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

Log-Based Intrusion Detection for Financial Cloud Applications through Novel ML-driven Algorithm

Dr. Amit Sharma[1*], Dr. Amandeep Gill[2], Anoop Dev[3], Dr. Bineet Desai[4], V. Haripriya[5], and Dr. Arvind Kumar Pandey[6]

[1*]Professor, School of Computer Applications, Lovely Professional University, Phagwara, Punjab, India. profamitsharma@gmail.com, https://orcid.org/0000-0003-1451-5892

[2]Dean R&D, Department of R&D, Vivekananda Global University, Jaipur, India. amandeep.gill@vgu.ac.in, https://orcid.org/0009-0008-2020-5966

[3]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. anoop.dev.orp@chitkara.edu.in, https://orcid.org/0009-0001-1301-6891

[4]Professor, Department of ISME, ATLAS Skill Tech University, Mumbai, Maharashtra, India. bineet.desai@atlasuniversity.edu.in, https://orcid.org/0009-0008-7664-225X

[5]Assistant Professor, Department of Computer Science and Information Technology, Jain (Deemed to be University), Bangalore, Karnataka, India. v.haripriya@jainuniversity.ac.in, https://orcid.org/0000-0003-2035-2452

[6]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

Received: August 20, 2025; Revised: September 26, 2025; Accepted: November 03, 2025; Published: November 28, 2025

Abstract

An intrusion detection system is an innovative part of software that analyzes a network for instances of fraud or violations of web-based application policies. Usually, a security data and management mechanism were utilized for notifying any hazardous act or infraction. The goal of this research is to develop a novel machine learning (ML)-driven technique for log-based detection of intrusions in financial cloud-based apps. In the financial industry, we introduced a new Coupling Catboost with Chameleon Optimization Algorithm (CC-COA) for identifying web or cloud-based application assaults. To develop our suggested model, we collected a dataset that contains information from the websites of significant local economic banks that store log files of activity. The CatBoost method was used to manage categorical information. Whereas the COA is used to optimize hyperparameters. A range of indicators, including accuracy (95%), precision (94%), F1 Score (93.5%) and recall (93%) are used in the outcome assessment phase to evaluate the effectiveness of the proposed model. The experimental outcomes demonstrate that the mentioned model outperformed the others in identifying different kinds of assaults in cloud financial apps.

Keywords: Log-Based Intrusion Detection, Financial Cloud, Machine Learning (ML), Coupling Catboost with Chameleon Optimization Algorithm (CC-COA), Cloud Data Security.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 4 (November), pp. 565-576. DOI: *10.58346/JISIS.2025.I4.041*

*Corresponding author: Professor, School of Computer Applications, Lovely Professional University, Phagwara, Punjab, India.

1 Introduction

Cloud computing has been employed more in the financial services industry to increase operational efficiency, mobility and accessibility. The inherent risks associated with technology include safety breaches and unauthorized access to private financial information (Patidar and Bansal (2019)). The intricacy and regularity of cyberattacks, conventional security measures are insufficient to secure data held in cloud-based financial apps. Log-based recognition of intrusions was essential for enhancing the protection of financial cloud-based applications against the attack (Bhattacharya et al., 2022). Log-based detection of intrusions in cloud computing environments refers to the systematic surveillance and evaluation of log files generated by different components, such as server infrastructure, servers for databases and applications (Feng et al., 2020). The organizations that examine their log problems could discover potential safety risks and take proactive measures to rectify them before entire disruptions. Compared to signature-based solutions, log-based detection of intrusions serves as a more flexible in adaptive defense mechanism, and it can discover new threats and zero-day flaws without relying on patterns of previous intrusions (Rabbani et al., 2020; Alsharifi, 2023).

The log-based detection systems for intrusions, especially for financial institutions, pertain to storing in cloud contexts (Gunalan et al., 2023). The increasing prevalence of the web-based financial sector, mobile device money platforms and digital payments, providers of financial services are accountable for preserving significant volumes of confidential customer data, including personally identifiable information (PII), accounting information and history of payments (Das et al., 2021). An organization's reputation could potentially be seriously damaged, along with financial losses and legal consequences, violation of the security, precision and availability of the data. Through the application of log-based detection of intrusions, institutions of finance could enhance their security protocols (Liu et al., 2023) (Farhood, 2023). IDS can compile and examine log information from several outlets, which include network traffic, web server records, along application data files to provide a comprehensive view of the accomplished cloud computing system (Jian et al., 2021). The cloud security teams are used to detect possible paths of attack and risks. Additionally, employing machine learning techniques and detection of anomalies techniques, IDS possess the capability to recognize the difference between regular user conduct and malicious behavior, resulting in a reduction of true positives and false negatives (Aoudni et al., 2022; Alzaidi, 2024).

Log-based detection of intrusions enables the prompt identification of hazards and reacting to incidents, allowing organizations to effectively manage and terminate breaches of cloud data security before serious effects (Sanjalawe & Althobaiti, 2023). IDS possesses the option to initiate automatic notifications and alerts to security staff through constantly inspecting log flows for departures from established standards and specified parameters (Moreau & Sinclair, 2024). Additionally, the historical data that includes the identities of users' dates as well as times and geo-locations, IDS enables security professionals to conduct extensive forensic evaluation and fundamental assessment (Nakamura & O'Donnell, 2025). The integration of log-based detection of intrusions in financial cloud services poses several challenges and aspects (Wang et al., 2022; Selvakumar et al., 2025). The implementation of decentralized topologies and accessible storage systems was necessary for substantial flexibility and efficiency limits posed by the enormous amount and rapid speed of log information accumulated in cloud-based settings (Sunil et al., 2023).

Improving protection stances is the research's goal of financial organizations that operate in cloud settings through the use of log information analysis and continuous surveillance procedures. The objective is to enhance the robustness of economic cloud-based services towards various cyber-attacks,

ensuring the protection of confidential financial information concerning privacy, reliability and accessibility (Deshmukh & Menon, 2025).

The organization of the research includes five sections. Phase 2 contains the related works; Part 3 involves the methodological framework and Phase 4 includes results and discussion. Phase 5 contain the conclusion.

2 Related Works

RM et al., (2022) proposed cloud computing as a developing pattern in the information technology (IT) service paradigm due to its ability to provide a range of economical streaming solutions for customers. The preservation of confidentiality and safety for consumers of cloud services emerged as a significant challenge (Chinnasamy, 2024). The Intrusion Detection System (IDS) method was utilized for identifying incidents on cloud computing systems. Farshchi et al., (2018) proposed a unique methodology for identifying faults in the performance of activities, specifically in the context of periodic upgrading activities. The approach depends on regression analysis and leverages the connection between log files of procedures and the impact of operational actions on the resources of the cloud. Cloud-based computing options provided the necessary capabilities to enhance the integrity of software services by mitigating the impact of distinct resource faults. The experimental outcome resolved the issue of controlling internet service activities by analyzing logs and metrics. Zhang, (2022) examined the particular demands of financial data required for management teams in organizations and the operational procedures of the accounting department. The cloud platform corporate accounting and finance enabled the convenient acquisition of resources for computing the internet, preservation and solutions according to the specific needs of the network's infrastructure (Shah & Bansalm, 2023). The result shows that the performance of the financial Information Management System (IMS) has exceeded its requirements.

Bhushan & Gupta, (2019) presented a unique methodology that utilizes network traffic analysis on the individual's side to identify and address Fraudulent Resource Consumption (FRC) assaults toward services hosted on the cloud. The structure of cloud-based computing attracts resistance from many entities hindering the widespread utilization of cloud data and services through various entities. The experiment's outcomes show the effectiveness and stability consume minimum resources for computation. Wen, (2022) proposed the use of cloud computing incursion detection systems employing a BP neural network (BP-NN). The primary objective of this research is to offer concepts and recommendations for the development of future cloud networking incursion identification techniques particularly considering BP-NN. Abbas & Myeong, (2023) proposed that cloud computing has transformed the process in various sectors, safeguarding, evaluating and retrieving information. The growing prevalence of cloud-based services led to reservations pertaining to the safeguarding of information. Machine learning (ML) represented a highly promising method for improving the security of cloud-based computing.

Rustogi et al., (2019) presented an innovative approach for identifying the FRC attempt in a web server hosted in the cloud. The websites were among multiple quantiles according to the attractiveness indexes. The quantiles are subjected to the Discrete Wavelet Transform to eliminate any high-energy distortions and improve the homogeneity of duration period statistics. Attou et al., (2023) proposed that cloud systems can be attractive to intruders because of common infrastructure. The design was necessary to incorporate robust safety precautions to tackle the safety issues. The system plays a crucial role in protecting the internet and cloud-based settings, including IDS that regulates network communications along with the system performance. Idhammad et al., (2018) introduced a system for detecting the Hypertext Transfer Protocol (HTTP) DDoS assaults in a cloud context, employing the knowledge

conceptual density principle and a random forest combined learning technique. The coefficient of entropy connection preamble features of incoming data packets was determined using a time-sensitive window sliding strategy.

3 Methodology

Figure 1 illustrates the proposed approach in this article. We collected a dataset that comprises data from important local economic banks' website hosting log files to train our proposed model. We proposed a novel Coupling Catboost with Chameleon Optimization Algorithm (CC-COA) for detecting attacks on web or cloud applications in financial sectors.

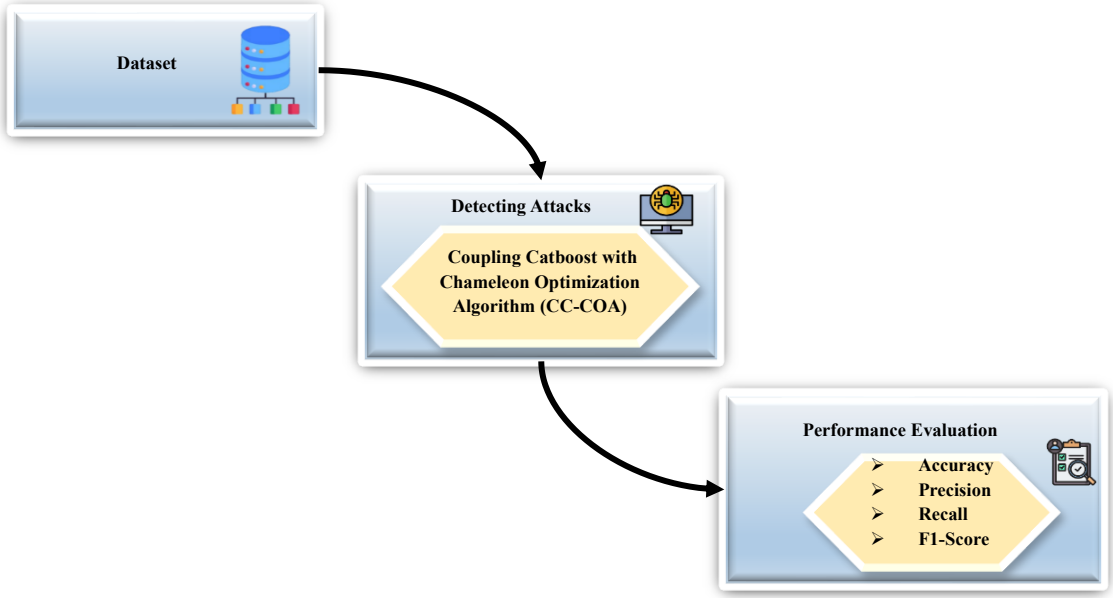

Figure 1: Proposed methodology

3.1 Dataset

The dataset includes information from important local economic banks' website hosting log files, both during and following the financial crisis. They provide the ability to investigate consumer actions. The log files that were acquired from a financial institution's website hosting server were used for a web-based inquiry. A sample of 2,071,235 recorded accesses was retrieved during the collection of data comprising the log files.

3.1 CatBoost (CB)

The gradient-boosting implementation of financial cloud applications enhances their categorical characteristics and can improve their security infrastructure by utilizing gradient boosting algorithms. The Greedy Target Statistics (Greedy TS) algorithm was very effective but has an inherent conditional displacement issue, and was typically used by conventional Gradient Boosted Decision Trees (GBDT) methods to handle categorical information. The targeted leakage, CatBoost technique adopts a method focused on organized principles to prevent the problem. Consequently, the approach handles classified characteristics during development time and provides the entire dataset available for the instructor's model to gain knowledge. CatBoost rotates the information during arbitrary selection, selects a specific

category function and computes the median to identify the value that represents the occurrence, and the identical category value is placed before the category of choice in the randomization. They state that the sample from the provided information as a set of permutations was replaced in the equation (1);

$$w_{\sigma_{o,l}} = \frac{\sum_{e-1}^{o-1}\left[w_{\sigma_{o,l}}=w_{\sigma_{o,l}}\right].\Upsilon_{\sigma_e}+\beta.o}{\sum_{e-1}^{o-1}\left[w_{\sigma_{o,l}}=w_{\sigma_{o,l}}\right]+\beta} \quad (1)$$

Where o represents a previous value, while β denotes the weight. The dataset's mean labeled price, aids in lowering the level of noise from the low-energy classification.

The transition of CatBoost from the classical gradient boosting method to sequential promoting represents a crucial improvement that solves the inherent issue of gradient distortion during repetition and improves adaptation capability. The conditional distribution for a training will vary from the test case, where GBDT replaces qualitative characteristics with numerical indicators according to the desired metric. Unbiased gradient boosting can be resolved by developing a model excluding a certain sample to render the baseline of classifiers unshifted. The approach focused in sequence concept, CatBoost creates arbitrary repeated variations to provide enough iterations to successfully reduce the effects of overfitting and improve the resilience of algorithms.

The treatment of classification characteristics, CatBoost creates greedy combinations of specific characteristics and employs them to generate additional attributes. Specifically, CatBoost integrates all dataset's type characteristics displayed in established structures. By using this technique, systems are more capable to capture high-order interactions and enhance prediction reliability.

CatBoost adopts an inattentive tree of decisions as base predictive factors, demonstrating another sophisticated and significant feature. These trees compute a fair decision using the same splitting for every tree level and perform more quickly, reducing the likelihood of excessive fitting and testing intervals.

3.3 Chameleon Optimization Algorithm (COA)

The highly specialized group of animals, chameleons can change their coloration to blend in with their surroundings. Chameleons consume insects and can survive as well as thrive in swamps, deserts, mountains and desert-like terrain settings. Animals need to track their prey, employ their sight to pursue it and finally attack the multi-step hunting for food operation. The following subsections provide an explanation of this algorithm's mathematical models and stages.

3.3.2 Setup and Assessment of Function

A cohort-based metaheuristic termed as COA creates a starting population at random to begin the optimization process. The dimensional exploration area was used to construct the n-person chameleon population, where every single member of the population is a possible solution to the optimization issue. Equation (2) describes the chameleon location in the target region at each individual iteration:

$$z_s^j = \left[z_{s,1}^j, z_{s,2}^j, \ldots\ldots z_{s,c}^j\right] \quad (2)$$

Here, the number of iterations was represented by $j = 1,2 \ldots . s$ and the location of the chameleon was denoted as $z_{s,c}^j$.

The quantity of chameleons in the region of interest is shown by equation (3) and issue dimensions are employed to construct the starting individuals:

$$z^j = k_i + q(v_i - k_i) \quad (3)$$

Where r is a randomly distributed integer ranges from 0 to 1, v_i and k_i denotes the top and bottom boundaries of the targeted region and z^j indicates the beginning vector of the q th chameleon. Considering the evaluation of the intended function, the quality of each step's solution was assessed for every shifting position.

3.3.2 Search of Prey

Equation (4) provides a basis for characterizing the motion activity of the chameleons throughout pursuit through the position modification technique.

$$z_{s+1}^{j,i} = \begin{cases} z_s^{j,i} + O_1\left(O_s^{j,i} - H_s^i\right)q_2 + O_2\left(H_s^i - z_s^{j,i}\right)q_1 \\ z_s^{j,i} + \mu\left(v^i - k^i\right)q_3 + k_a^i sgn(rand - 0.5)q_1 < O_o \end{cases} q_1 \geq O_o \quad (4)$$

The iteration steps s and $(s+1)$ denote the s th and $(s+1)$) th, respectively. In the *i*th width, the ith chameleon was represented by *j* and *i*. The chameleon's present position is $z_s^{j,i}$ and its new position in $z_{s+1}^{j,i}$. The chameleon's optimal postures are shown by $O_s^{j,i}$ and O_s^i respectively.

In this case, exploratory ability is controlled by two positive values, O_1 and O_2. The integers q_1 , q_2 and q_3 are generated at random, uniformly and span from 0 to 1. At index *i*, a uniformly random integer between 0 and 1 is formed represented as q_j. The chameleon's probability of spotting food is indicated by O_o. The direction of exploration and exploitation is affected by $sgn(rand - 0.5)$, which can be either −1 or 1. As an indication of the iteration's parameter, μ falls as the amount of phases rises.

3.3.2 Chameleon's Eyes Rotation

Chameleons can spot their prey even when they are not using their sense of sight. They can see the prey around 360 degrees in a rotating function.

- The focal point of gravity was located at the chameleon's initial place of residence.
- The rotation vector identifying the prey's spot was identified.
- The spinning matrix at the center of gravity was employed to update the chameleon's orientation.
- At last, chameleons are put back into their starting place.

3.3.2 Hunting Prey

The ideal chameleon, generally closest to the prey, was considered to produce the most effective outcomes. The chameleon employs a tongue to attack an individual. The chameleon's situation is improved by its capacity to multiply the length of its tongue. They facilitate the chameleon's exploitation of the pursuing space and enable it to successfully seize victims. The chameleon's tongue was expanded regarding the victims represented in Equation (5).

$$u_{s+1}^{j,i} = \omega u_s^{j,i} + d_1\left(H_s^i - z_s^{j,i}\right) + d_2\left(O_s^{j,i} - z_s^{j,i}\right)q_2 \quad (5)$$

Where the final velocity of the *j*th chameleon in the *i*th dimension of iteration $s+1$ is shown by $u_{s+1}^{j,i}$ and the present velocity in the *i*th dimension was indicated by $u_s^{j,i}$.

3.3.2 Coupling Catboost with Chameleon Optimization Algorithm (CC-COA)

A hybrid method was suggested for log-based detection of intrusion in financial cloud-based services that combines the CC-COA, a potent gradient boosting algorithm recognized for its efficiency in handling classification data. The system's ability to identify minor patterns indicates the intrusions in log information were enhanced by CatBoost's proficient handling of classified information. The COA dynamically modifies CatBoost's parameters to enhance its performance, deriving influence from chameleons' ability to adapt to their environments. The financial cloud applications ensure the confidentiality and integrity of information. The machine learning and optimization techniques offer a potential remedy for cybersecurity issues in financial systems that rely on the cloud.

4 Results and Discussion

The recommended work was done using TensorFlow 1.12.0, which was expedited by Nvidia GPUs. Python has to be deployed together with other applications to finish the process. The assessment of the proposed approach and the use of outcomes for evaluating the method's efficacy. It also contrasts our proposed method's efficacy with that of other approaches already in use. "Random Forest (RF), supported vector machines (SVM), and K-nearest neighbor (KNN)" are among the current techniques (Kolla, 2023). The findings of the prediction are provided in Table 1.

By determining the proportion of correctly anticipated strike indicator occurrences to all occurrences, accuracy evaluates the accuracy of the model and offers a solid assessment of the technique's performance. A comparison of the accuracy of the suggested and traditional methods is shown in Figure 2 and Table 1. With a performance level of 95%, the proposed CC-COA outperforms current techniques like RF, KNN, and SVM, which have accuracies of 89%, 87%, and 72%, respectively. For log-based intrusion detection for commercial applications that utilize cloud computing, our suggestion offered better results.

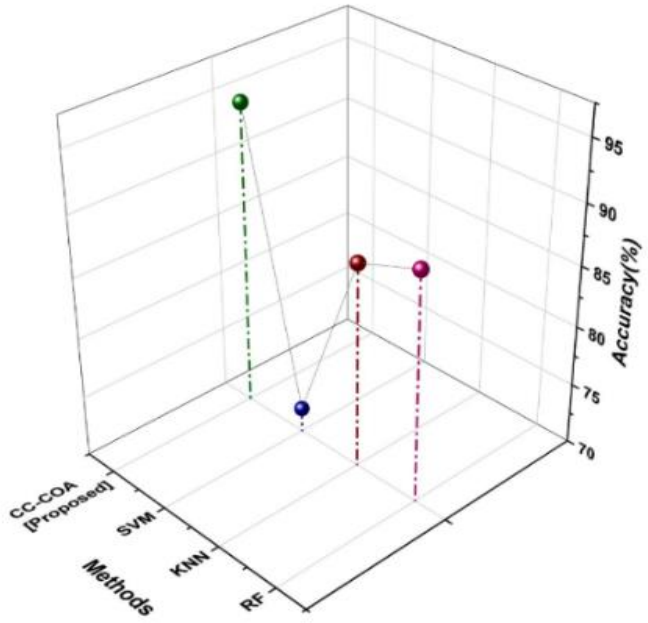

Figure 2: Outcome of accuracy

A model's degree of precision indicated how accurate its predictions proved. The percentage of successfully predicting beneficial outcomes to the overall quantity of anticipated advantages is assessed. Table 1 and Figure. 3 provide a precision analysis. The proposed CC-COA achieves a precise level of 94%, compared with 90%, 88%, and 72% using traditional methods such as RF, KNN, and SVM. Our suggested approach improved the detection of log-based attacks in cloud-based financial applications.

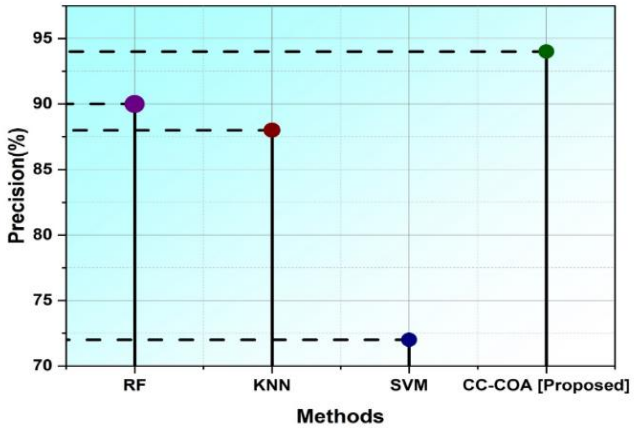

Figure 3: Result of precision

The ratio of precisely anticipated positive instances to all actual positive instances is known as the recall measure. The evaluation of recall across the suggested procedures in comparison to other existing methods is shown in Figure. 4 as well as Table 1. The suggested CC-COA achieves a greater recall rate of 93% than current approaches like RF, KNN, and SVM, which obtain remember rates of 89%, 87%, and 72%, respectively. The proposed approach proved to be more effective than current techniques for log-based intrusion detection in cloud-based financial applications.

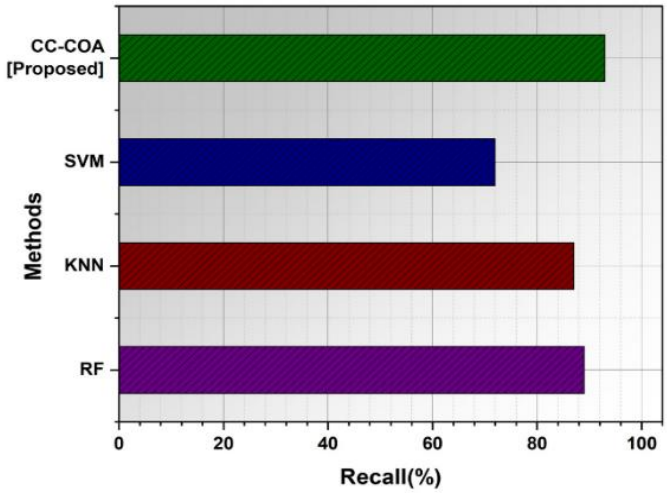

Figure 4: Consequence of recall

The F1 combination is the average value of accuracy and memory. It provides a balance between accuracy and storage. Table 1, as well as Figure. 5, shows the F1-score evaluation. Compared to current techniques such as RF, KNN, and SVM, which achieve F1-Scores of 89%, 87%, and 72%, respectively,

the proposed CC-COA achieves an F1-Score of 93.5%. The suggested technique was successful in identifying log intrusions in cloud-based financial applications.

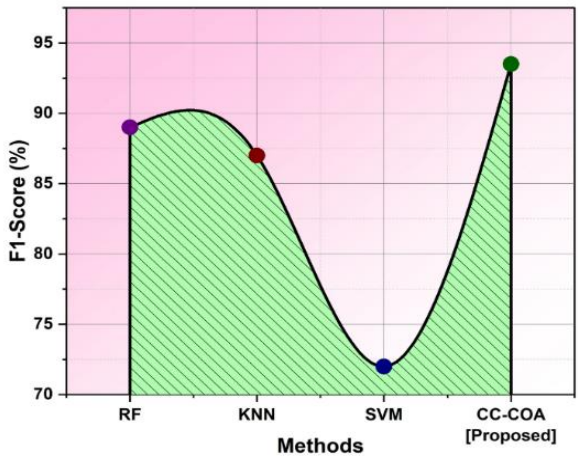

Figure 5: Result of F1-score

Table 1: Prediction outcomes value

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
RF	89	90	89	89
KNN	87	88	87	87
SVM	72	72	72	72
CC-COA [Proposed]	95	94	93	93.5

5 Conclusion

In this study, we introduced a novel approach called Coupling Catboost with Chameleon Optimization Algorithm (CC-COA) has proven to be a strong and effective method for financial cloud uses. Detecting attacks on login in financial cloud applications. The results of the suggested technique were contrasted compared to the remaining previously used algorithms, and the evaluations' results demonstrated that the recommended approach was more successful for financial cloud applications in terms of accuracy (95%), precision (94%), F1 Score (93.5%) and recall (93%). Cloud-based ecosystems exhibit a high degree of mobility and intricacy, characterized by a diverse array of interconnected elements and applications. Evaluating logs during the instances can be difficult due to the large quantity, coupled with the variety of log information produced by different applications and networks. Future research moving towards the development of behavioral assessment computations could detect departures from regular patterns of behavior in log information. The log data could allow reactive identification of threats and reactions extending beyond the detection of signatures.

References

[1] Abbas, Z., & Myeong, S. (2023). Enhancing industrial cyber security, focusing on formulating a practical strategy for making predictions through machine learning tools in cloud computing environment. *Electronics*, *12*(12), 2650. https://doi.org/10.3390/electronics12122650

[2] Alsharifi, A. K. H. (2023). Total quality management strategies and their impact on digital transformation processes in educational institutions: An exploratory, analytical study of a sample

of teachers in Iraqi universities. *International Academic Journal of Organizational Behavior and Human Resource Management, 10*(1), 1–16.

[3] Alzaidi, E. R. (2024). Optimization of deep learning models to predict lung cancer using chest X-ray images. *International Academic Journal of Science and Engineering*, *11*(1), 351-361. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1140

[4] Aoudni, Y., Donald, C., Farouk, A., Sahay, K. B., Babu, D. V., Tripathi, V., & Dhabliya, D. (2022). Cloud security-based attack detection using transudative learning integrated with Hidden Markov Model. *Pattern recognition letters*, *157*, 16-26. https://doi.org/10.1016/j.patrec.2022.02.012

[5] Attou, H., Mohy-eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., Alabdultif, A., & Almusallam, N. (2023). Towards an intelligent intrusion detection system to detect malicious activities in cloud computing. *Applied Sciences*, *13*(17), 9588. https://doi.org/10.3390/app13179588

[6] Bhattacharya, S., Ghorai, S., & Khan, A. K. (2022). Systematic Study of Detection Mechanism for Network Intrusion in Cloud, Fog, and Internet of Things Using Deep Learning. In *Human-Centric Smart Computing: Proceedings of ICHCSC 2022* (pp. 31-43). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-5403-0_3.

[7] Bhushan, K., & Gupta, B. B. (2019). Network flow analysis for detection and mitigation of Fraudulent Resource Consumption (FRC) attacks in multimedia cloud computing. *Multimedia Tools and Applications*, *78*(4), 4267-4298. https://doi.org/10.1007/s11042-017-5522-z.

[8] Chinnasamy. (2024). A Blockchain and Machine Learning Integrated Hybrid System for Drug Supply Chain Management for the Smart Pharmaceutical Industry. *Clinical Journal for Medicine, Health and Pharmacy, 2*(2), 29-40.

[9] Das, M. S., Govardhan, A., & Doddapaneni, V. L. (2021). A model of cloud forensic application with assurance of cloud log. *International Journal of Digital Crime and Forensics (IJDCF)*, *13*(5), 114-129. https://doi.org/10.4018/IJDCF.20210901.oa7

[10] Deshmukh, S., & Menon, A. (2025). Machine Learning in Malware Analysis and Prevention. *In Essentials in Cyber Defense Periodic Series in Multidisciplinary Studies.* pp. 74-89.

[11] Farhood, A. S. (2023). Analyze the Efficiency of Banking Risk Management in Banks Operating in The Local Environment Through the Application of Basel Standards in Financial Risk Management. *International Academic Journal of Social Sciences, 10 (2), 39–52*. https://doi.org/10.9756/IAJSS/V10I2/IAJSS1011

[12] Farshchi, M., Schneider, J. G., Weber, I., & Grundy, J. (2018). Metric selection and anomaly detection for cloud operations using log and metric correlation analysis. *Journal of Systems and Software*, *137*, 531-549. https://doi.org/10.1016/j.jss.2017.03.012.

[13] Feng, L., Xu, S., Zhang, L., Wu, J., Zhang, J., Chu, C., ... & Shi, H. (2020). Anomaly detection for electricity consumption in cloud computing: framework, methods, applications, and challenges. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), 194. https://doi.org/10.1186/s13638-020-01807-0.

[14] Gunalan, N., Kavin Kumar, R., Saravanan, B., Surya, S., & Saran Sujai, T. (2023). Investing data flow issue by using Rayleigh model in cloud computing. *International Academic Journal of Innovative Research, 10*(1), 8–13. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1002

[15] Idhammad, M., Afdel, K., & Belouch, M. (2018). Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest. *Security and Communication Networks*, *2018*(1), 1263123. https://doi.org/10.1155/2018/1263123.

[16] Jian, Z., Jin, Z., Xie, X., Lu, Y., Li, G., Chen, X., & Baker, T. (2021). Sysnif: A log-based workflow construction method and performance measurement in intelligent IoT system. *Measurement*, *186*, 110175. https://doi.org/10.1016/j.measurement.2021.110175

[17] Kolla, T. (2023). *A Machine Learning Approach to Identifying Malicious DNS Requests through Server Log Analysis* (Doctoral dissertation, Dublin Business School).

[18] Liu, J., Huang, J., Huo, Y., Jiang, Z., Gu, J., Chen, Z., ... & Lyu, M. R. (2023). Scalable and adaptive log-based anomaly detection with expert in the loop.

[19] Moreau, I., & Sinclair, T. (2024). A Secure Blockchain-Enabled Framework for Healthcare Record Management and Patient Data Protection. *Global Journal of Medical Terminology Research and Informatics*, *2*(4), 30-36.

[20] Nakamura, H., & O'Donnell, S. (2025). The Effects of Urbanization on Mental Health: A Comparative Study of Rural and Urban Populations. *Progression Journal of Human Demography and Anthropology*, 27-32.

[21] Patidar, M., & Bansal, P. (2019). Log-Based Approach for Security Implementation in Cloud CRMs. In *Data, Engineering and Applications: Volume 2* (pp. 33-43). Singapore: Springer Singapore.

[22] Rabbani, M., Wang, Y. L., Khoshkangini, R., Jelodar, H., Zhao, R., & Hu, P. (2020). A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing. *Journal of Network and Computer Applications*, *151*, 102507. https://doi.org/10.1016/j.jnca.2019.102507

[23] RM, B., K Mewada, H., & BR, R. (2022). Hybrid machine learning approach based intrusion detection in cloud: A metaheuristic assisted model. *Multiagent and Grid Systems*, *18*(1), 21-43.

[24] Rustogi, R., Agarwal, A., Prasad, A., & Saurabh, S. (2019, October). Machine learning based web-traffic analysis for detection of fraudulent resource consumption attack in cloud. In *IEEE/WIC/ACM International Conference on Web Intelligence* (pp. 456-460). https://doi.org/10.1145/3350546.3352567.

[25] Sanjalawe, Y., & Althobaiti, T. (2023). DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning. *Computers, Materials & Continua*, *75*(2). https://doi.org/10.32604/cmc.2023.037386.

[26] Shah, V., & Bansalm, T. (2023). Multidisciplinary Approaches to Climate Change Monitoring Using Cloud-based Environmental Data Systems. *Cloud-Driven Policy Systems*, 25-31.

[27] Sunil, S., Suresh, A., & Hemamalini, V. (2023, April). Log based anomaly detection: relation between the logs. In *2023 International Conference on Networking and Communications (ICNWC)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICNWC57852.2023.10127571

[28] Wang, B., Hua, Q., Zhang, H., Tan, X., Nan, Y., Chen, R., & Shu, X. (2022). Research on anomaly detection and real-time reliability evaluation with the log of cloud platform. *Alexandria Engineering Journal*, *61*(9), 7183-7193. https://doi.org/10.1016/j.aej.2021.12.061

[29] Wen, L. (2022). Cloud computing intrusion detection technology based on BP-NN. *Wireless Personal Communications*, *126*(3), 1917-1934. https://doi.org/10.1007/s11277-021-08569-y.

[30] Zhang, X. (2022). Application of fusion of fuzzy mathematical clustering analysis in enterprise financial management cloud platform. *Mathematical Problems in Engineering*, *2022*(1), 5354573. https://doi.org/10.1155/2022/5354573

Authors Biography

Dr. Amit Sharma is a Professor in the School of Computer Applications at Lovely Professional University (LPU), Phagwara, Punjab, India. He has extensive teaching and research experience in the field of computer science and applications. His research interests include artificial intelligence, machine learning, big data analytics, and software engineering. Dr. Sharma has published numerous research papers in reputed national and international journals and conferences. He is passionate about fostering innovation, guiding research scholars, and promoting technology-driven education and applied research.

Dr. Amandeep Gill is the Dean of Research and Development (R&D) at Vivekananda Global University, Jaipur, India. He has extensive experience in research management, academic leadership, and innovation-driven education. His areas of expertise include artificial intelligence, data science, machine learning, and emerging technologies. Dr. Gill has published numerous research papers in reputed national and international journals and has been instrumental in fostering a strong research culture within the university. He is dedicated to promoting interdisciplinary collaboration, innovation, and excellence in higher education and research.

Anoop Dev is affiliated with the Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. His research interests focus on interdisciplinary approaches that enhance measurable research impact and outcomes through innovation, data-driven analysis, and strategic academic collaboration. He actively contributes to advancing research quality and visibility within higher education ecosystems.

Dr. Bineet Desai is a Professor in the Department of ISME at ATLAS SkillTech University, Mumbai, Maharashtra, India. He has extensive academic and research experience in the fields of management, innovation, entrepreneurship, and business strategy. Dr. Desai has published several research papers in reputed national and international journals and actively contributes to conferences and professional development programs. His work focuses on bridging the gap between academia and industry through research, innovation, and experiential learning.

V. Haripriya is an Assistant Professor in the Department of Computer Science and Information Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India. She has several years of academic and research experience in the field of computer science education and applied computing. Her primary research interests include artificial intelligence, data analytics, and intelligent information systems, with a focus on developing innovative solutions to real-world challenges. She actively contributes to academic research, publications, and interdisciplinary collaborations aimed at advancing technology-driven education and societal impact.

Dr. Arvind Kumar Pandey is an Associate Professor in the Department of Computer Science and Information Technology at ARKA JAIN University, Jamshedpur, Jharkhand, India. He has significant teaching and research experience in the field of computer science. His areas of expertise include artificial intelligence, machine learning, data analytics, and software engineering. Dr. Pandey has published numerous research papers in reputed national and international journals and conferences. He is actively involved in mentoring students, guiding research projects, and promoting innovation and technology-driven learning in higher education.