ISSN: 2182-2069 / E-ISSN: 2182-2077

An Innovative AI-driven Autotuning and Autoselection for Intelligent Financial Cloud Security

Dr. Trupti Manish Rathi[1*], Dr. Ashutosh Panchbhai[2], Dr. Arvind Kumar Pandey[3], Kshipra Jain[4], R. Hannah Jessie Rani[5], and Dr. Anita Sable[6]

[1*]Assistant Professor, NICMAR University, Pune, India. truptimanish1504@gmail.com, https://orcid.org/0000-0002-8963-6333

[2]Assistant Professor, Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR); Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University) (SIU), Pune, India. ashutosh.panchbhai@symlaw.ac.in, https://orcid.org/0000-0003-4799-7250

[3]Associate Professor, Department of Computer Science & IT, ARKA JAIN University, Jamshedpur, Jharkhand, India. dr.arvind@arkajainuniversity.ac.in, https://orcid.org/0000-0001-5294-0190

[4]Faculty, Department of ISME, ATLAS SkillTech University, Mumbai, Maharashtra, India. kshipra.jain@atlasuniversity.edu.in, https://orcid.org/0009-0007-3240-3428

[5]Assistant Professor, Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India. jr.hannah@jainuniversity.ac.in, https://orcid.org/0000-0002-5449-104X

[6]Assistant Professor, Symbiosis Law School, Nagpur, India. dranitasable01@gmail.com, https://orcid.org/0000-0002-6537-9854

Received: May 29, 2025; Revised: July 15, 2025; Accepted: August 13, 2025; Published: August 30, 2025

Abstract

Data from the financial cloud network monitoring is dispersed and Innovative. There can be intermittent appearances of signals to monitor the cloud or vary in significance and clearness. As a result, machine learning (ML) techniques that are adjusted to a particular data set cannot be sufficient for very long. A model's accuracy can decrease as a result of changes in the qualities and input data throughout time. For this reason, it is frequently necessary to use distributed learning with creative model selection. However, there are several drawbacks to ensemble machine learning. These include the necessity of constant training, the need for high amounts of processing power and big training datasets, the significant danger of over fitting along with the lengthy and laborious process of developing a model. In this research, offer a unique cloud methodology that is competitive using the methods used today for automatically choosing and fine-tuning ML models. Our approach automates the process of selecting and developing the model. Before the automatic construction of focused supervised learning models of Support Vector Machine (SVM) and Extreme Gradient Boost (XG Boost), leverage unsupervised learning models of K-means Clustering and singular Value Decomposition to more thoroughly investigate the data domain. Specifically, research utilize an innovative autoscaling method to build and assess ML algorithm instances dynamically and with the help of messages between instances and container orchestration, research present a Cloud ML

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 626-638. DOI: *10.58346/JISIS.2025.I3.042*

*Corresponding author: Assistant Professor, NICMAR University, Pune, India.

framework for autotuning and selection. Datasets related to financial cloud security for finance are used to illustrate the suggested technique and tool.

Keywords: Autotuning and Selection, Machine Learning (ML), Financial Cloud Security.

1 Introduction

Renting gear and software, only paying for the services used and other financial features is the part of cloud computing. They describe how computer hardware, software and other information technology services are given over a network according to the particular needs of each client or customer (Aldhyani & Alkahtani, 2022). Smart devices in finance can be made to learn a given task from data or behaviors by using computational intelligence (CI) techniques, such as evolving computing, neural networks, fuzzy logic, learning theory, probabilistic and related computational models (Zhao et al., 2020). Technologies powered by AI will strengthen cyber resilience and help adversaries hone in on cyber threats within the framework of cyber security. However, those with malicious intent are well aware of the present opportunities and will probably attempt to exploit them to do precise research (Bala et al., 2022). Service providers are currently deploying their apps in cloud centers to leverage different cloud resources to offer users expert services. In finance service providers could accept application jobs from users and consumers are freed from the responsibility of installing, running and maintaining application systems themselves (Li et al., 2024). Artificial intelligence (AI) makes it possible to analyze and make decisions with intelligence; it has transformed several industries (Thooyamani et al., 2014). However, setting up infrastructure, choosing algorithms and fine-tuning parameters are difficult tasks when using AI models in practical applications (Ambika et al., 2020). Different types of organizations, finance and software can be encountered by analysts and organization administrators. Every organizational application has unique finance features and requirements for how it should be executed, which can vary dynamically over time and space (Annapurna & Rao, 2020). Bioinspired techniques are better at working with nonlinear multidimensional mathematical functions; they are used by modern computing systems that are primarily focused on optimizing complicated issues (Khairuddin, 2021). In this particular field of research in finance, a subgroup of algorithms applies the behavior seen in natural evolutionary events to optimize several issues by looking for a workable solution (Costa & Oliveira, 2023). This work aims to create an automated process for network security dataset-based ML techniques selection and optimization in innovative finance cloud settings (Aadiwal et al., 2025).

2 Related Works

(Singh & Mannepalli, 2021) identified various cloud environment trends that aid in classifying traffic as malicious or legitimate. The training dataset was first sent through a convolution filter to facilitate learning. (Larriva-Novo et al., 2020) defined a set of reasoner modules by determining which model matches better with each type of attack in finance. (Jain et al., 2023) reviewed the body of research on container security issues and finance solutions. The interval between an incident's occurrences and its discovery should be as brief as feasible to enable prompt and effective assessment of the incident's scope and compromised systems. (Mohammad et al., 2023) created an energy-aware optimal task allocation strategy for semi-asynchronously training an ML model among numerous learners connected by the resource-constrained wireless edge network. (Sharma et al., 2022) expedite the process of evaluating the security of various Docker-using systems by automating the scanning, testing and summarizing of Docker image images for vulnerabilities. (Kumar Das & Sinha, 2022) presented a safe cloud framework that consists of two distinct parts: encryption and classification in finance (Vij & Prashant, 2024). Here,

the primary focus was on classifying the data using the Hybrid Naïve Bayes machine learning algorithm, which divides the data into three categories: basic, sensitive and very sensitive. (Nassif et al., 2021) leverage the paper's primary aspiration to influence the direction of finance cloud security in the future by utilizing ML algorithms like convolution neural networks (CNNs), which can offer automated and adaptable methods for improving security in cloud environments. (Mishra & Tyagi, 2022) assessed the various ML techniques that address the difficulties in managing Internet of Things (IoT) data. Big data was produced via the IoT and smart device connectivity, and it was stored on cloud servers in finance (Yamuna & Sasirekha, 2017; Qayyum et al., 2020) described the taxonomy of ML algorithms and explained how various methods were applied to data obtained via IoT devices. The research discovered that the idea of using ML as a service platform to launch and repel different kinds of attacks was becoming more and more popular among researchers. (Attou et al., 2023; Prakash & Prakash, 2023a) provided a cloud-based intrusion detection model based on random forest (RF) and finance feature engineering in finance. In particular, the suggested detection model's accuracy was improved by obtaining and integrating the RF classifier. (Mohammad & Pradhan, 2021) looked into using big data analytics in conjunction with an ML-Assisted Cloud Computing Model (ML-CCM) to increase data transmission speeds and security in finance. Cloud storage was the easiest way to store massive amounts of data. Massive distributed data sets can be stored or managed in clouds using big data. (García et al., 2020) demonstrated how ML practitioners can leverage a distributed architecture to gain access to a variety of tools and cloud services that cover each phase of the ML development cycle, from building, training, validating and testing models to sharing and publishing them as services.

3 Methodology

This section covers a novel approach to intelligent financial cloud security through AI-driven autotuning and auto selection (Prakash & Prakash, 2023b). A baseline ML was assessed in advance of creating the new methods so that they could be compared later. Three unsupervised ML methods (clustering) and seven supervised (also known as classifiers) are selected at random. Extreme Gradient Boost (XG Boost) and Support Vector Machine (SVM) are two of the supervised techniques. The Singular Value Decomposition (SVD) model and K-Mean clustering are examples of unsupervised algorithms. Python is used to write ML algorithms. Figure 1 shows the proposed flow

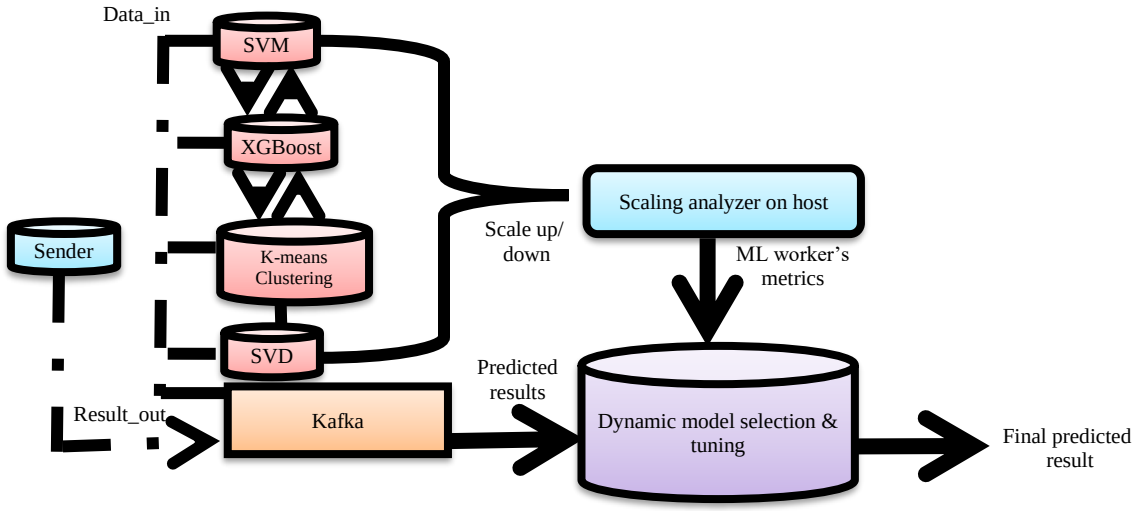

Figure 1: Overview of the Proposed Methodology

3.1. Dataset

The study used the "UNSW-NB15" dataset (Moustafa & Slay, 2015) for ML implementations' training and testing. It was processed and utilized the data in online for this research. Utilizing the samples, intrusion detection was evaluated and network anomaly systems. The three categorical variables in it are "proto, service and state." Text values representing different qualities are available for these variables. The term proto refers to transaction protocols such as “TCP, UDP, CRT P, GGP, and HMP”. The connection shell is described as a service like “SSH, SSL, FTP - Data, DNS, DHCP” and so forth. The protocols are dependent utilized, such as “INT, REQ, CON, RST, etc”., are referred to as "state." With 82, 332 records for training and 175, 341 records for testing, the data set contains characteristics of both typical and modern synthetic assault activities of network traffic. Attributes of various data kinds, such as binary, float, nominal and integer are included in each record. The feature set consists of 10 labels, which include nine distinct attack names and a normal ("NO-ATTACK") label, in addition to protocols, service names, port numbers, packet transmission statistics, IP addresses and other information. Conventional samples like "KDD98, KDDCUP99 band NSLKDD”; offer only a restricted quantity of assaults and obsolete packet information. Additionally, the UNSW dataset was created with several well-known programs, including Argus, Bro-IDS and the IXIA traffic generator.

3.2. Classification with Supervised and Unsupervised Learning

3.2.1. Supervised Learning

Supervised learning is a machine learning function that converts a yield set into a yield, involving multiple preparation models. Managed learning is a crucial part of data science, while administered learning starts a limit using named preparation data and multiple models.

Support Vector Machine (SVM): The SVM trains nonlinear connections, aiming to limit generalization error rather than empirical error. The SVM uses nonlinear mapping to convert input spaces into high-dimension spaces and identify nonlinear correlations. With limited training samples, large dimensions and local optima, it can identify global optimal solutions. Applications in finance, such as pattern recognition and nonlinear regression, demonstrate the generalizability of SVMs and provide a collection of observational financial data. The following regression function equation (1) can be obtained for the SVM-based regression problem:

$$e(W) = \sum_{j=1}^{m}\left(\propto_j - \propto_j^*\right)L(W_j.W_i) + a, \quad (1)$$

where $L()$is the kernel function, $L\left(W_j, W_i\right) = \phi\left(W_j\right)\phi(W_i).\propto, \propto^*$meaning that, a and can be found by resolving the subsequent quadratic programming issue is represented in equation (2):

$$X(\propto, \propto^*) = -\frac{1}{2}\sum_{j,i=a}^{m}(\propto_i - \propto_i^*)\, L\left(W_j.W_i\right) + \sum_{j=a}^{m} z_j(\propto_i - \propto_i^*) - \varepsilon \sum_{j=1}^{m}\left(\propto_j - \propto_i^*\right) \quad (2)$$

According to equation (3),

$$\sum_{j=a}^{m}\left(\propto_j - \propto_i^*\right) = 0,\ 0 \le D, j = 1,2, \ldots m. \quad (3)$$

The relationship between the maximum variance that can be tolerated and the degree of flatness is established by the constant$D > 0$.

Extreme gradient boosting (XG-boost): One of the applications of gradient boosting machines (GBM), which is regarded as one of the most effective algorithms used in supervised learning, is XG-boost. It can be applied to issues involving both classification and regression. Data scientists favor XG-

boost due to its fast execution speed outside the core computation. The XG-boost financially operates in the following manner: For instance, suppose research have a dataset CT with m characteristics and n samples, such that CT represents the anticipated result of an ensemble tree model produced using the subsequent equation (4):

$$Å._j = \emptyset(W_j) = \sum_{l=1}^{L} e_l\,(W_j), e_l \in \Im \tag{4}$$

To solve the following equation, where e_l is the model's representation of the total amount of trees the user must determine the optimal combination of financial functions by minimizing the loss and the regularization target in financial applications using equation (5).

$$\mathcal{L}(\emptyset) = \sum_j 1\,(z_j, Å._j\,) + \sum_l \Omega(\,e_l) \tag{5}$$

The loss function, denoted by the symbol l, is the difference between the predicted output,$\hat{z}_j$ and the actual output, $\hat{z}_j$. This keeps the model from being overfat even though O is a measure of the model's complexity and it is calculated using the equation (6) below:

$$\Omega(e_l) = \gamma S + \frac{1}{2}\lambda\|x\|^2 \tag{6}$$

The number of leaves on the tree is represented by S in the equation above, and each leaf's weight is indicated by x.In decision trees, boosting is used to minimize the objective function, and boosting entails introducing a new function f while the model is still being trained. Consequently, on the $t-th$ iteration, the new function (tree) that follows is introduced in equation (7) to (10):

$$\mathcal{L}^{(s)} = \sum_{j=1}^{m} 1\left(z_j, Å._j{}^{(s-1)} + e_l\left(z_j\right)\right) + \Omega(e_l) \tag{7}$$

$$l_{split} = \frac{1}{2}\left[\frac{\left(\sum_{j\epsilon J_K} h_j\right)^2}{\sum_{j\epsilon J_K} g_j+\lambda} + \frac{\left(\sum_{j\epsilon J_Q} h_j\right)^2}{\sum_{j\epsilon J_Q} g_j+\lambda} - \frac{\left(\sum_{j\epsilon J} h_j\right)^2}{\sum_{j\epsilon J}\, g_j+\lambda}\right] - \gamma \tag{8}$$

$$h_j = \partial_{Å.^{(s-1)}} 1(z_j, Å._j{}^{(s-1)} \tag{9}$$

$$G_j = \partial^2{}_{Å.^{(s-1)}} 1(z_j, Å._j{}^{(s-1)} \tag{10}$$

3.2.2. Unsupervised Learning

An ML approach known as "unsupervised learning" is used to infer conclusions from datasets that contain data without clearly identifiable reactions. The most popular method for unsupervised learning is cluster analysis. It is used in exploratory information analysis to find hidden patterns or groupings within the data.

K-Means Clustering: K-Means is a simple unsupervised learning method for clustering data sets. It uses predefined clusters and determines *L* centroids for each cluster to prevent disparate outcomes. An early group is formed when no points are left and cluster centers are recalculated to include *L* new centroids. A loop is created when a fresh binding is established between data points and the closest new centroid and the *L* centroids gradually shift their positions until they stop. The technique's ultimate goal is to minimize an objective function, in this case, the squared error function and the objective's function in equation (11).

$$X(T, D) = \sum_{L-1}^{L} \sum_{j\epsilon T_L} \left\|z_j - d_l\right\|^2 \tag{11}$$

The entity set represented by vectors z_j $(i \in J)$ in the M-dimensional feature space is partitioned into K clusters, T, which are made up of non-empty, non-overlapping clusters T_L, each with a centroid ck $(L = 1,2, \ldots L)$.

Singular value decomposition (SVD): The SVD is a method for factorizing rectangular real or complex matrix, enhancing its resilience against numerical errors. It can compute the financial pseudo inverse, solve homogeneous linear equations, find approximation matrices and solve the total least square minimization problem. It is used in signal processing, picture processing, principal component analysis and pattern recognition. Numerous other fields, including scientific computing, signal processing, automated control and many more, have found use for the SVD in equation (12).

$$B = V\sum U^S \tag{12}$$

In this case, $\sum$ is a $n \times m$ diagonal matrix with entries in decreasing order along the diagonal, and U is an $an \times n$orthogonal matrix.

3.3 Auto Selection Models

It is necessary to have an automated model selection technique that dynamically selects the correct model from the available real-time data. The weighted majority rule voting method is one method for automated model selection. The different models predicted accuracies dictate the vote weights. The model auto-selection process in ML methods employs weighted majority voting. The training dataset is available. During forecasting, unsupervised ML ascertains the number of clusters in testing information sample. Every classification model then processes this sample of data and predicts its label. The "Innovative Model Selection & Tuning" module receives these expected labels after they have been collected. A dynamically changing live data stream is required to evaluate the model selection procedure. 10,000 entries in a dataspace drawn from UNSW-NB15's experimental sample are produced to replicate such Innovative finance features. The creative modification to the ML ranking throughout the dataspace is shown by the model rankings for the labels "NO-ATTACK and Generic" after each dataspace. The chosen models for each sample are shown in a bold green type enclosed in rings. Clustering contributes to increased prediction accuracy for some labels, including "DoS, NO-ATTACK, Fuzzers and Exploits." Not all clusters have improved classifier accuracy as the number of clusters is increased.

3.4. ML parameters of Autotuning

Accuracy of knob-like parameters is essential to the performance of ML models of SVM and XG Boost accuracy about parameter selections. An ML model's variables should be allowed to change throughout its lifespan to maximize the model's performance in response to innovative variations in the information wave patterns and associated financial feature patterns. Previous to a certain model is fully deactivated, as specified in the ML strategy auto selection, it is advised to adjust its settings while monitoring its accuracy and documenting any appreciable increase in accuracy as a consequence of the adaptation process. The ML Stats module stores model parameters, which are adjusted based on threshold crossings and the "Scaling Analyzer" module provides updated settings to ML docker containers. The precision of the "NO-ATTACK" XG Boost classification across the whole testing dataset yields a prediction accuracy of 23.9%. However, when an auto-tuning approach is used, the precision that is attained is greater and varies dramatically throughout time. In an additional experiment, each dataspace time window begins with the parameters adjusted.

An automated procedure for choosing the optimal ML model and fine-tuning its parameters based on past accuracy is described in the script that is given. It starts by analyzing several clustering methods and choosing the one that produces the best accuracy when compared to unflustered data. The model parameters are repeatedly increased or decreased within user-defined bounds in response to accuracy trends. The script reduces the size of the ML container if parameters don't increase accuracy in predetermined bounds or if decrementing continues beyond a certain point. To ensure effective resource use, this procedure strives to maximize model performance while keeping monitoring out for overfitting or underperformance.

4 Statical Result

In this section, research assessed the efficacy of two unsupervised learning and two supervised learning models for financial cloud security. One node served as the master and three other nodes as slaves in a four-node cluster running Spark version 2.4.1 in cluster mode for all of the research covered in this section related to financial cloud security. Because hyper-threading was turned on, each node has two 10-core $Intel®Xeon\ E5-2630\ v4$ CPUs running at $2.20GHz$, for a total of $40\ threads$ per node. Additionally, each node included $128\ GB$ of RAM and a $10Gbps$ Ethernet network linked them together.

The process of automatically selecting the characteristics from the finance dataset that have the greatest influence on the prediction label is known as feature selection. While unselected features have a finance detrimental effect on the predicted performance of ML models, selected finance features can show the dataset records' time-dependent development. Reductions in training time and model overfitting are two other benefits of feature selection. In this work, the univariate selection of finance features is modified to selected finance features based on their highest cross-correlation statistics between the output variables. In this work, the selection of univariate fiancé features is modified to selected finance features based on their greater experimental output element with cross-correlation. The classification accuracies utilizing the top $10, 15, and\ 20$ finance features are displayed in Figure 2, along with a comparison with a model that incorporates all features.

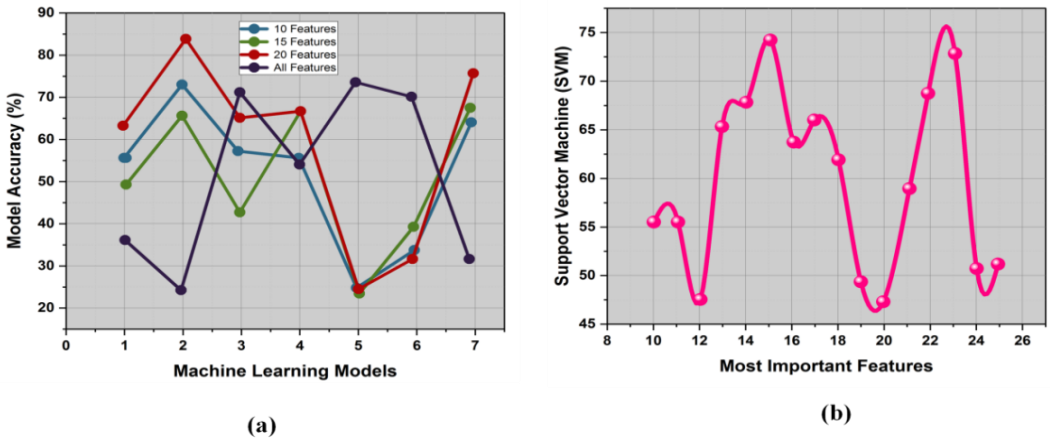

Figure 2 (a-b): SVM Classifier Accuracy

The SVM classifier uses Recursive Feature Elimination (RFE) to select significant finance features and then iteratively removes the least significant attribute; ensuring accurate models based on remaining finance characteristics. This suggests the need for statistically separate data spaces to demonstrate the

effectiveness of strategy auto-selection and auto-tuning procedures. Dynamic model selection and tweaking are required because the significance of finance features in ML algorithms might vary over time. 10,000 Histories through the testing and training datasets were utilized and new classifications were generated innovatively for each to illustrate in Figure 3. Test results, however, indicated reduced accuracy, pointing to Q-learning as a potential solution. To increase accuracy and resilience, ensemble machine learning (EML) integrates many models; one potent EML model is XgBoost. Regarding cross-validation accuracy for label predictions on the UNSW-NB15 dataset, XG-Boost methods perform better than auto-selection and auto-tuning algorithms, especially in novel settings where data storage and finance characteristics are subject to change.

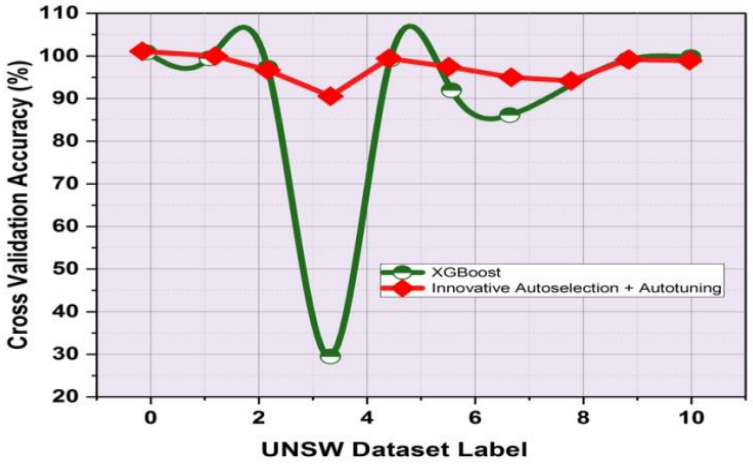

Figure 3: Statically Tuned Accuracy

A dataset has been used to compare deep neural networks to conventional learning techniques. Many hyperparameters in deep learning can be adjusted to provide precise model construction. The number of hidden layers, input units, initialization, optimization, activation and output activation are among the hyperparameter finance variables shown in Figure 4.

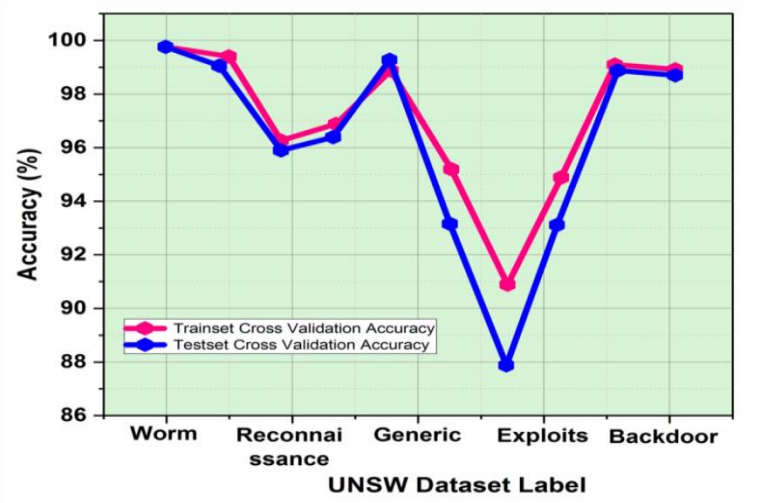

Figure 4: Accuracy of DL for Every Label

The outcome is displayed in Figure 4. The hyperparameter elements are listed below: {Activation for output = $Softmax$}, Activation for hidden layer = Ruu, The number of units entered= 43, Optimization = $Adam$, Probability of dropout = 0.4, Initialization = He}. As seen in Figure 5, extensive experimentation and the determination of ideal hyperparameter values can result in 100% prediction accuracy, albeit at the expense of lengthy training cycles. The earlier sections are the best design decisions for increasing classification accuracy without compromising run time.

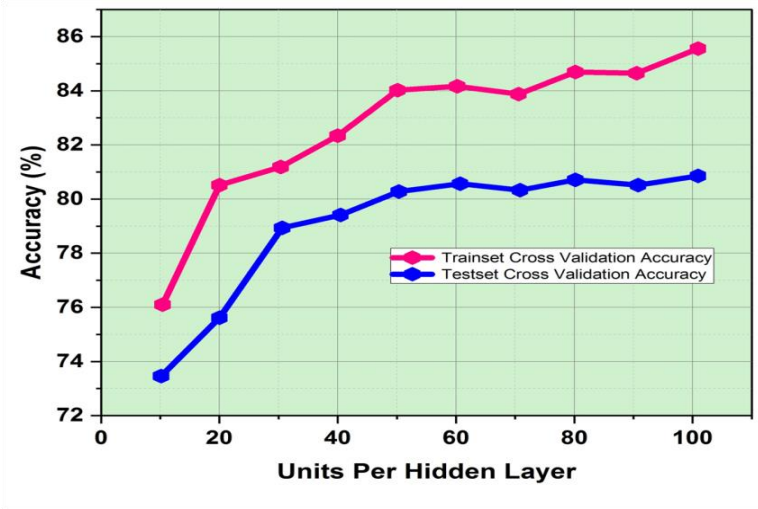

Figure 5: Accuracy of DL in Multilabel Classification

Table 1 displays the training and forecasting timeframes for every ML strategy utilized in the previous parts. As predicted, the slowest ML strategy for training is the SVD, whereas the least rapid strategy for prediction is the SVM. Figure 6 depicts the existence of these MLs as a vital channel in the auto-selection configuration. XG-Boost focuses on improving accuracy over time and developing innovative learning methods to adapt to changing datasets.

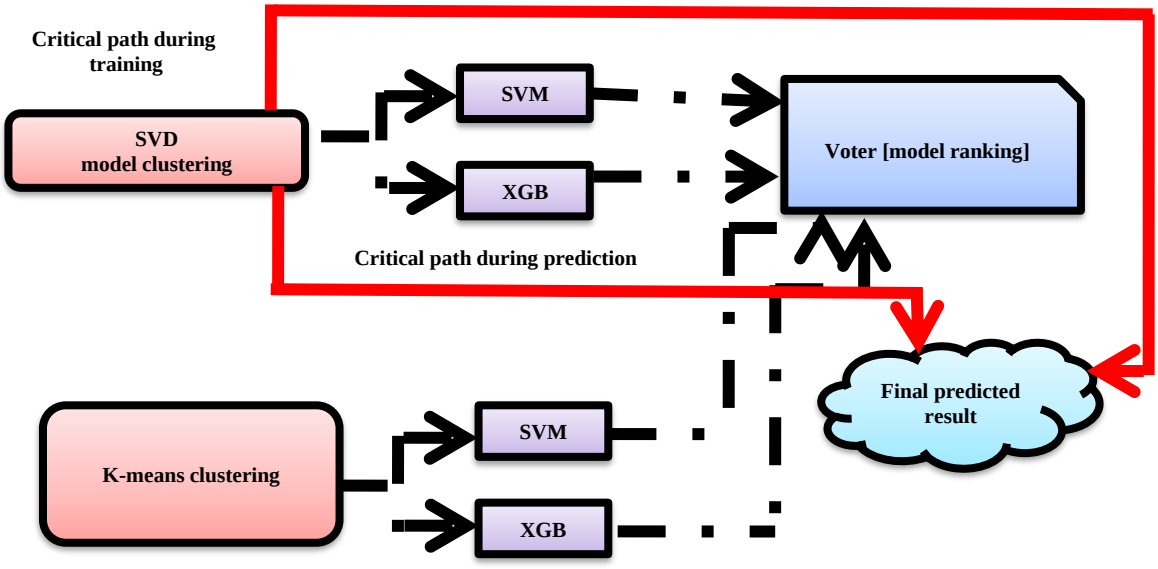

Figure 6: Crucial Route in Model Selection

Table 1: Training and Prediction Timeframes for ML Model

Method Type	Prediction Time (s)	Training Time (s)
K-Means Clustering	0.009	2.200
Singular Value Decomposition (SVD)	0.036	8.821
Support Vector Machine (SVM)	0.277	5.585
XG-Boost	0.0056	0.514

5 Conclusion

This study presents the combination and use of many supervised and unsupervised ML models on a cloud security dataset in finance features. To anticipate each kind of security attack, several models are developed to increase accuracy. It has been demonstrated that improved prediction accuracy requires the use of unsupervised strategy in addition to supervised methods. To offer an innovative data evolution-based machine learning method for selecting models. Innovation strategies are "brought online" and "trained offline" when required, whereas previously tuned strategy is deleted when they are unable to attain enough forecasting precision. After that is brought online, strategy is mechanically adjusted once again to adjust the forecast precision to the changing samples. An explanation is given of the prerequisites in the setting of distributed learning for the selection of innovative financial features. A comparison with XG Boost demonstrates that innovative model selection is superior to statically trained. Plans include for augmenting the toolkit's collection of autotuned and autoselected machine learning models with models for reinforcement learning would also like to test the enlarged toolbox on a range of datasets related to cloud computing.

References

[1] Aadiwal, V., Upadhyay, S., Nagappan, B., & Wani, T. A. (2025). Investigating the Influence of Physiographic Factors on Habitat Selection by Cetacean Species in Marine Environments. *Natural and Engineering Sciences*, *10*(1), 301-311. https://doi.org/10.28978/nesciences.1646474

[2] Aldhyani, T. H., & Alkahtani, H. (2022). Artificial intelligence algorithm-based economic denial of sustainability attack detection systems: Cloud computing environments. *Sensors*, *22*(13), 4685. https://doi.org/10.3390/s22134685

[3] Ambika, M., Priya, S. H. R., & Narayanasamy, S. (2020). Artificial Intelligence in Cloud Computing Environment-Auto-Selection Method. *NeuroQuantology*, *18*(8), 144. https://doi.org/10.48047/nq.2020.18.8.nq20217

[4] Attou, H., Guezzaz, A., Benkirane, S., Azrour, M., & Farhaoui, Y. (2023). Cloud-based intrusion detection approach using machine learning techniques. *Big Data Mining and Analytics*, *6*(3), 311-320. https://doi.org/10.26599/BDMA.2022.9020038

[5] Bala, P. M., Usharani, S., Rajmohan, R., Jayalakshmi, S., & Divya, P. (2022). The Cyber Artificial Intelligence Platform for Cloud Security. In *Privacy and Security Challenges in Cloud Computing* (pp. 229-256). CRC Press.

[6] Costa, H., & Oliveira, R. (2023). Adaptive radiation as an autotuning strategy for genetic algorithms on dynamic problems. In *Proceedings of the Brazilian conference on computational intelligence (CBIC)* (Vol. 9).

[7] García, Á. L., De Lucas, J. M., Antonacci, M., Zu Castell, W., David, M., Hardt, M., ... & Wolniewicz, P. (2020). A cloud-based framework for machine learning workloads and applications. *IEEE access*, *8*, 18681-18692. https://doi.org/10.1109/ACCESS.2020.2964386

[8] Jain, V., Singh, B., Choudhary, N., & Yadav, P. K. (2023). A Hybrid Model for Real-Time Docker Container Threat Detection and Vulnerability Analysis. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(6s), 782-793.

[9] Khairuddin, A. R. (2021). *Hybrid dragonfly algorithm with neighbourhood component analysis and gradient tree boosting for crime rates modelling* (Doctoral dissertation, Universiti Teknologi Malaysia).

[10] kumar Das, P., & Sinha, N. (2022). Secure cloud framework based on machine learning approach. *Journal Of Algebraic Statistics*, *13*(2), 1383-1390.

[11] Larriva-Novo, X., Sánchez-Zas, C., Villagrá, V. A., Vega-Barbas, M., & Rivera, D. (2020). An approach for the application of a dynamic multi-class classifier for network intrusion detection systems. *Electronics*, *9*(11), 1759. https://doi.org/10.3390/electronics9111759

[12] Li, X., Pan, L., Song, W., Liu, S., & Meng, X. (2024). Performance analysis of parallel composite service-based applications in clouds. *Future Generation Computer Systems*, *153*, 27-40. https://doi.org/10.1016/j.future.2023.11.021

[13] Mishra, S., & Tyagi, A. K. (2022). The role of machine learning techniques in internet of things-based cloud applications. In *Artificial intelligence-based internet of things systems* (pp. 105-135). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-87059-1_4

[14] Mohammad, A. S., & Pradhan, M. R. (2021). Machine learning with big data analytics for cloud security. *Computers & Electrical Engineering*, *96*, 107527. https://doi.org/10.1016/j.compeleceng.2021.107527

[15] Mohammad, U., Sorour, S., & Hefeida, M. (2023). Energy Aware Task Allocation for Semi-Asynchronous Mobile Edge Learning. *IEEE Transactions on Green Communications and Networking*, *7*(4), 1766-1777. https://doi.org/10.1109/TGCN.2023.3244710

[16] Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 military communications and information systems conference (MilCIS)* (pp. 1-6). IEEE. https://doi.org/10.1109/MilCIS.2015.7348942

[17] Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. *IEEE Access*, *9*, 20717-20735. https://doi.org/10.1109/ACCESS.2021.3054129

[18] Prakash, M., & Prakash, A. (2023). An Energy Efficient Cluster Head Selection in WSN Based on Enhanced Chicken Swarm Optimization. *International Academic Journal of Science and Engineering*, *10*(2), 80–88. https://doi.org/10.9756/IAJSE/V10I2/IAJSE1011

[19] Prakash, M., & Prakash, A. (2023). Cluster Head Selection and Secured Routing Using Glowworm Swarm Algorithm and Hybrid Security Algorithm for Over IoT-WSNs. *International Academic Journal of Innovative Research*, *10*(2), 01-09. https://doi.org/10.71086/IAJIR/V10I2/IAJIR1004

[20] Qayyum, A., Ijaz, A., Usama, M., Iqbal, W., Qadir, J., Elkhatib, Y., & Al-Fuqaha, A. (2020). Securing machine learning in the cloud: A systematic review of cloud machine learning security. *Frontiers in big Data*, *3*, 587139. https://doi.org/10.3389/fdata.2020.587139

[21] Sharma, A., Keswani, B., & Gupta, P. K. (2022). A novel framework for docker and container security and their risk assessment. *Suresh Gyan Vihar Univ. J. Eng. Technol.*, *8*(1), 28-42.

[22] Singh, R., & Mannepalli, P. K. (2021, October). Cloud Malicious Threat Detection Using Convolution Filter and EBPNN. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE. https://doi.org/10.1109/ISCON52037.2021.9702492

[23] Thooyamani, K. P., Khanaa, V., & Udayakumar, R. (2014). Wide area wireless networks-IETF. *Middle-East Journal of Scientific Research*, *20*(12), 2042-2046.

[24] Vij, P., & Prashant, P. M. (2024). Predicting aquatic ecosystem health using machine learning algorithms. *International Journal of Aquatic Research and Environmental Studies*, *4*(S1), 39-44. https://doi.org/10.70102/IJARES/V4S1/7
[25] Yamuna, D., & Sasirekha, N. (2017). Optimal Classifier Selection Using Genetic Algorithm for Software Bug Prediction. *International Journal of Advances in Engineering and Emerging Technology*, *8*(4), 140-155.
[26] Zhao, S., Li, S., Qi, L., & Da Xu, L. (2020). Computational intelligence enabled cybersecurity for the internet of things. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *4*(5), 666-674. https://doi.org/10.1109/TETCI.2019.2941757

Authors Biography

Dr. Trupti Manish Rathi is an accomplished legal professional with over 15 years of experience spanning academia and industry. She specializes in corporate law, banking law, insolvency and bankruptcy law, and corporate governance. A Ph.D. holder in Corporate Laws from Symbiosis International University, she has extensive teaching experience at prestigious institutions, including Symbiosis Law School, Pune. Dr. Rathi has contributed significantly to legal research, with multiple publications in Scopus-indexed journals and international conferences. She is an active member of INSOL India and INSOL International and serves as the Editor-in-Chief of the International Journal for Business Law Studies. In addition to her academic and research contributions, she has participated in various faculty development programs, webinars, and legal panels, reflecting her commitment to continuous learning and professional excellence.

Dr. Ashutosh Panchbhai is an Assistant Professor at the Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR), Symbiosis Law School, Pune (SLS-P), a constituent of Symbiosis International (Deemed University), Pune, India. He specializes in advanced legal studies and is dedicated to fostering research excellence in the field of law. His academic interests include constitutional law, jurisprudence, and public policy. Dr. Panchbhai actively contributes to the legal academic community through research, publications, and academic initiatives.

Dr. Arvind Kumar Pandey is an Associate Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. With a strong focus on computer science education and research, he is engaged in advancing knowledge in areas such as software engineering, data analytics, and information technology. Dr. Pandey is committed to academic excellence and contributing to the growth of his students and the broader research community.

Kshipra Jain is a faculty member in the Department of ISME at ATLAS SkillTech University, Mumbai, Maharashtra, India. She is involved in teaching and research with a focus on management studies and interdisciplinary approaches in education. Kshipra is dedicated to fostering academic growth and contributing to innovative research in her field.

R. Hannah Jessie Rani is an Assistant Professor in the Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology at Jain (Deemed-to-be University), Bangalore, Karnataka, India. She specializes in electrical and electronics engineering, focusing on innovative teaching and research in her field. Hannah is committed to advancing technological education and contributing to academic research excellence.

Dr. Anita Sable is an Assistant Professor at Symbiosis Law School, Nagpur, India. She has expertise in legal studies and is actively engaged in teaching, research, and academic development. Dr. Sable focuses on contemporary legal issues and contributes to the legal academic community through scholarly work and mentorship.