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

# AI-Enabled Cloud Security: Malicious Mining Code Recognition for Financial Sectors

Harshit Raichura[1*], Sneha Kashyap[2], Dr. Divya Pant[3], Deepak Minhas[4], Solomon Jebaraj[5], and Pratibha Sharma[6]

[1*]Associate Director, Department of uGDX, ATLAS SkillTech University, Mumbai, Maharashtra, India. harshit.raichura@atlasuniversity.edu.in, https://orcid.org/0009-0005-1361-708X

[2]Assistant Professor, Department of Computer Science & IT, Arka Jain University, Jamshedpur, Jharkhand, India. sneha.k@arkajainuniversity.ac.in, https://orcid.org/0000-0003-0276-9449

[3]Assistant Professor, Jaipuria Institute of Management, Ghaziabad, Uttar Pradesh, India. divyapant2050@gmail.com, https://orcid.org/0000-0003-3874-4016

[4]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh, India. deepak.minhas.orp@chitkara.edu.in, https://orcid.org/0009-0002-0585-6046

[5]Assistant Professor, Department of Computer Science and Information Technology, Jain (Deemed to be University), Bangalore, Karnataka, India. solomon.j@jainuniversity.ac.in, https://orcid.org/0000-0002-3385-207X

[6]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. pratibha.sharma.orp@chitkara.edu.in, https://orcid.org/0009-0000-4708-182X

Received: April 26, 2025; Revised: June 11, 2025; Accepted: July 28, 2025; Published: August 30, 2025

## Abstract

The financial sector has been taking up cloud technology at a fast pace, altering where risks are positioned and making it more difficult to implement security requirements adequately. One of the next-generation online security threats is the malicious mining code. Consequently, this kind of programming is able to cause currency loss by using computer resources secretly and thus resulting in decreased system operation. This research's major goal is to recognise and eliminate the risk factors with a coupling of One-Class Support Vector Machine and Monarch Butterfly Optimisation (COCSVM- MBO), an Artificial Intelligence (AI) method. The technology is capable of discovering patterns representing malicious mining bots via the application of machine learning techniques (Vij & Prashant, 2024). The min-max is implemented for data pre-processing. COCSVM improves security by detecting strange behaviour and patterns in the cloud environment and uncovering malicious mining codes in the banking industry. Through cutting down machinations in cloud systems, malicious code mining detection and information security enhancement, the MBO improves the financial sector security. The data set named FinPile was gathered. It is proposed that the given approach of financial institutions reinforces their resilience against mining attacks by ensuring data security and system integrity. The proposed approach can be able to assist in delivering enhanced resilience and accuracy compared to the traditional classifiers.

*Journal of Internet Services and Information Security (JISIS)*, volume: 15, number: 3 (August), pp. 245-256.
DOI: *10.58346/JISIS.2025.I3.017*

*Corresponding author: Associate Director, Department of uGDX, ATLAS SkillTech University, Mumbai, Maharashtra, India.

**Keywords:** Coupling One-Class Support Vector Machine and Monarch Butterfly Optimization (COCSVM-MBO), Malicious Mining Code, Artificial Intelligence (AI), Cloud Security, Financial Sector.

# 1 Introduction

Cloud security is the safeguarding of data in the cloud that could otherwise be exposed to illegal access, intrusions and data loss due to security threats (Pragadeswaran et al., 2024). It can be understood as a mix of technologies, policies and methodologies that cloud providers use to defend their systems and resources. The central features of cloud security can be segmented as identity and access management (IAM), data encryption, network security, and the function which concerns compliance with industry regulations (Karn et al., 2020). Security in the cloud by introducing strong security mechanisms is inevitable because shared responsibility of security by cloud service providers and users is also necessary. Out-of-hours monitoring, threat detection, as well as incident response measures are required; meanwhile, rising cyber threats for maximum security for cloud (Kannagi et al., 2023).

Malicious mining code is a program that is meant for the stealthy seizure of the computing power of users to mine cryptocurrencies without the permission or awareness of the user. These protocols abuse the computational capabilities of infected devices, e.g. computers, smartphones, or servers, to perform computationally complicated currency transactions (Aldallal & Alisa, 2021). These types of malware can be distributed via phishing emails, compromised websites, or malicious software downloads, but they can stay undetected for long periods, caused by power decrease and increased energy consumption on infected devices. There are critical cybersecurity issues within this system, such as the damaged integrity of information, rising money in energy bills, and risks of further malware or data losses. Diligence against fraudulent emails and timely software updates with strong security (Sulfath et al., 2025) measures are primary factors for mitigating the risk of getting infected by malicious mining code (Ullah et al., 2019).

The financial sector is a system consisting of entities and markets used for money management that involve banking, investment, insurance, and real estate, respectively. Banks, of course, are one of the key players since they make loans, manage deposits, and process payments. Investment firms, among other activities, hold assets like shares, bonds, and mutual funds as they are essential tools to help people get wealthier (Qiu et al., 2019). Insurance providers act as a safety net against different hazards, ranging from health, property, and life. The real estate sector comprises buying, selling, and renting out properties and contributes to the lifestyle of an individual and the prosperity of the business sector. Finally, the financial sector incorporates regulatory bodies, such as central banks and government agencies, whose job is to supervise the work of financial institutions, making the system secure and of high quality (Ashik et al., 2021).

Malicious Mining Code Recognition for Financial Sectors is about developing sophisticated algorithms and tools that are deployed to recognise and fight against the vice of illegal cryptocurrency mining within the financial sector. These institutions are a potent magnet for opportunists who can use the computing resources at their disposal to mine cryptocurrency illegally. It is a challenge to identify such code, as techniques like anomaly detection, behaviour analysis, and signature-based detection are employed to find patterns that demonstrate a cryptojacking activity (Mohammad & Pradhan, 2021)). Financial institutions implement strict cybersecurity measures to protect their infrastructure and avoid unauthorised access, acceptance of which is becoming more and more necessary as the consequences of security breaches may be severe, ranging from financial losses to reputation damage. Through the process of continuous monitoring for malicious mining italic code and acting fast when a threat is detected, financial institutions will lessen the possibility of attacks by these covert criminal tools. Thus, the integrity and security (Ayaz, 2019) of financial operations will be ensured (Muna et al., 2018). A technique that builds a detection model using a coupling One-Class Support Vector Machine with Monarch Butterfly Optimisation (COCSVM-MBO) algorithms is demonstrated to detect malicious mining code initiatives in cloud platforms (Elankavi et al., 2017).

# 2 Related Works

Ashfaq et al., (2022) presented an effective fraud classification framework that makes use of the blockchain system and "machine learning (ML)" approaches to detect fraud and odd activity in transactions made with Bitcoin. Transaction classification and prediction are made possible by integrating the random forest and XGBoost techniques with a comprehensive security evaluation. Vinod et al., (2019) examined the use of ML and empirical estimation in System calls utilised to protect smartphones from malware on the move. The findings demonstrate the effectiveness of classifiers but also their susceptibility to data manipulation and label-flipping attempts. A significant reduction in accuracy in classification was observed in adversarial situations.

Pastor et al., (2020) proposed deep learning and machine learning strategies for crypto mining activities detection, comparing their results to prior studies and conducting experiments with both encrypted and non-encrypted data flows.

Veeraiah et al., (2022) proposed distributed Gaussian process regression to locate risks, lower bandwidth consumption, and repel attacks more quickly in systems based on the cloud. It also seeks to detect and anticipate recognised and unique attacks. Intelligent self-defence techniques can be incorporated by fog computing into dispersed fog nodes, enabling quicker assault scenario management.

Rabbani et al., (2020) suggested a novel method for enhancing security in cloud computing surroundings: employing a particle swarm optimisation-based probabilistic neural network (PSO-PNN) to model user actions. The technique shows promise in identifying harmful behaviour and improving monitoring of security for cloud service suppliers.

Alshammari & Aldribi, (2021) presented a safe identification of fraud strategy that employs blockchain and machine learning technologies to combat fraud and abnormalities within the network of Bitcoin. The model classifies and predicts transactions using XGboost and random forest techniques, and it includes a rigorous security evaluation.

Soviany et al., (2018) presented a machine learning-based solution for malware for Android recognition and detection that incorporates blockchain-based crypto-mining applications and employs a hierarchical categorisation technique with numerous judgment phases.

Mubalaike & Adali, (2018) proposed "deep learning (DL)" techniques as an effective method for identifying scams. Methods from ML, including autoencoders that are stacked and an ensemble of decision trees, were applied. The results showed the utmost level of precision that could be attained, which could help avoid online banking fraud and decrease harm done to individuals or organisations (Sato et al., 2019).

# 3 Methodology

Initially, research gathered the FinPile dataset, and preprocessing used min-max normalisation. To detect malicious mining code using coupling one-class Support Vector Machine with Monarch Butterfly Optimisation (COCSVM-MBO). Figure 1 shows the flow of the proposed method.

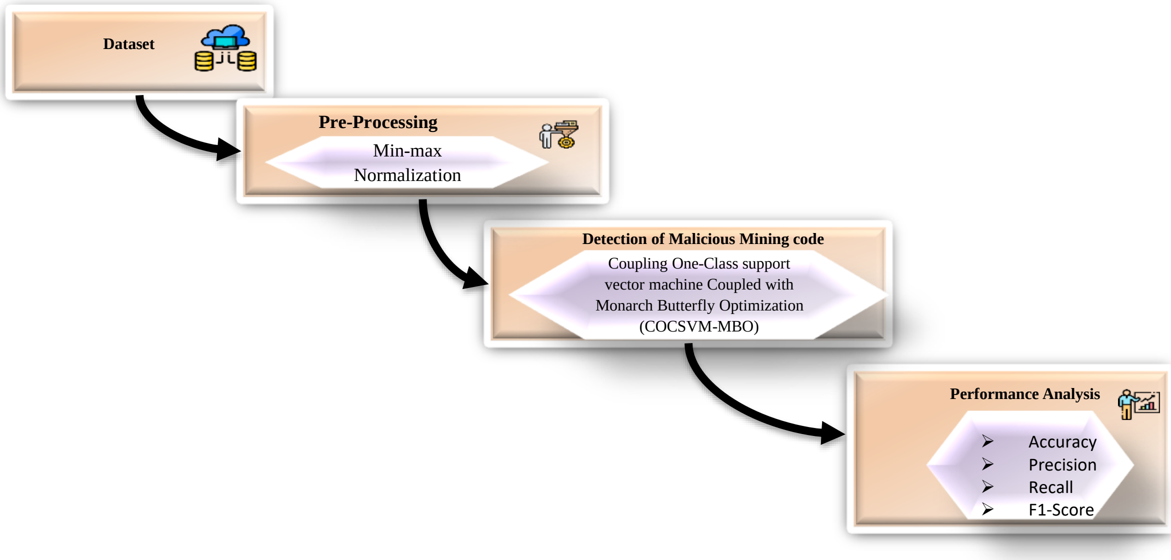


Figure 1: Recognition of Malicious Mining Code Process

### 3.1. Dataset

The dataset was gathered from (Wu et al., 2023). Research created "FinPile", a dataset containing English financial papers from Bloomberg archives, including news, filings, press releases, social media, and web-scraped documents.

### 3.2. Data Preprocessing

#### 3.2.1. Min-Max Normalisation

Min-Max Normalisation in the financial area of cloud security portrays abnormalities, such as illegal mining by scaling all data within a specified range. It does that by normalising attributes that are necessary to protect cryptocurrency mining from illegal purposes.

Min-Max Scaling maps features into a range to give better clarity in finding the malicious mining code in cloud computing for the financial sector. It provides uniformity, relieving the identification of defects and threats.

Min-Max Normalisation is a linear translation of the initial information x into the interval of interest ($New_{min}$, $New_{max}$).

$$w_j = New_{min} + (New_{max} - New_{min}) \times \left(\frac{w_j - w_{min}}{w_{max} - w_{min}}\right) \quad (1)$$

$$w_{max} = \underset{1 \le j \le M}{max w_j}, w_{min} = \underset{1 \le j \le M}{max w_j}$$

This approach scales the data proportionally between ($w_{max}, w_{\min}$)and $New_{min}, New_{max}$. This technique has the benefit of accurately preserving all data value associations. It does not bring any presumptions into the information.

### 3.3. One-class Support Vector Machine (OCSVM)

OCSVM is utilized in cloud security for the financial industry to identify malicious mining code. It improves threat detection by detecting abnormalities according to a single class of data. The basic concept of a one-class "support vector machine (SVM)" is to locate a hyperplane in feature space using the largest margin to split the anticipated data from the original. This is done by mapping the input space using a kernel function to train data from the input space towards the space of features.

Take the training data with$W = \{w_1, w_2, \ldots, w_M\}$, where function $(w_j)$classifies $w_j \epsilon Q^m$as normal or outlier and employs a hyperplane with maximum margin $(x.\Phi(w_j) = \rho)$in feature space $(\Phi(w): W \to G)$ to divide the point of data from the source. $\frac{\rho}{\|x\|}$the separation between the hyperplane and the origin. The inequality constraint and objective function are given below:

$$e(x) = min\frac{\|x\|^2}{2} - \rho + \frac{1}{vM}\sum_{j=1}^{M}\xi_j \tag{2}$$

$$\text{subject to} z_j\left(x.\Phi(w_j) + a\right) \geq \rho - \xi_j, \quad \forall j \epsilon M$$

where$\rho$is the offset or bias term of the hyperplane, and $x$is the weight vector in the feature space. The separation between the ideal hyperplane and the origin, or slack variable $\xi_j \geq 0$, indicates errors in the boundaries of the decision on the data elements. A quantile parameter controls the trade-off between the biggest margin and the number of outliers (errors) $v\epsilon(0,1]$. The given value of parameter v establishes the support vectors with the lower bound of parameter v and indicates the number of anomalies, including the upper bound of $v$. The constrained optimisation issue can be solved using multipliers $\lambda_j \geq 0, \mu_j \geq 0$:and the Lagrange multiplier approach, as outlined in the formulation below:

$$K(x, \xi, \rho, \lambda, \mu) = \frac{\|x\|^2}{2} - \rho + \frac{1}{vM}\sum_{j=1}^{M}\xi_j - \tag{3}$$

By calculating according to the parameters, the derivative $x$and $\rho$, and putting them at zero, the smallest value of the Lagrangian is found. The subsequent restrictions on the multipliers of Lagrange result from converting constraints on inequality to equality.

$$\lambda_j\left[\left(x.\Phi(w_j)\right) - \rho + \xi_j\right] = 0 \tag{4}$$

$$\mu_j\xi_j = 0 \tag{5}$$

The following takes into account the Karush-KuhnTucker (KKT) requirements for every data point $w_j$:

1. The criterion stated by Equation (4) indicates that $\left(x.\Phi(w_j)\right) < \rho$if $\mu_j = 0, \xi_j > 0\ and \lambda_j = \frac{1}{vM}$. Stated otherwise, $\Phi(w_j)$lies between the origin's distance and the hyperplane.
2. Equation (4) implies that $\left(x.\Phi(w_j)\right) = \rho$satisfies the requirement $\xi_j = 0\ and\ 0 < \lambda_j, \frac{1}{vM}$if $(\mu_j > 0\ and \mu_j \neq \frac{1}{vM})$. As a result, $\Phi(w_j)$is a support vector because it is located on the feature space's hyperplane.
3. Equation (4) suggests that $\left(x.\Phi(w_j)\right) > \rho$means $\xi_j = 0\ and \lambda_j = 0$if ui>0 and $(\mu_j > 0\ and \mu_j = \frac{1}{vM})$. $\Phi(w_j)$is a point in the non-support vector feature space that is situated outside the hyperplane. Inferred from the criterion specified by Equation (5) is the absence of exceptions. A kernel function is executed in the input space of the following dual issue to prevent a dot result in the feature space:

$$\min \frac{1}{2} \sum_{j=1}^{M} \lambda_j \lambda_i l(w_j, w_i)$$

$$subject\ to 0 < \lambda_j < \frac{1}{vM}, \sum_{j=1}^{M} \lambda_j = 1 \qquad (6)$$

The following is the derivation of the one-class SVM decision function:

$$e(x) = sign\big(x.\Phi(w_j) - \rho\big) = sign\big(\sum_{J=1}^{M} \lambda_j l(w_j, w) - \sum_{J=1}^{M} \lambda_j l(w_j, w_i)\big) \qquad (7)$$

Any measurement point $w_i$can have its parameter p computed by

$$\rho = \Big(x.\Phi(w_j)\Big) = \sum_{J=1}^{M} \lambda_j l(w_j, w_i) \qquad (8)$$

### 3.4. Monarch Butterfly Optimisation

MBO modifies the behaviour of butterflies to detect harmful mining codes present in cloud financial systems. By quickly identifying risks and optimising detection algorithms, it improves security and protects financial sectors from illicit bitcoin mining activities.

#### 3.4.1. Migration Operator

The whole population of monarch butterfly individuals (solutions), represented by the number $SN$ (solution number), is split into two subpopulations: Sub-population 1 ($SP1$) and Sub-population 2 ($SP2$). The two lands wherein they're situated, Lands 1 and 2, are denoted by the 1 anders $SP1$and $SP2$, accordingly.

$$SP1 = ceil(s.SN) \qquad (9)$$

$$SP2 = SP - SP1 \qquad (10)$$

Where $o$ is the $SP1$ Individual's migration ratio.

The migration procedure is carried out as follows:

$$w_{j,i}^{s+1} = \begin{cases} w_{q1,i}^{s} if q \leq o, \\ w_{q2,i}^{s} otherwise \end{cases} \qquad (11)$$

where j represents the $ith$component and $xt$+1$i$,$j$ is the $ith$element of the $jth$individual at iteration $s+1$. The locations of $q$1and $q$2individuals who are randomly selected from $SP1$and $SP2$, respectively, at iteration $s$, are represented by the symbols $w_{j,i}^{s+1}.w_{q1,i}^{s}$ and $w_{q2,i}^{s}$.

Depending on the value of $q$, either SP1 or SP2 will produce the $ith$} element of the new solution. A random number ($rand$) and the migration period ($peri$) are multiplied to determine the value of $q$.

$$q = rand.peri \qquad (12)$$

where 1.2 is the recommended $peri$ value.

#### 3.4.2. Butterfly Adjusting Operator

The butterfly adjusting operator is the second mechanism that directs the individuals toward the optimal location inside the search space. If $rand \leq o$during this operation, the position will be adjusted using the formula below:

$$w_{j,i}^{s+1} = w_{best,i}^{s} \qquad (13)$$

where$w_{best,i}^{s}$ represents the $ith$parameter of the fittest option at iteration $s$, and $w_{j,i}^{s+1}$ is the updated position of the monarch butterflies.

Alternatively, if the random number exceeds the migration ratio $(rand > o)$, the position updating is carried out using the subsequent formula:

$$w_{j,i}^{s+1} = w_{q3,i}^{s} \tag{14}$$

where, in the current iteration, $w_{q3,i}^{s}$denotes the $ith$element of a selected at random solution from SP2.Moreover, the individual is updated using the following equation if the uniformly distributed number at random exceeds the adjustment rate (butterfly adjustment rate, $BAR$):

$$w_{j,i}^{s+1} = w_{j,i}^{s+1} + \alpha \times (cw_i - 0.5) \tag{15}$$

If $cw_i$denotes the $jth$individual's walk step and $cw$ is acquired via Lévy flight:

$$cw = Levy(w_j^s) \tag{16}$$

This is how the scaling ratio $\alpha$is determined:

$$\alpha = T_{max}/s^2 \tag{17}$$

where$s$indicates the current iteration and $T_{max}$represents the maximum walking step that a person can take at a time.

The proper ratio of diversity to intensification is determined by the parameter $\alpha$. In contrast, if the significance of $\alpha$is smaller, the looking process is carried out in favour of intensification (exploitation); if its value is bigger, the investigation (diversification) is prominent.

### 3.5. Hybrid of COCSVM-MBO

The intersection of the One-Class Support Vector Machine (OCSVM) with Monarch Butterfly Optimisation (MBO) leads to a COCSVM-MBO hybrid that is unmerged but efficient. OCSVM, a machine learning algorithm, is excellent at identifying anomalies using data points either as normal or abnormal and by this, workers can quickly identify outliers in databases with no labels. MBO, a marvel of nature, mines solutions from the butterfly's foraging behaviour by successively adapting parameters upon the outcomes of the fitness assessments. In COCSVM-MBO, OCSVM and MBO collaborate, using OCSVM as a fitness evaluator, helping MBO to locate the best solution from the parameter space. However, this blended technique augments anomaly detection by exploring more solution space and fitting to different forms of data distribution. By connecting the classification skills of OCSVM with MBO optimising power, COCSVM-MBO becomes a relevant expected resolution for the tasks in anomaly detection that would be a problem for the traditional methods if they were used, especially in cases where patterns are complex and unstable.

## 4 Results and Discussion

To assess the effectiveness of the proposed methodology, it is critical to use a variety of quantitative indicators such as "F1-score, recall, accuracy, and precision." The effectiveness of the proposed method is evaluated in comparison to the current methods, CNN, CNN_BN, and RNN_GRU (Wang et al., 2021). With an Intel Xeon CPU running at 2.10 GHz and 36 cores, the machine is outfitted with an Nvidia Titan V GPU and runs Ubuntu 18.04 Linux. Strong computing and development environments are offered by the Python 3.11.8-based framework and APIs.

A model's accuracy determines the overall accuracy of its predictions. Figure 2 assesses and contrasts the accuracy of the proposed method with that of current approaches. Convolutional neural network (CNN), Convolutional neural network and Batch Normalisation regularisation algorithm (CNN_BN), & Recurrent neural network and Gated Recurrent Unit (RNN_GRU) achieved accuracy rates of 98%, 98%, and 95%, in that order. The accuracy rate that our suggested method (COCSVM-MBO) achieved was 98.4%. The suggested method demonstrates that the recognition of malicious mining code in financial sectors is improved by higher accuracy scores.

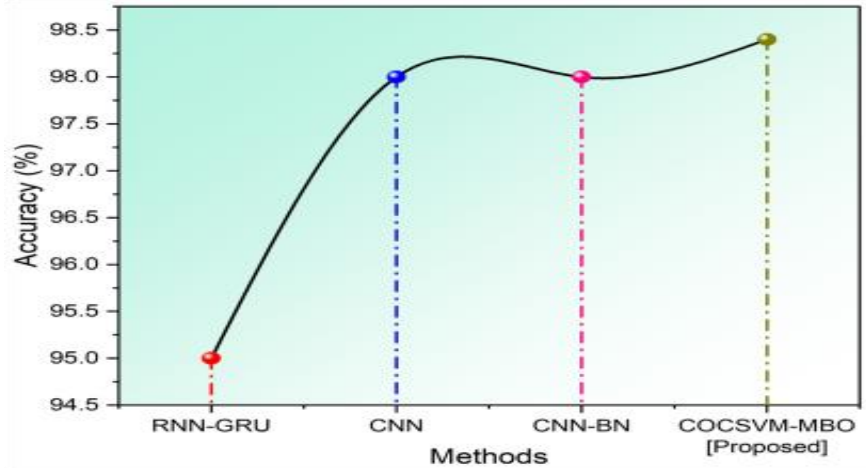


Figure 2: Result of Accuracy

The capacity of a model to accurately identify positive incidents that happen among events that the structure predicts as favourable is measured by its precision. It is computed by dividing the overall amount of true positives by the total amount of genuine positives. Figure 3 assesses and contrasts the precision rate of the proposed method with that of existing approaches. CNN, CNN_BN, & RNN_GRU achieved precision rates of 97%, 96%, and 86%, in that order. Research proposed COCSVM-MBO and achieved a precision rate of 98.3%. The recommended approach shows that greater precision scores enhance the recognition of malicious mining code in the financial sector.

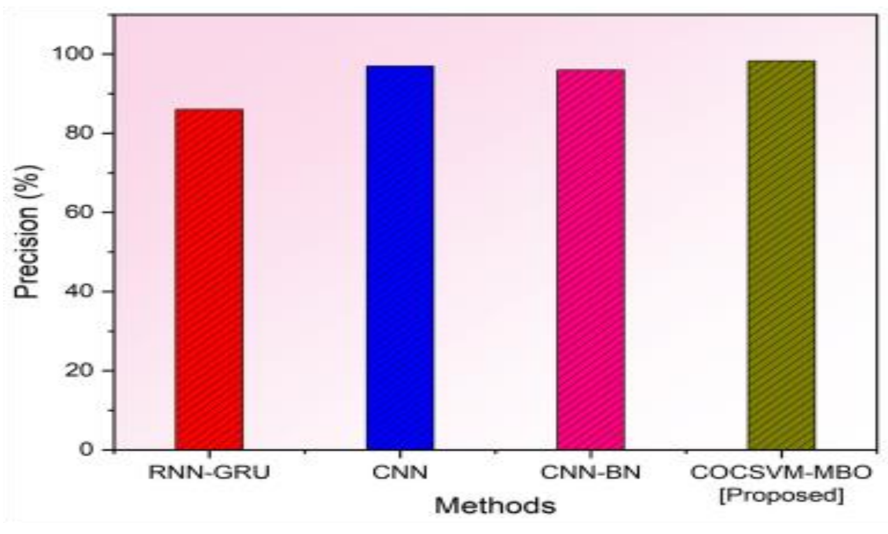


Figure 3: Result of Precision

Recall quantifies a model's precision in accurately identifying every positive instance. In some places, it is also referred to as the real positive rate or sensitivity. Figure 4 assesses and contrasts the recall of the proposed strategy with that of existing approaches. CNN, CNN_BN, & RNN_GRU achieved recall rates of 92%, 94%, and 85%, in that order. The recall rate that our suggested method (COCSVM-MBO) achieved was 96.8%. The proposed approach shows that greater recall scores lead to better recognition of malicious mining code in financial sectors.

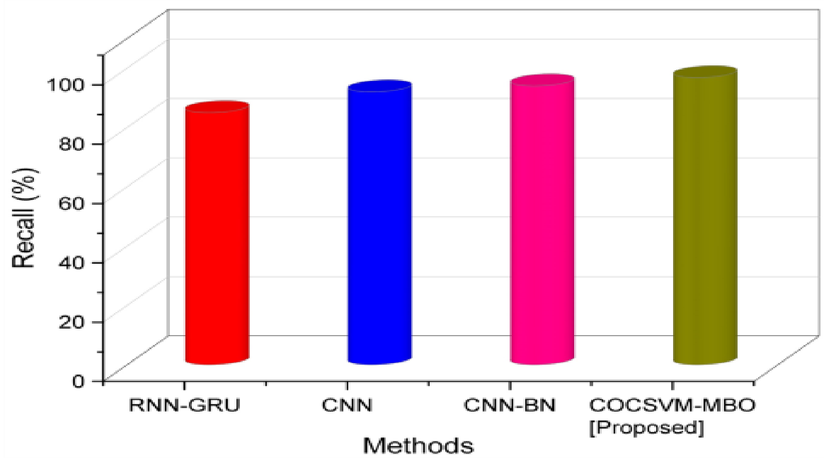


Figure 4: Result of Recall

The F1-score presented an accurate evaluation of a method's effectiveness since it is a periodic mean of recall and precision. It assists in achieving a balance between recall and precision. Figure 5 assesses and contrasts the F1-score of the proposed strategy with that of existing approaches. F1-score rates of 93%, 95%, and 85% were reached by CNN, CNN_BN, & RNN_GRU, in that order. Our suggested method, COCSVM-MBO, achieved a F1-score rate of 97.3%. The proposed approach shows that greater F1-score values enhance the recognition of malicious mining code in financial sectors.

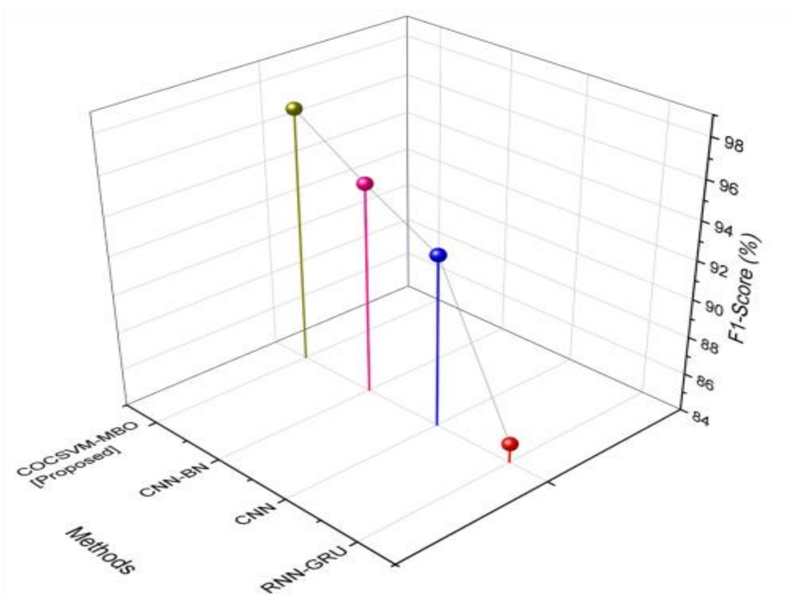


Figure 5: Result of F1-Score

## 5 Conclusion

Finally, the cloud technology that is growing fast in the finance sector has created a breeding ground for the emergence of malicious mining and is now the biggest issue. This research proposes a new AI-powered tool, COCSVM-MBO, which is a special solution for the early detection and mitigation of DoS attacks in a smart electrical grid. Through the integration of machine learning algorithms and by using the FinPile dataset, this approach improves security with the identification of anomalies that could signal a malicious mining operation. By applying COCSVM for detection and MBO for optimisation, a proposed approach reinforces the security of financial institutions against attacks. As a result, the integrity of information is maintained, and operational interruptions in a cloud environment are minimised. Contrary to common classifiers, this approach enables higher accuracy, which has the extra advantage of robustness, and therefore it provides a proactive defence mechanism against the rising risks of malicious mining, that is, it saves the integrity of sensitive financial information and the system in general. The attackers can attempt to sabotage the recognition technique by using adversarial attacks. In the experimental findings, it was demonstrated that the proposed COCSVM-MBO technique achieved the highest values of accuracy (98.4%), f1-score (97.3%), precision (98.3%), and recall (96.8%). These attacks can be categorised in the following way: the inputs are manipulated so that the system detects an activity as benign, which is in actuality malicious or vice versa, and this undermines the reliability of the system. The future perspective also encompasses augmenting detection models with effective adversarial training to prevent attacks that are crafted to subvert the systems. Research on reactive defences, anomaly detection, and ensemble methods has potential, which will help in getting the right diagnosis even in cases of advanced manipulation attempts.

## References

[1] Aldallal, A., & Alisa, F. (2021). Effective intrusion detection system to secure data in the cloud using machine learning. *Symmetry, 13*(12), 2306. https://doi.org/10.3390/sym13122306

[2] Alshammari, A., &Aldribi, A. (2021). Apply machine learning techniques to detect malicious network traffic in cloud computing. *Journal of Big Data, 8*(1), 90. https://doi.org/10.1186/s40537-021-00475-1

[3] Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. *Sensors, 22*(19), 7162. https://doi.org/10.3390/s22197162

[4] Ashik, M., Jyothish, A., Anandaram, S., Vinod, P., Mercaldo, F., Martinelli, F., &Santone, A. (2021). Detection of malicious software by analyzing distinct artifacts using machine learning and deep learning algorithms. *Electronics, 10*(14), 1694. https://doi.org/10.3390/electronics10141694

[5] Ayaz, A. T. (2019). The Role of International Non-governmental Organizations (NGO) in preserving international peace and security. *International Academic Journal of Social Sciences, 6*(1), 62–66. https://doi.org/10.9756/IAJSS/V6I1/1910006

[6] Elankavi, R., Kalaiprasath, R., & Udayakumar, R. (2017). A fast clustering algorithm for high-dimensional data. *International Journal of Civil Engineering and Technology (Ijciet)*, *8*(5), 1220-1227.

[7] Kannagi, A., Mohammed, J. G., Murugan, S. S. G., &Varsha, M. (2023). Intelligent mechanical systems and its applications on online fraud detection analysis using pattern recognition K-nearest neighbor algorithm for cloud security applications. *Materials Today: Proceedings, 81*, 745-749. https://doi.org/10.1016/j.matpr.2021.04.228

[8] Karn, R. R., Kudva, P., Huang, H., Suneja, S., &Elfadel, I. M. (2020). Cryptomining detection in container clouds using system calls and explainable machine learning. *IEEE transactions on parallel and distributed systems*, 32(3), 674-691. https://doi.org/10.1109/TPDS.2020.3029088

[9] 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

[10] Mubalaike, A. M., &Adali, E. (2018, September). Deep learning approach for intelligent financial fraud detection system. *In 2018 3rd International Conference on Computer Science and Engineering (UBMK)* (598-603). IEEE. https://doi.org/10.1109/UBMK.2018.8566574

[11] Muna, A. H., Moustafa, N., &Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. *Journal of information and applications*, *41*, 1-11. https://doi.org/10.1016/j.jisa.2018.05.002

[12] Pastor, A., Mozo, A., Vakaruk, S., Canavese, D., López, D. R., Regano, L., ...&Lioy, A. (2020). Detection of encrypted cryptomining malware connections with machine and deep learning. IEEE Access, 8, 158036-158055. https://doi.org/10.1109/ACCESS.2020.3019658

[13] Pragadeswaran, S., Subha, N., Varunika, S., Moulishwar, P., Sanjay, R., Karthikeyan, P., ... & Vaasavathathaii, E. (2024). Energy Efficient Routing Protocol for Security Analysis Scheme Using Homomorphic Encryption. *Archives for Technical Sciences*, *31*(2), 148-158. https://doi.org/10.70102/afts.2024.1631.148

[14] Qiu, J., Luo, W., Pan, L., Tai, Y., Zhang, J., & Xiang, Y. (2019). Predicting the impact of android malicious samples via machine learning. *IEEE Access*, *7*, 66304-66316. https://doi.org/10.1109/ACCESS.2019.2914311

[15] 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

[16] Sato, S., Hirose, S., & Shikata, J. (2019). Sequential Aggregate MACs from Any MACs: Aggregation and Detecting Functionality. *J. Internet Serv. Inf. Secur.*, *9*(1), 2-23.

[17] Soviany, S., Scheianu, A., Suciu, G., Vulpe, A., Fratu, O., &Istrate, C. (2018, October). Android malware detection and crypto-mining recognition methodology with machine learning. *In 2018 IEEE 16th International conference on embedded and ubiquitous computing (EUC)* (14-21). IEEE. https://doi.org/10.1109/EUC.2018.00010

[18] Sulfath, K. K., Ramakrishnan, P. R., Shareef, P. M., & Shanmugam, H. (2025). Enhancing IT Service Management in Indian IT Organizations: A Technological Integration of ISO 20000 with AI, Blockchain, Predictive Analytics, and Zero Trust Sulfath, K. K., Ramakrishnan, P. R., Shareef, P. M., & Shanmugam, H. (2025). *Indian Journal of Information Sources and Services*, *15*(1), 267–273. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.34

[19] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., &Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. *IEEE access*, *7*, 124379-124389. https://doi.org/10.1109/ACCESS.2019.2937347

[20] Veeraiah, D., Mohanty, R., Kundu, S., Dhabliya, D., Tiwari, M., Jamal, S. S., & Halifa, A. (2022). Detection of malicious cloud bandwidth consumption in cloud computing using machine learning techniques. *Computational Intelligence and Neuroscience*, *2022*(1), 4003403. https://doi.org/10.1155/2022/4003403

[21] 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

[22] Vinod, P., Zemmari, A., & Conti, M. (2019). A machine learning based approach to detect malicious android apps using discriminant system calls. *Future Generation Computer Systems*, *94*, 333-350. https://doi.org/10.1016/j.future.2018.11.021

[23] Wang, H., Long, H., Wang, A., Liu, T., & Fu, H. (2021). Deep learning and regularization algorithms for malicious code classification. *IEEE Access*, *9*, 91512-91523. https://doi.org/10.1109/ACCESS.2021.3090464

[24] Wu, S., Irsoy, O., Lu, S., Dabravolski, V., Dredze, M., Gehrmann, S., ...& Mann, G. (2023). Bloomberggpt: A large language model for finance. https://doi.org/10.48550/arXiv.2303.17564

## Authors Biography

**Harshit Raichura** is the Associate Director in the Department of uGDX at ATLAS SkillTech University, Mumbai, Maharashtra, India. With a leadership role in interdisciplinary design education, his areas of expertise include user-centered design, creative strategy, and academic innovation. Harshit is actively involved in curriculum development, industry collaboration, and mentoring students in emerging areas of design and technology.

**Sneha Kashyap** is an Assistant Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. Her teaching and research interests lie in the fields of computer science, software development, and data-driven technologies. She is dedicated to academic excellence and student mentorship, and actively contributes to institutional research and curriculum enhancement.

**Dr. Divya Pant** is an Assistant Professor at Jaipuria Institute of Management, Ghaziabad, Uttar Pradesh, India. Her academic and research interests include management studies, organizational behavior, and strategic leadership. Dr. Pant is actively engaged in mentoring students, conducting impactful research, and contributing to academic excellence in the field of business and management.

**Deepak Minhas** is affiliated with the Chitkara Centre for Research and Development at Chitkara University, Himachal Pradesh, India. He contributes to research management, academic collaboration, and institutional research impact enhancement. Deepak plays a key role in fostering interdisciplinary projects and supporting the development of high-quality academic outputs.

**Solomon Jebaraj** is an Assistant Professor in the Department of Computer Science and Information Technology at Jain (Deemed-to-be University), Bangalore, Karnataka, India. His academic interests include computer science education, artificial intelligence, and data analytics. He is actively engaged in guiding students, developing innovative teaching methodologies, and contributing to quality research in the field.

**Pratibha Sharma** is affiliated with the Centre of Research Impact and Outcome at Chitkara University, Rajpura, Punjab, India. She is actively involved in enhancing research quality, managing academic collaborations, and supporting impactful scholarly initiatives. Her work focuses on research planning, publication strategies, and institutional development.