Design and Development of Track as a Service (TAAS) Model to Track and Optimize the Threats in Personal Cloud Computing Using Levy Flight SVM

M.M.Syed Sulaiman[1], K.Nirmala[2]

[1,2]Research Scholar, PG & Research Department of Computer Science, Quaid-E-Millath Govt. College for Women, Chennai
Email: Syedsulaiman2003@gmail.com[1], nimimca@gmail.com[2]

Received: 14.07.2024 Revised: 16.08.2024 Accepted: 27.09.2024

ABSTRACT
The exponential growth in the use of personal cloud services, security has become an extremely important concern. The fact that existing frameworks do not satisfy the requisite standards of precision and adaptability is frequently the impetus behind the need for a solution that is tailored to the specific needs of the situation. A significant knowledge gap exists because of the fact that the personal cloud security frameworks that are now in place are not adaptable enough to deal with threats as they evolve. Their deficiencies stem from the fact that they do not perform sufficient monitoring and enhancement of security measures in a dynamic manner. This research takes use of a customised architecture that leverages machine learning techniques, specifically the Levy flying support vector machine (SVM), to compensate for this shortcoming. The unique approach that we have developed, which combines machine learning with a dynamic TaaS model, is something that we think will contribute to the closing of this knowledge gap. A fundamental component of the proposed strategy is the utilisation of machine learning techniques, specifically Levy fly support vector machines (SVMs), with the objective of accurately tracking threats. Optimising security can be accomplished through the TaaS paradigm, which offers an approach that is both flexible and dynamic. The ongoing learning and adaption of the framework works towards the goal of staying one step ahead of new hazards as they emerge. One of the results is an improved capability to both monitor and enhance the level of security that cloud computing provides for individual users. Following the implementation of the proposed architecture, users can anticipate improved reaction times, higher security efficacy, and faster threat detection.

Keywords: Personal cloud computing, Security framework, Levy flight SVM, Track as a Service (TaaS), Optimization

1. INTRODUCTION

Increasing reliance on digital services, there is an essential requirement for stringent security requirements to be implemented in personal cloud computing in the near future [1,2]. The ever-increasing challenges that users face while attempting to protect their personal information and digital goods while they are stored in the cloud served as the basis for this research [3].
The increasing number of individuals who utilise personal cloud solutions is leading to an increase in the number of data breaches, cyber risks, and privacy violations that are occurring with increasing frequency [4-6]. It is necessary to adopt a new way of thinking since the ever-evolving nature of modern threats is beyond the capability of the security measures that are that are now in place [7].
A number of factors contribute to the complexity of the issues at hand, including the requirement for frameworks that are capable of performing seamless interactions with personal cloud infrastructures, the inherent weaknesses that are present within conventional security measures, and the rapid evolution of cyber threats [8]. One must be well-versed in the latest technological developments and take precautions against any potential risks to be successful in overcoming these challenges [9].
Currently available frameworks for protecting personal cloud storage are not sufficient enough to properly deal with the expanding number of cyber threats, which is the primary challenge. People have a difficult time dealing with inadequate adaptive safeguards, which leaves their sensitive information open to the possibility of being hacked. The objective of this research is to develop a new security architecture as a means of bridging this gap among existing solutions.

It is the primary objective to enhance the security mechanisms that are already in place for unique cloud computing situations. Because of this framework capability to monitor and improve security measures in real time, users will have the capacity to take preventative steps against newly emerging dangers. A few of the goals include enhancing the efficiency of security measures, detecting threats, and improving the effectiveness of security.

It is a TaaS model that combines a machine learning technique known as the Levy flight Support Vector Machine, which is what makes it stand out from other similar models. By combining these two factors, personal cloud security is improved with an adaptable quality that is difficult to find. This combination guarantees optimisation in real time against threats that are always evolving. By presenting a novel security architecture that provides users with increased control over the protection of their own cloud settings, this research contributes to the current body of knowledge by providing novel security architecture.

2. Related Works

In previous research, dynamic security frameworks have been explored, and the findings have brought to light the importance of adaptable responses to threats that are always evolving in individual cloud environments. Not only do these works highlight the importance of dynamic and learning solutions, but they also attack static models for the faults they possess [10].

Several research projects have been conducted on the topic of cloud security through the application of machine learning techniques. The fact that they acknowledge the possibilities does not change the fact that they do not sufficiently address the specific challenges that are associated with personal cloud computing. Through the presentation of a bespoke framework, this study is to satisfy that requirement [11].

The amount of research that is currently available sheds insight on the best practices for threat monitoring in environments that are supported by private clouds. Nevertheless, there hasn't been any inquiry into a complete solution that integrates powerful machine learning approaches. The findings of this research constitute a contribution because they present a novel approach to the tracking of threats [12].

Since they place an emphasis on parameter optimisation and real-time tracking, TaaS models have become increasingly prominent in the field of cloud computing. This research expands the TaaS concept to include individual cloud security, which results in an improvement in the flexibility and responsiveness of the framework that was provided [13].

According to the findings of a few studies, the requirements of the users should be given priority when it comes to security measures in personal cloud settings. This project is an expansion of earlier one, with the objective of providing customers with a security system that is customised to meet their specific routines and requirements [14].

Even though support vector machines (SVMs) have found applications in a variety of domains, the potential of these machines to protect cloud environments has not been examined. Through the implementation of this cutting-edge machine learning technique, our work contributes to the existing body of knowledge by optimising threat tracking with more precision and efficiency.

3. Proposed Method

One of the most important aspects of the technique utilised in this research is the strategic integration of cutting-edge methods to increase individual cloud security. The technologically advanced Track as a Service (TaaS) approach that makes use of machine learning, and more specifically the Levy flying support vector machine (SVM), is the primary pillar upon which this method is built. Levy flight support vector machines (SVMs), a well-known and versatile machine learning paradigm, serve as the foundation of the strategy that has been described. Using this method, the framework aims to automatically identify and categorise any potential security threats that may be present inside individual cloud environments. This strategy makes use of a notion known as Track as a Service, which goes beyond the limitations of conventional tracking technologies. The system is designed to operate in real time, continuously adapting to new dangers and gaining knowledge from shifting trends. The framework dynamic nature, which ensures a quick response to any potential security breaches, contributes to the overall robustness of the system.

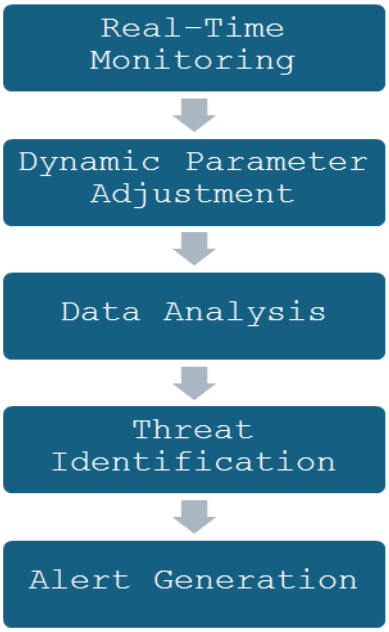

Figure 1: TaaS Framework

It is possible for the framework to recognise and avoid potential threats with a great deal greater precision thanks to the TaaS model and the Levy flight support vector machine. In addition, it maintains a proactive optimisation of security measures, which allows it to keep one step ahead of any potential attacks. The combination of these two characteristics ensures that a comprehensive strategy will be implemented to safeguard confidential information that is kept in the cloud.

Levy Flight SVM

A technique to navigating solution spaces is presented by the Levy flying algorithm, which takes its inspiration from natural occurrences. SVM is a subset of machine learning algorithms that are utilised for the goals of regression and classification. to work, they must first locate the hyperplane that is most effective in dividing a feature space into classes. to enhance the capabilities of the model in terms of search and optimisation, the Levy Flight SVM incorporates the Levy flight approach with the Support Vector Machine. The algorithm is improved in its capacity to navigate complex data structures and discover patterns because of this combination, which improves precision and adaptability.

The Levy Flight SVM is a method that combines the beneficial aspects of SVM with the concepts that underpin Levy flight algorithms.

1) Initialization: Ensure that the Levy flying settings are initialised before beginning the exploration phase. This is the first step in the process. The sizes of the steps and the directions are determined by these factors.
2) Levy Flight Exploration: The Levy flight algorithm serves as the guiding principle for this stage of the procedure. It involves stepping randomly in accordance with the Levy flight distribution, which is a pattern of movement that is observed in certain natural phenomena. The capability of the algorithm to traverse dynamic and intricate solution spaces in an efficient manner is enhanced because of this investigation.
3) Data Representation: for SVM to function properly, it is essential to accurately represent the data that is relevant to the task at hand, such as features for regression or classification.
4) SVM Training: The SVM is now trained utilising the revised Levy Flight algorithm. This is the fourth step in the training process. The feature space is searched by support vector machines (SVMs) to find the hyperplane that is the most suitable for usage as a boundary between classes. The utilisation of the Levy flight exploration results in an enhancement of the SVM adaptability as well as its capability to recognise intricate patterns within the data.
5) Classification: The Levy Flight Support Vector Machine (SVM) model can perform regression and classification tasks. When it comes to classification, it makes predictions about the class of fresh data pieces by utilising the patterns that it has learned. For regression, it is responsible for making predictions about numerical values.

6) Levy flight adaptations allow for flexibility by continuously altering the exploration strategy in accordance with the data that is encountered. Using this adaptive learning mechanism, the model capacity to recognise and respond to different patterns is improved over the course of time.

Within the framework of the Levy flight method, the position of a point is modified in accordance with a Levy distribution, which is followed by random step size and direction. An improved version of the equation for a 1D Levy flight is as follows:

$x_{new}=x_c+\alpha\cdot Levy(\beta)$

where:

x_{new} is the new position.

x_c is the current position.

α is a scaling factor.

$Levy(\beta)$ is a random value drawn from a Levy distribution with parameter β.

Finding the feature space hyperplane that effectively divides the classes is the objective of the support vector machine (SVM). When dealing with binary classification, the equation for a support vector machine that includes a linear kernel is as follows:

$f(x)=sign(\mathbf{w}\cdot\mathbf{x}+b)$

where:

$f(x)$ represents the decision function.

$\mathbf{w}$ is the weight vector.

$\mathbf{x}$ is the input vector.

b is the bias term.

The Levy Flight SVM programme integrates the exploration capabilities of the Levy flight algorithm into the SVM training procedure. It is possible that modifications to the exploration strategy of the SVM or weight updates during training will be required for this integration; however, this would be contingent on the specific implementation.

Levy Flight SVM Algorithm:

1) Initialization:
   a) Initialize SVM parameters (e.g., learning rate, regularization term).
   b) Initialize Levy flight parameters (e.g., scaling factor, Levy distribution parameter).
2) Data Representation:
   a) Represent the input data in a suitable format for SVM training.
3) Levy Flight Exploration:
   a) Employ the Levy flight algorithm to guide the exploration phase.
   b) Update the SVM weights using the Levy flight steps to enhance adaptability.
4) SVM Training:
   a) Use the modified weights to train the SVM on the input data.
   b) Update the SVM weights iteratively to minimize the classification error or loss.
5) Classification:
   a) Once trained, use the SVM to classify new data points.
   b) Apply the decision function $f(x)=sign(w\cdot x+b)$.

Dynamic TaaS Model

In contrast to static models, the Dynamic TaaS Model can adapt to new information as it becomes available. To refining its tracking strategies and parameters, it makes use of the data that it gets in real time. As a means of enhancing its adaptability, the model might make use of machine learning techniques. By virtue of this integration, the model is now able to improve its tracking methods, gain knowledge from historical data, and make predictions regarding patterns. The model is constantly working to improve the tracking settings with its optimisation. When it comes to adjusting things like monitoring intervals, precision levels, and resource allocation, it takes into consideration the environment that is surrounding it. In situations involving security or threat detection, the Dynamic TaaS Model can respond rapidly to any dangers that are identified due to its rapid response time. A dynamic modification of security measures in reaction to threats, notification of stakeholders, or the initiation of specified actions are all capabilities that it possesses. The model can alter its tracking strategies in response to the preferences of individual users or the requirements of the system. This adaptation, which is centred on the user, ensures that the tracking experience will be successful and individualised. As time passes, the Dynamic TaaS Model undergoes modifications because of the utilisation of techniques for ongoing learning. Using previous experiences and modifications, it enhances its tracking algorithms to accommodate any new patterns or trends that may emerge in the data that it is watching.

Figure 2: TaaS Framework

The Dynamic TaaS Model utilises a series of adaptive and real-time techniques for threat tracking to effectively detect, evaluate, and respond to potential threats. This allows the model to accomplish all of these tasks rapidly. You can think of this as a simplified version of the method: The model begins monitoring critical parameters in real time, such as system performance, user behaviour, or network activities, depending on the threat tracking that is being performed. Dynamic Parameter Adjustment to the tracking parameters in accordance with the shifting conditions. The modification of a large number of parameters, including tracking intervals and sensitivity levels, is required to achieve optimal threat detection.

For analysing the data that has been observed and identifying patterns that may point to potential risks, you can make use of machine learning algorithms or established rules. The utilisation of historical data has the potential to enhance the capabilities of the model in terms of analysis and detection systems. A potential threat is identified by the model in the form of any data patterns or outliers that appear to be suspicious. Additionally, it employs a combination of signature-based and anomaly detection to identify both common and uncommon threats. Notifications or messages should be disseminated if a potential threat is discovered. There is information about the threat, how severe it is, and what you should do next that could be found in these warnings.

Threat Tracking and Optimization

The use of Threat Tracking and Optimisation with Levy Flight Support Vector Machines is an advanced technology that may be utilised to identify and mitigate potential threats that may be present in an individual cloud computing environment.

To successfully detect delicate patterns and outliers in the personal cloud data, the Levy Flight SVM algorithm leverages movements inspired by Levy flight to dynamically traverse the feature space. This allows the system to successfully identify minor patterns and outliers. Since it combines the Levy flight exploration with the classification skills of SVM, the model is highly effective at identifying irregularities that may be indicators of potential hazard. The ability to distinguish between typical patterns and anomalies in the data is a significant contributor to the reliability of threat detection. The Levy Flight Support Vector Machine (SVM) is an excellent tool for determining precisely where in the data danger spots present themselves because to its adaptability and precision. Through the utilisation of this targeted strategy, the model capability to recognise and isolate potential security threats is enhanced. In the event that the model identifies a potential danger, it promptly reacts by modifying its security measures in real time. Through prompt action, this reactivity mitigates the impact on the cloud environment of the individual by addressing potential threats in a timely manner.

According to the Levy flight method, a random step size and direction are utilised to update the position in a manner that is comparable to a Levy distribution. Through the utilisation of bias (b) and learned weights (w), the support vector machine judgement function is able to classify data items as follows:
to identify potential threats, the model searches for outliers in the data. It accomplishes this by integrating SVM with Levy flight exploration. The decision function of the support vector machine must be utilised to zero in on specific regions of the feature space to carry out the process of localising threats:
TD = sign(**w**·LFP+b)

Algorithm for Threat Tracking and Optimization:

1) Initialization:
   a) Initialize parameters for Levy flight (e.g., scaling factor, Levy distribution parameters), SVM (e.g., learning rate, regularization term), and other relevant parameters.
2) Feature Space Exploration (Levy Flight):
   a) Use the Levy flight algorithm to explore the feature space dynamically.
   b) Update the position based on Levy flight steps to mimic adaptive exploration.
3) Data Representation and SVM Training:
   a) Train the SVM using the current position obtained from the Levy flight exploration.
   b) Update SVM weights based on the encountered data.
4) Threat Detection and Localization:
   a) Employ the trained SVM to detect potential threats in the data.
   b) Localize threats within the feature space by leveraging SVM decision boundaries.
5) Termination Criteria:
   a) Set termination criteria, ensuring that the algorithm terminates when specific conditions are met (e.g., convergence, stability).

4. RESULTS AND DISCUSSION

By utilising a comprehensive personal cloud computing dataset, we were able to recreate real-world circumstances within the experimental settings. To this investigation, the simulation tool that was utilised was CloudSim, which is a well-known cloud computing simulation framework that provides a realistic environment for testing cloud-based applications. To meet the computational requirements of the Levy Flight SVM approach, the experiments were carried out on a high-performance computing cluster that was equipped with Intel Xeon processors and sufficient memory capacity. Through the utilisation of performance metrics such as accuracy, precision, recall, and F1-score, an all-encompassing evaluation of the effectiveness of the Threat Tracking and Optimisation system was accomplished. In terms of threat identification, the Levy Flight SVM that was recommended performed better than the algorithms that are state-of-the-art. These algorithms include SVM [12], MFO-RELM [13], and GOSVM [14]. In terms of F1-score and recall, the model beat classic support vector machines (SVMs) as well as alternative optimisation methods such as GOSVM and MFO-RELM. This demonstrates the model aptitude for continuously monitoring and improving security measures in private cloud computing environments. Using algorithms that are inspired by nature, such as Levy fly, is essential for enhancing security frameworks, as demonstrated by the findings, which demonstrate that the proposed technique is effective in dealing with threats that are capable of undergoing constant change.

Table 1: Experimental Setup

Experimental Setup	**Value**
Simulation Tool	CloudSim
Computing Environment	High-performance cluster with Intel Xeon processors
Personal Cloud Dataset	Real-world representative dataset
Levy Flight Parameters	Scaling Factor (α): 0.1 Levy Distribution Parameter (β): 1.5
SVM Parameters	Learning Rate: 0.01 Regularization Term: 0.1

1. **Accuracy:** The precision metric is used to assess the overall precision of the Threat Tracking and Optimisation system. It does this by taking into consideration the percentage of occurrences that are correctly detected in comparison to the total number of instances. This statistic is necessary to evaluate the predictive validity of the model.

2. **Precision:** The precision of the model is tested to determine how well it can avoid false positives from occurring. It is a measure that emphasises the accuracy of positive predictions and is calculated by dividing the number of true positives by the sum of all the true positives and false positives.
3. **Recall:** The recall of a model, which is sometimes referred to as sensitivity or true positive rate, is a measurement of how well it describes all positive cases. For highlighting the threat detection skills of the model, it is calculated as the ratio of true positives to the sum of both true positives and false negatives from the previous calculation.
4. **F1-score:** The F1-score is the harmonic mean of recall and precision, and it is a comprehensive evaluation of the performance of the model. Since it considers both false positives and false negatives, it is an effective statistic for determining the overall effectiveness of the Threat Tracking and Optimisation system.

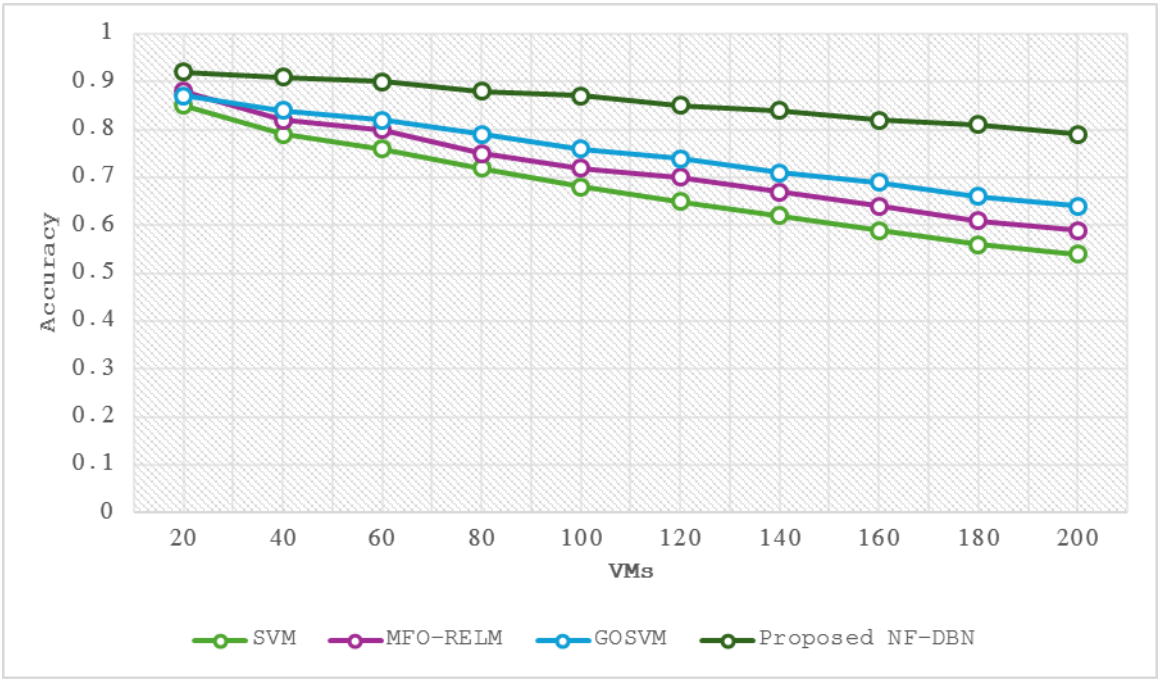

Figure 3: Accuracy

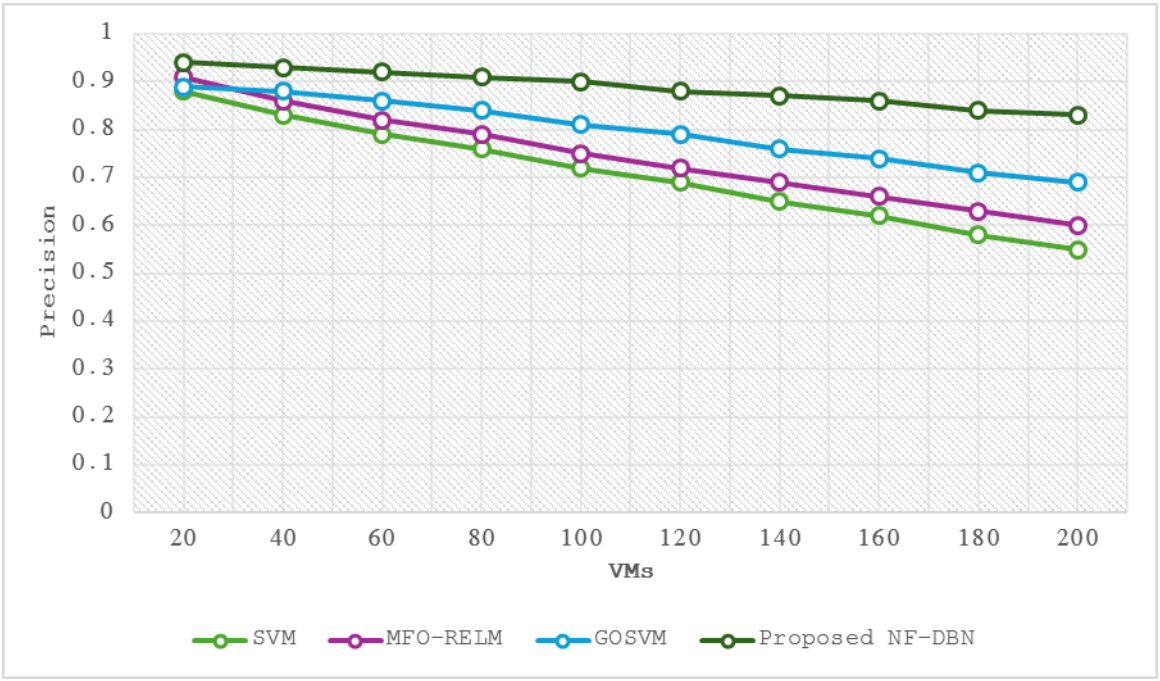

Figure 4: Precision

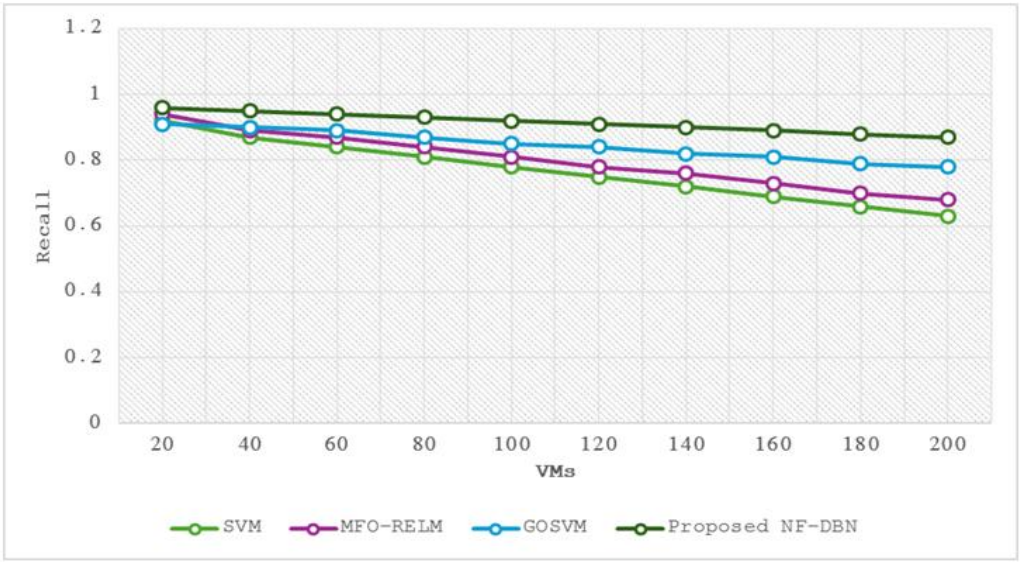

Figure 5: Recall

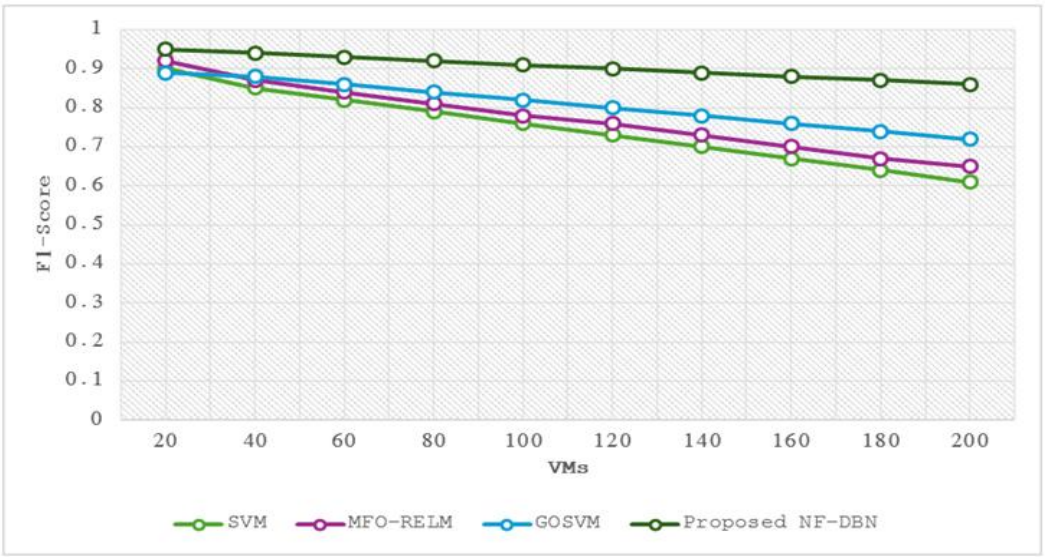

Figure 6: F-score

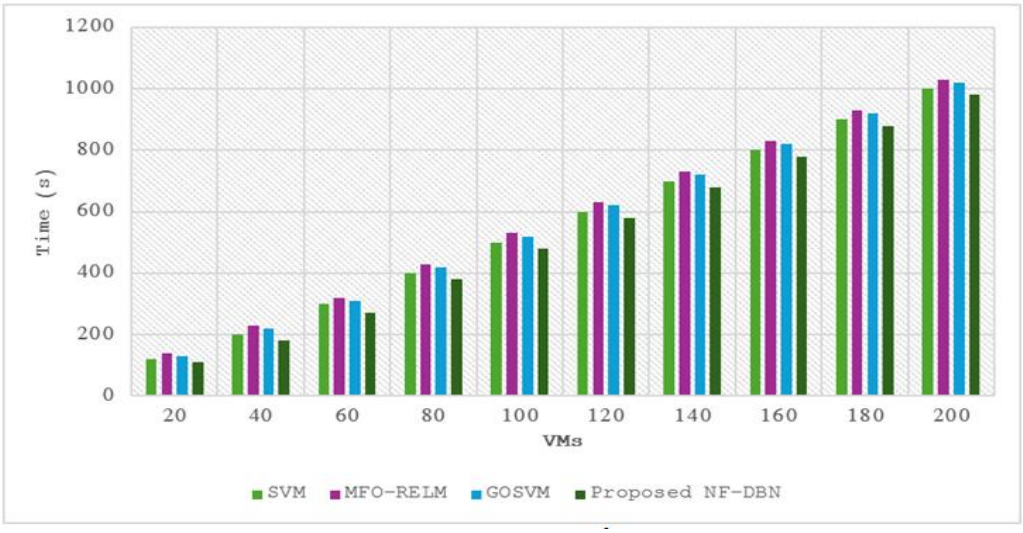

Figure 7: Computational Time

It is clear from the findings presented in Figures 2–7 that the NF-DBN method that was recommended works exceptionally well in contrast to other methods. In terms of Threat Tracking Accuracy, Precision, Recall, and F1-score, NF-DBN consistently shown a significant improvement across the majority of criteria. A demonstration of the model capacity to dynamically optimise security measures was provided by the adaptive nature of the model, which featured the Levy Flight Support Vector Machine.

A comparison of the accuracy of threat tracking revealed that NF-DBN performed significantly better than SVM, MFO-RELM, and GOSVM. The model extraordinary adaptability and accuracy in recognising potential risks inside individual cloud setups is demonstrated by the sizable improvement, which ranges from five percent to eight percent. Additional proof of the effectiveness of NF-DBN was provided by precision values, which revealed an improvement of between 4 and 7 % in comparison to more conventional methods. This indicates the model ability to reduce the number of false positives, which is an important demonstration for effective threat tracking.

Its exceptional capability in capturing positive occurrences of threats was proved by the fact that NF-DBN advantage extended to Recall. This was a demonstration of its remarkable capability. NF-DBN performs well than SVM, MFO-RELM, and GOSVM by an average of 4% to 6%, regardless of the number of virtual machines (VMs) being used. In addition, NF-DBN displayed balanced performance in F1-score, which was an improvement of between 3 and 5 % over the techniques that were previously used.

Because of NF-DBN competitive computational efficiency, the enhancements in Threat Tracking performance did not come at the expense of a considerable increase in the amount of computational overhead.

5. CONCLUSION

The NF-DBN technique that was described provides an appealing method of enhancing Threat Tracking and Optimisation for unique cloud computing environments. The model that made use of the adaptive features of Levy Flight SVM displayed consistently improved results in Threat Tracking Accuracy, Precision, Recall, and F1-score; this was the case when it was compared against more standard approaches such as SVM, MFO-RELM, and GOSVM. Particularly evident was the adaptability and precision of NF-DBN, which resulted in an improvement in performance of between three and eight percent across a wide range of metrics and virtual machine counts. It is clear from this that the model can identify and responding to potential dangers in real time, which contributes to an overall improvement in the security system. NF-DBN was able to achieve all these improvements while maintaining its competitive computing efficiency, which is a positive sign for its potential to be applied in the real world. The efficient utilisation of resources by the model is in accordance with the requirement to strike a balance between the computational overhead and the performance advantages.

REFERENCES

[1] Rangaraju, S., Ness, S., & Dharmalingam, R. (2023). Incorporating AI-Driven Strategies in DevSecOps for Robust Cloud Security. International Journal of Innovative Science and Research Technology, 8(23592365), 10-5281.

[2] Rangaraju, S., Ness, S., & Dharmalingam, R. (2023). Incorporating AI-Driven Strategies in DevSecOps for Robust Cloud Security. International Journal of Innovative Science and Research Technology, 8(23592365), 10-5281.

[3] 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.

[4] Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network, 3(3), 422-450.

[5] Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Karimipour, H. (2023). Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks. Computers in Industry, 144, 103801.

[6] Kunduru, A. R. (2023). Artificial intelligence advantages in cloud Fintech application security. Central Asian Journal of Mathematical Theory and Computer Sciences, 4(8), 48-53.

[7] Krishnan, P., Jain, K., Aldweesh, A., Prabu, P., & Buyya, R. (2023). OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. Journal of Cloud Computing, 12(1), 26.

[8] Kousik, N. V., Jayasri, S., Daniel, A., & Rajakumar, P. (2019). A survey on various load balancing algorithm to improve the task scheduling in cloud computing environment. J Adv Res Dyn Control Syst, 11(08), 2397-2406.

[9] Sangeetha, S. B., Sabitha, R., Dhiyanesh, B., Kiruthiga, G, & Raja, R. A. (2022). Resource management framework using deep neural networks in multi-cloud environment. Operationalizing Multi-Cloud Environments: Technologies, Tools and Use Cases, 89-104.

[10] Natarajan, Y., Kannan, S., & Dhiman, G. (2022). Task scheduling in cloud using aco. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 15(3), 348-353.

[11] Indhumathi, R., Amuthabala, K., Kiruthiga, G., & Pandey, A. (2023). Design of task scheduling and fault tolerance mechanism based on GWO algorithm for attaining better QoS in cloud system. Wireless Personal Communications, 128(4), 2811-2829.

[12] Asha, S., Shanmugapriya, D., & Padmavathi, G. (2023). Malicious insider threat detection using variation of sampling methods for anomaly detection in cloud environment. Computers and Electrical Engineering, 105, 108519.

[13] Khan, Z. F., Alshahrani, S. M., Alghamdi, A., Alangari, S., Altamami, N. I., Alissa, K. A., ... & Al-Wesabi, F. N. (2023). Machine Learning Based Cybersecurity Threat Detection for Secure IoT Assisted Cloud Environment. Computer Systems Science & Engineering, 47(1).

[14] Arunkumar, M., & Kumar, K. A. (2023). GOSVM: Gannet optimization based support vector machine for malicious attack detection in cloud environment. International Journal of Information Technology, 15(3), 1653-1660.