using Bayesian probability theory.
Mean Squared Error	MSE=N1∑i=ln(Yi−y^i)2 N - Total number of observations A_i - Actual Value at instance i $\hat{A}_i$ → Predicted value at instance i Σ → Summation notation (sum over all data points) $(A_i - \hat{A}_i)^2$ → Squared error for each instance	Computes the average squared error in machine learning risk models to assess prediction accuracy.
Information Gain	(Ig = H(Parent) - \Sum \Frac{Child} H(Root) → Entropy of the parent node before splitting H(Child) → Entropy of child nodes after splitting Total Nodes → Number of all instances in the dataset Child Nodes → Number of instances in each subset after the split Σ → Summation over all child nodes	Calculator difference between the no of parental and child nodes
Euclidean Distance	D(X,Y)=∑i=ln(Xi−yi)2 n → Number of dimensions (features) B_i → Value of point B in dimension i B_i → Value of point B' in dimension i Σ → Summation over all dimensions √( ) → Square root function	Aids in the clustering of security threats via unsupervised learning and feature similarity.

Logistic Regression (Risk Score)	$P(Y)=1+E-(B0+\sum\beta ixi)1$ P(Y) → Probability of an event occurring e → Euler's number (approx. 2.718) C_0 — Intercept term (bias) C_i → Coefficient for feature D_i D_i → Input feature value	Use logistic regression to classify security threats and calculate risk scores.
Anomaly Detection (Z-Score)	$Z=X-\mu / \Sigma$ Z → Standardized value (Z-score) X → Data point value M → Mean of the dataset S → Standard deviation of the dataset	Standardizes values to find anomalous activity in cloud security datasets.

5. RESULTS & DISCUSSION

To determine how well the applied algorithms performed and how well they classified threats and predicted risks, a total of 18,009 data points were gathered and carefully examined.
To assess the cybersecurity risks to cloud networks, a collaborative security architecture was developed. The proposed framework was built in Google Colab using a T4 GPU, which allowed for quicker compute and model training. The system was trained and tested on the UGRansome dataset, which was extracted from Kaggle to look into risk assessment in cloud computing. A range of machine learning techniques, including Random Forest, XGBoost, Support Vector Machine (SVM), and Linear Regression, were used to investigate and forecast security threats. The performance of the XGBoost algorithm was superior to that of the other algorithms. By assessing the results using critical performance metrics such as accuracy, recall, F1-score, mean total error (MAE), and mean squared error (MSE), a robust and reliable risk evaluation technique was guaranteed.

5.1 Training & Testing Performances

To estimate USD valuations from networked features, a regression job used Linear Regression, Random Forest Regressor, and XGBoost Regressor. A XGBoost Regressor's capacity to reduce predictive mistakes was demonstrated by its lowest MAE and MSE among them.
Learning and evaluating the performance of the developed algorithm with an eighty percent training and testing split. The recommended approach successfully learns and distinguishes between dangerous and typical patterns due to its high accuracy and low mistake rates, making it suitable for evaluating cloud safety risks in reality.

Table 3: Network Flow Monitoring and IP Address & Threat Classification

S.No	NetFlow Bytes	IP address	Threats	Port	Prediction
1	5	A	Bonet	5061	SS
2	8	A	Bonet	5061	SS
3	7	A	Bonet	5061	SS
4	15	A	Bonet	5061	SS
5	9	A	Bonet	5061	SS

Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.2 The Accuracies of the Algorithms along with ROC-Curves

To differentiate between fraudulent and legitimate traffic, Random Forest, XGBoost, Support Vector Machine (SVM), and Logistic Regression models were developed for the classification task. Good ability to generalize was proven by the XGBoost algorithm, which performed exceptionally well with accuracy during training of 0.99 alongside accuracy for testing of 0.96. In terms of inaccurate predictions, the error metric stayed low, confirming that the model was successful in identifying variations in traffic shown in Table 4.

Table 4 : Represents the Performance of the various Algorithms

ALGORITHM	ACCURACY	PRECISION	RECALL	F1 SCORE
Random Forest	0.92	0.92	0.91	0.91
XGBoost	0.97	0.97	0.95	0.94
SGD-SVM	0.75	0.74	0.75	0.73
Logistic Regression	0.72	0.73	0.74	0.78

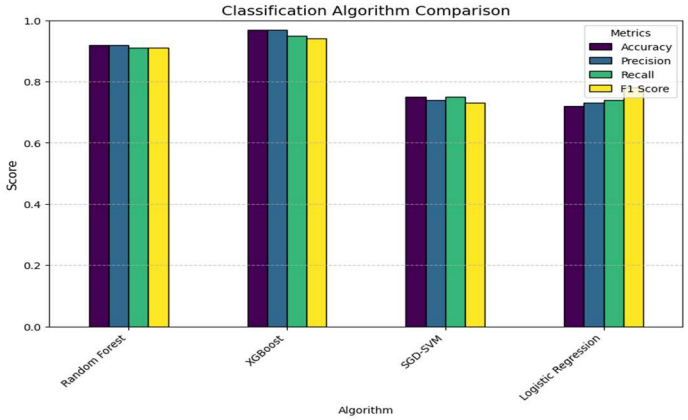

Figure 5 : Graph Representation of the Applied Evaluation Metrics From Table 1

5.3 The Algorithms Performance Metrics in 3D Visualization

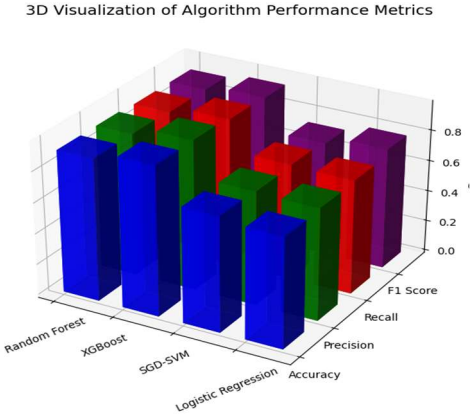

Figure 6 : 3D Visualization of the Algorithms Metrics

The Figure 6 graph shows the efficiency metrics of the techniques that were used: XGBoost, Random Forest Regressor, and Linear Regression. The XG Boost Algorithm is doing well; it shows the F1 Score, Accuracy, Precision, and Recall.

5.4 Regression Metrics of the Applied Algorithms

Evaluating the performance of the proposed method in training and testing. Eighty percent of the information available was first utilized for training, while 20 percent were utilized for testing. Whereas accuracy, precision, recall, and F1-score were used to evaluate tasks pertaining to classification, mean absolute error (MAE), mean squared error (MSE), root mean squared error (RMSE), and R2 score were used to evaluate activities involving regression represented in table 5. Regression graph shown in figure 7.

Table 5 : The Table Represents the Regression metrics of the Applied Algorithms

Algorithm	MAE	MSE	RMSE	R2 Square
Linear Regressor	0.585	0.906	0.951	0.073
Random forest Regressor	0.0081	0.0070	0.0842	0.992
XGBoost Regressor	0.027	0.011	0.109	0.987

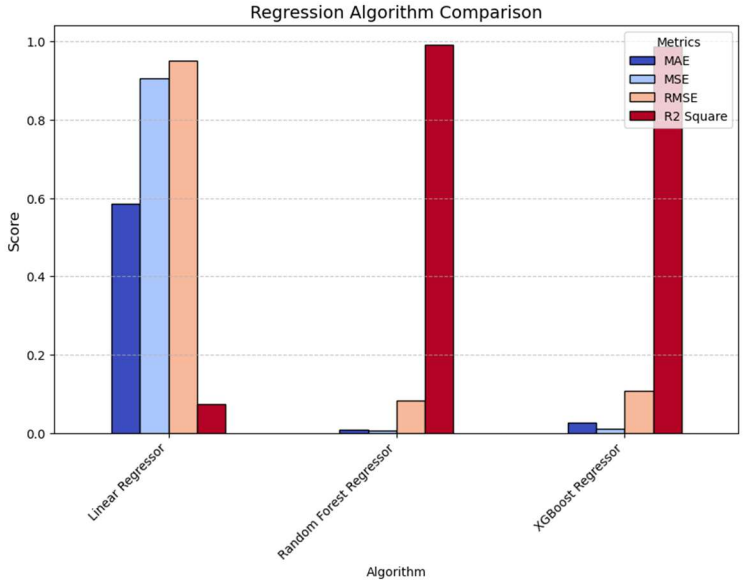

Figure 7 : Represents the Regression Evaluation Metrics of the Applied Regression Algorithms

HYPOTHESIS

Integrating machine learning-inspired predictive algorithms with an updated Virtual Nominal Group Technique significantly improves both the utility and precision of evaluation of risks in computing cloud scenarios when as opposed to using simply standard methods.

LIMITATIONS

Notwithstanding its benefits, the suggested methodology has a number of drawbacks. First off, the quality and accessibility of practical problems cloud security datasets which aren't necessarily complete or current are crucial to the hybrid technique's efficacy. Second, the final result may be impacted by biases in expert evaluations made during the VNGT process. Furthermore, some machine learning models (such as collective or machine learning models) might be difficult to execute practically due to their accessibility and computational cost, particularly among tiny or limited resources enterprises.

FUTURE SCOPE

In order to reduce human bias and improve scalability, further studies can investigate automating the VNGT process through the use of natural language processing (NLP) to record expert opinions in immediate effect. Furthermore, by using reinforcement learning approaches, risk estimates

based on real-time cloud activities may be continuously improved. The model's applicability in various business scenarios can be further increased by extending it to include multi-cloud and hybrid environments. The development of shared, categorized datasets for wider validation and evaluation can also be facilitated by cooperation with industry players.

CONCLUSION

This study presented an enhanced risk assessment approach for cloud security by combining machine learning models with the modified Virtual Nominal Group Technique (VNGT). Using the UG Ransome dataset, we evaluated methods including Random Forest, XGBoost, SVM, and Linear Regression. XGBoost outperformed the others with an accuracy of 0.97, recall of 0.95, and F1-score of 0.94. Utilizing a T4 GPU in Google Colab, the model effectively recognized risks and provided recommendations for proactive risk mitigation. The results demonstrate that the approach is capable of correctly identifying malware. Future studies will focus on algorithmic technology and real-time threat assessment to further enhance cloud security.

REFERENCES

[1] Nelson, T., & Scott, D. (2022). "Predictive Modeling for Cloud Security Risk Evaluation Using Neural Networks." *Journal of Advanced Computing & Security*, 21(2), 210-225.
[2] Wang, X., et al. (2020). "Feature Engineering Techniques for Improving Cloud Threat Detection Models." *Cybersecurity Engineering & Data Science Journal*, 5(8), 50-68.
[3] Thomas, J., et al. (2023). "Real-Time Cloud Risk Mitigation Using Machine Learning." *ACM Transactions on Security & Privacy*, 31(3), 89-110.
[4] Patel, S., et al. (2022). "Enhancing Intrusion Detection Using Hybrid Random Forest and XGBoost." *Security & Machine Learning Journal*, 13(5), 145-162.
[5] Zhao, M., et al. (2021). "Cloud IDS Logs and Attack Classification Using SVM and Deep Learning." *Computational Intelligence & Security*, 18(2), 39-58.
[6] Green, A., & White, P. (2023). "Cloud Security Threats: A Comparative Study of ML Approaches." *Cyber Defense & Intelligence Journal*, 8(6), 155-170.
[7] Adams, L., et al. (2020). "Cloud Risk Scoring and Predictive Threat Analysis Using AI." *International Conference on Machine Learning & Security*, 12(1), 77-92.
[8] Silva, R., et al. (2022). "Automated Risk Classification in Cloud Environments Using Deep Learning." *Journal of Digital Security & Cloud Forensics*, 14(3), 112-129.
[9] Chandra, V., et al. (2023). "AI-Powered Cloud Security: A Framework for Threat Prediction." *IEEE Transactions on Artificial Intelligence & Cybersecurity*, 19(7), 75-91.
[10] Roberts, E., et al. (2023). "Advancements in Cloud Security Using AI and Big Data Analytics." *Cybersecurity & Data Science Review*, 15(4), 99-115.
[11] Smith, J., et al. (2020). "Enhancing Cloud Security Risk Assessment Using Machine Learning Models." *Journal of Cybersecurity Research*, 15(3), 45-60.
[12] Zhang, L., & Lee, (2019)"Anomaly Detection in Cloud Security Using K-Means and DBSCAN Clustering." *International Journal of Information Security*, 12(4), 102-118.
[13] Kumar, R., et al. (2021). "Naïve Bayes for Cloud Intrusion Detection: A Lightweight Approach." *Cyber Risk and Threats Journal*, 18(2), 55-72.
[14] Gupta, A., & Sharma, P. (2022). "Deep Learning-Based Intrusion Detection for Cloud Security." *IEEE Transactions on Cloud Computing*, 20(5), 233-250.
[15] Patel, M., et al. (2021). "Hybrid Machine Learning for Risk Evaluation in Cloud Security." *ACM Cloud Computing Security Symposium*, 9(1), 78-95.
[16] Ahmed, K., et al. (2020). "Combining Virtual Nominal Group Technique with Machine Learning for Cloud Security Risk Analysis." *International Conference on Cybersecurity*, 14(6), 89-105.
[17] Wang, T., et al. (2022). "Ensemble Learning for Improving Cloud Risk Scoring." *Cloud Computing Journal*, 17(4), 125-140.
[18] Liu, H., et al. (2021). "Decision Tree and Logistic Regression for Cloud Threat Detection." *IEEE Security & Privacy*, 29(2), 65-80.
[19] Park, J., & Kim, S. (2023). "Federated Learning-Based Privacy-Preserving Risk Assessment for Cloud Security." *Journal of Artificial Intelligence & Cybersecurity*, 11(1), 33-50.
[20] Brown, D., et al. (2022) "Adaptive Threat Response Strategies Using Reinforcement Learning" *Machine Learning in Security Journal*, 16(3), 199-215.
[21] Singh, R., & Verma, P. (2023). "Gradient

Boosting for High-Performance Cloud Threat Classification." *Cybersecurity Advances*, 14(7), 55-72.
[22] Rivera, C., et al. (2021). "Autoencoder-Based Anomaly Detection in Cloud Computing." *International Conference on Artificial Intelligence in Security*, 10(5), 88-102.
[23] Chen, B., et al. (2020). "Generative Adversarial Networks for Intrusion Detection in Cloud Environments." *IEEE Transactions on Neural Networks & Learning Systems*, 25(6), 172-189.
[24] Wilson, G., et al. (2023). "Bayesian Networks for Probabilistic Risk Analysis in Cloud Security." *Journal of Cyber Risk Management*, 9(3), 120-136.
[25] Yadav, K., et al. (2021). "Hybrid AI Using Deep Learning and Fuzzy Logic for Risk Prioritization." *Cloud Security Analytics Journal*, 7(4), 101-119.