Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Early Cloud Computing Intrusion Detection Using Time Series Data: A Multivariate Neural Model and Improved Zebra Optimization Algorithm Approach

Aditya Kumar Shukla[1], Ashish Sharma[2 *]

[1]Research Scholar, Department of Computer Engineering and Applications, GLA University, NH#2, Delhi Mathura Highway, Post Ajhai, Mathura (UP) India

Email Id: uraditya@gmail.com

[2]Department of Computer Engineering and Applications, GLA University, NH#2, Delhi Mathura Highway, Post Ajhai, Mathura (UP) India

*Corresponding Email: ashishs.sharma@gla.ac.in

ARTICLE INFO

Received: 25 Dec 2024

Revised: 15 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Utilizing the cloud is not growing as fast as it might because of security and privacy issues. False positives are still a problem with network intrusion detection systems (NIDS), even with their widespread usage. Moreover, the intrusion detection problem has not been treated as a time series problem, necessitating time series modelling, in many research. In this paper, we use time series data to suggest a unique method for early cloud computing intrusion detection. Our strategy uses a forecasting model built using the Multivariate Neural Model of the prophet and an Improved Zebra Optimization Algorithm (IZOA) to gauge its effectiveness. The problem of making false linkages between time series anomalies and assaults is particularly addressed by this method. Our findings show a notable decrease in the quantity of forecasters used within our forecast model—from 70 to 10—while demonstrating an improvement in performance metrics like median absolute percentage error (MDAPE), dynamic temporal warping (DTW), mean absolute percentage error (MAPE), mean square error (MSE), root mean square error (RMSE), and mean absolute error (MAE). In addition, our method has shown reductions in cross-validation, forecasting, as well as training durations of around 97%, 15%, and 85%, respectively.

Keyword: Cloud Computing Security, Intrusion Detection, Time Series Analysis, Multivariate neural Prophet, Machine Learning

INTRODUCTION

Cloud computing is a rapidly expanding subject that involves computing over the internet. It utilizes virtual desktops and shared servers to provide platforms, resources, software, and infrastructure [1]. The open structure of cloud computing renders it susceptible to attacks. Security and privacy arevital for The triumph of cloud computing [2]. Traditional security protocols are inadequate for providing suitable answers to this challenge. Two types of attacks, The Sybil assault and the Denial of Service (Do's) inevitable forms of assault [3]. Among the most established and crucial online safety problems is detecting malicious network activities. Due to the diverse range of technologies employed and the rapid growth of networks, security concerns have become increasingly intricate. Furthermore, unusual network behavior is often misconstrued as indicating a compromised device or network [4].

To safeguard cloud settings from a range of dangers as well as assaults, Systems for detecting intrusions (IDS) have emerged as the greatest often employed element of the safety and security of computer

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

systems protocols [5]. Intrusion Detection Systems (IDS) employ various reaction mechanisms to detect vulnerabilities, uncover illicit activity, and put into action preventive actions to keep pace Using the advancements in offenses involving computers [6]. However, a recent assessment of studies has found limited investigation into the issue with intrusion detection from a sequence of times perspective [7].

This paper introduces a new method for efficiently identifying intrusions in cloud computing at an early stage by employing temporal sequence data novel Zebra Algorithm A strategy for selecting characteristics is suggested, which incorporates temporal sequence analytic methods utilizing detecting anomalies, stationary, and causal relationships testing to effectively tackle the problem of false associations the relationship between anomalies and assaults. The approach was assessed use the dataset CSE-CIC-ID2018. The information pretreatment stage was conducted use of IDS-Dataset-Cleaning program, and the consistency was assessed with the KPSS assessment. The information was further divided into 5-minute intervals, and only Granger causality in columns values below A 0.05 were chosen. The anomalies were then identified using the ADTK tool. A matrix of Granger causality was computed using the specified temporal range, and only peculiarities that had an impact on future attack labels were chosen.

Furthermore, the study introduces an anticipatory model that utilizes the Facebook Prophet framework to assess the efficacy of the suggested technique, alongside the suggested collaborative feature selection approach. The performed experiments have shown that the forecasters used inside the forecasting model include greatly enhanced the performance indicators and decreased the resource's intricacy use of the prototype. The evaluation outcomes demonstrated a noteworthy improvement in forecasting accuracy, a reduction Within the overall quantity of predictors in the input, and a reduction in the forecasting time. The predictor count was decreased from 70 to 10, resulting in enhanced execution indicators, such as DTW, MAE, MSE, RMSE, MAPE, and MdAPE. Cloud computing is the term used to describe the provision offering computer support over World Wide Web, where users pay for the services they use. Cloud computing presents various benefits, including scalability, flexibility, affordability, and accessibility [8]. However, moreover, it given rise to safety and difficulties and worries. Online storage and processing involves the identification and response to unlawful entry, malevolent actions, stability, and safety threats, which is known as intrusion detection [9]. Among the challenges in protection against cloud computing intrusions is the large amount amounts of data requiring analysis in real-time. Artificial intelligence algorithms possess the ability to handle substantial amounts information and detect trends as well as irregularities that could potentially signify compromises in system security. Consequently, they serve as crucial instruments in safeguarding safety and dependability to systems hosted in the cloud and apps. By using the capabilities of artificial intelligence, enterprises can enhance safety and dependability across all of their online platforms and apps [10].

The fundamental contribution of this work is the invention and implementation of the Improved Zebra Optimization Algorithm (IZOA) to maximize the performance of the Multivariate Neural Prophet model, a unique technique that has not previously been investigated in the literature. The IZOA improves the traditional Zebra Optimization Algorithm by dynamically modifying its parameters, hence increasing the convergence rate and accuracy of the optimization process. This adaptive approach enables the algorithm to explore complicated search spaces while avoiding local optima, resulting in improved overall model tuning performance. Therefore, this study contributes new information to the domains of optimization algorithms and machine learning by giving a flexible tool for improving predictive modelling skills in a variety of applications.

Related Work

Network security faces significant threats from the daily discovery of new vulnerabilities swiftly exploited in zero-day attacks. Researchers have developed numerous technologies for network security, including firewalls, intrusion detection systems (IDSs), and honeypots. IDSs are common active defense systems used to detect and identify unauthorized access in various network contexts. They are crucial for improving network security and protecting user privacy and data. IDSs are categorized into misuse-based and anomaly-based systems. Misuse-based IDSs identify network intrusions using known attack signatures but suffer from high false-negative rates and limited flexibility in handling diverse application scenarios [11]. In contrast, anomaly-based IDSs can identify new types of attacks but have

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

a significant false-positive rate. Recently, researchers have focused on machine learning-based anomaly detection techniques, which have proven effective for detecting network intrusions [12].

China's rapid cloud computing growth, supported by national policies, has increased cloud security concerns. Criminals use advanced cloud technologies for illicit activities, posing significant risks to cloud network operations, the economy, and national security [13].

Techniques for safeguarding network security include intrusion detection, data encryption, access control, and authentication [14]. This work employs deep learning techniques in intrusion detection research. Detecting anomalies in network traffic can identify and intercept attacks early, mitigating the damage caused by cyberattacks. Early detection and classification relied on manually created criteria, but machine learning models now use manually selected features for classification. However, feature selection is challenging in complex network environments. Deep learning techniques autonomously extract features for classification, addressing the shortcomings of earlier methods. Despite positive results, deep learning faces challenges like data imbalance. Prediction error rates increase when data departs significantly from the norm, as models tend to resemble more abundant data [15]. Different attacks require varying amounts of data for detection. For instance, DDoS and Port Scan attacks involve many packets, while infiltration attacks involve fewer packets. Techniques like under-sampling, over-sampling, and co-sampling address data imbalance but have their own merits and demerits. This work uses a novel data processing approach and feature fusion methodology to mitigate data imbalance's impact on test outcomes. Early fusion of multi-scale characteristics in traffic data enhances classification precision and reduces data imbalance's influence on experimental results.

The data processing approach separates network traffic into transport layer-based traffic, extracting flow information while preserving original traffic distribution. This approach hastens model convergence, strengthens resilience, and prevents the introduction of excessive zero components. Many existing deep learning algorithms only consider temporal or geographical variables, limiting detection accuracy. This research presents a temporal-spatial feature-based anomaly detection model (ITSN) that fully understands traffic information's inherent characteristics. ITSN uses deep learning, feature fusion technology, and traffic data characteristics to enhance detection accuracy [16].

Network intrusion detection is vital for information systems' long-term viability and regular functioning. Cyber-systems face serious threats from malicious actors and complex threat patterns. This research introduces new deep learning algorithms for threat and alert detection using network data from an open-source firewall like pfSense, which offers robust security features. The goal is to develop a reliable and efficient solution that regulates traffic patterns using advanced deep learning structures like LSTMs and CNNs. The effectiveness of this approach is evaluated through quantitative tests and comparisons with state-of-the-art formulations [17].

Contribution of Study

1. This study aims to develop models that are scalable and capable of real-time detection, improving upon current autoencoder-based approaches.
2. With the advanced methods such as multivariate Neural Prophet models, the study seeks to enhance detection accuracy and reduce false alarms.
3. The study will explore sophisticated autoencoder designs and innovative approaches like the modified Zebra Algorithm to optimize feature extraction and fusion.
4. The study will examine how autoencoders combined with multivariate time series forecasting methods like Neural Prophets can be used to predict future threats based on historical data.

METHODOLOGY

The methodology used in this study is essential to guaranteeing the accuracy and dependability of the findings. The procedures for selecting and pre-processing the datasets are described in this part, along with the metrics that are used to evaluate the intrusion detection system's effectiveness.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Dataset

The CICIDS2018 dataset obtained from the (kaggle.com), made by the CIC/Canadian Institute of Cybersecurity, captures contemporary network data, which both standard and malicious activities. It features labelled network traffic data with key attributes such as flow duration, protocol type, source and destination IPs, ports, packet size, and various flow-related statistical metrics. This dataset is instrumental for cybersecurity studying the topic and creating efficient threat detection and mitigation tactics.

Improved Zebra Optimization Algorithm Based Features Selection

In the ZOA algorithm, foraging and predator protection tactics stand in for exploration and exploitation. The best zebra is referred to as the pioneer zebra in the exploration method, and it is this individual who will guide other zebras to feed [Figure-1]. There are two categories for the exploitation process that are based on defense mechanisms against the actions of predators. When zebras are assaulted by lions in the initial phase, they choose to flee by turning randomly to the side and zigzagging. The goal of the IZOA is to enhance the process of exploration and exploitation for using RES to solve TEP difficulties. To extend the exploration method The Lévy flight distribution function is in the first phase. proposed. Furthermore, in the second phase, a revised exploitation approach is also suggested.

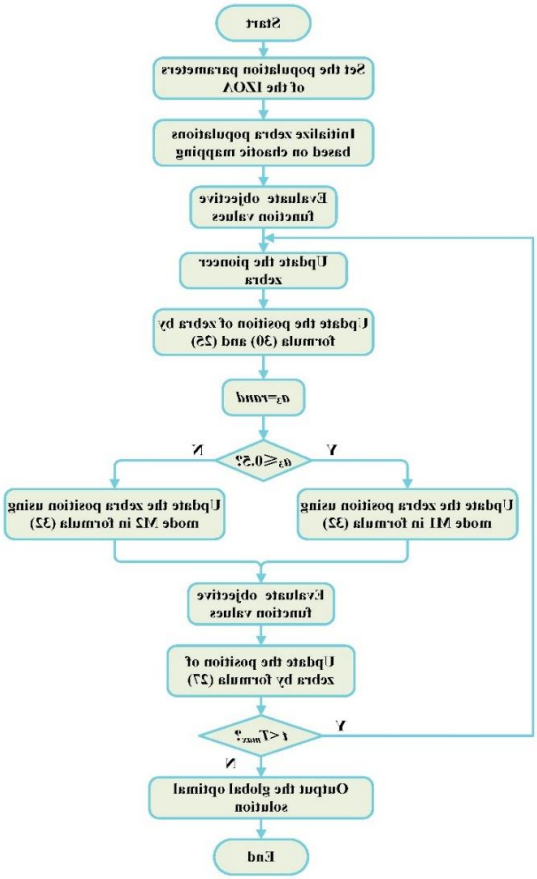

Figure 1. Flow Chart of Improved zebra optimization algorithm

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Time Series Forecasting Using Multivariate Neural Prophet Model

An ongoing model-based methodology is demonstrated using a sequence of dates that depicts the frequency of assaults on a particular connected computer system or network across a period of time. Certain models are designed to specifically support particular model families, such as ARIMA or neural networks, while others are capable of supporting more general forecasting frameworks. While there exist prediction frameworks that offer more extensive coverage, they lack interfaces to popular machine learning tools such as sci-kit-learn [18]. A deficiency exists in the availability of an open-source toolbox that connects existing machine learning tools, enabling the construction, alteration, and evaluation of models [19]. Using the Lévy flight distribution function, the exploration procedure can be explained as

$$x_{ij}^{P1} = PZ_j + Levy(\lambda).(PZ_j - x_{ij})$$

(eq:-1)

The following formula can be used to calculate the Lévy flight distribution function, where $\mathbf{I}ij(\lambda)$ is the Lévy flight distribution function, $Revy$ is the role of the pioneering zebra, and I=round(rand+1) is the random number [1, 2], while r is randomly produced in the interval [0,1], and xij is the role of the i th zebra.

$$levy = s.\frac{w.\sigma}{|k|^{\frac{1}{\lambda}}}$$

(eq:-2)

In Eq. (2), s where w and k are variables that are randomly chosen and has a fixed value of 0.01. integers between the numbers 0 and 1, and A random number denoted as λ created set to λ=1.5 in this, inside the interval [0, 2]. study. To calculate σ, apply Equation (3).

$$\sigma = \frac{r(1+\lambda).\sin(\frac{\pi\lambda}{2})}{r\left(\frac{1+\lambda}{2}\right).\lambda 2^{(\frac{\lambda-1}{2})}}$$

(eq:-3)

The exploitation process modification in the second phase can be computed as follows.

$$x_{ij}^{p2} = x_{ij} + I.r.\sin(2\pi * r).(PZ_j - \frac{AZ_j + x_{ij}}{2})$$

(eq:-4)

Where I=round(rand+1) is the random value, while r is a random integer between 0 and 1., PZj and AZj are the positions of the pioneer and attacked zebras, and xij is the status of the in the subsequent stage, the in the subsequent stage, the ith zebra.

There are six modules in total: trend (T), auto-regressor (AR), seasonality (S), event (E), future-regressor (FR), and delayed regressor (LR)., make up the segmented explainable model Neural Prophet (NP) [20]. Each module adds a component to the forecast curve. To create the model, each component can be integrated and modified separately. However, for every The amount of future time steps that need to be forecast, all six modules generate h outputs, which are added to the future values of yt, ⋯, yt+h−1 as yt^, ⋯., y^t+h−1. The representation of the entire model is given by Eq. (5).

$$Mode(y_t) = T(t) + S(t) + E(t) + FR(t) + AR(t) + LR(t)$$

(eq:-5)

By putting a growth rate k and an offset m together, the trend component can be represented as a continuous linear sequence with pieces that allows for changes at different points. The computation of at time t1, the impact is illustrated in Eq. (6).

$$T(t) = T(t_0) + k\Delta t = m + k(t, -, t_0)$$

(eq:-6)

As a result, the trend module's interpretable nonlinear model is produced. Only NC, the number of change points that is finite, in our model is five and matches each of the five lockdowns that were

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

implemented in India at the various times, will cause the growth rate of the linear trend to vary. C= (c1, c2…, cn) is one way to define the set C. The trend continued to grow at the same rate in between change points. A growth vector (δ) that is a function of the offset vector (ρ) can be used to illustrate how the growth rate is adjusted at each change point. The status at time t with respect to each change point is represented by another vector, Γ(t)∈RnC. Thus, the definition of at time t, the trend T(t) may be found in Eq.(7)

$$T(t) = (\delta_0, +, \Gamma, (t)^T, \delta).t + (\rho_0, +\Gamma, (t)^T, \rho)$$

(eq:-7)

where,

$$\delta = (\delta_1,,,\delta_2,,,\delta_3,,,\delta_{n_c}), \rho = (\rho_1,,,\rho_2,,,\rho_3,,,\rho_{n_c}),$$

(eq:-8)

$$\Gamma(t) = \left(\Gamma_1,(t),,,\Gamma_2(t),,,\Gamma_3(t)\ldots.,,,.\ldots,,,\Gamma_{n_c}(t)\right),$$

(eq:-9)

$$\Gamma_j(t) = \begin{cases} 0, & other \\ 1, & if\ x \geq c_j \end{cases}$$

(eq:-10)

The annual seasonal fluctuations' periodic impact for this situation is modeled using the Fourier series and is shown in Eq. (11).

$$s(t) = \sum_{n=1}^{N} \left(a_n, cos, \left(\frac{2\pi nt}{P}\right), +, b_n, sin, \left(\frac{2\pi nt}{P}\right)\right)$$

(eq:-11)

where P is set to 365.25 by default and N to 6.

Algorithm 1 Improved Zebra Optimization Algorithm (IZOA)

Initialize parameters
$N \leftarrow 50$ {Population size}
$T \leftarrow 100$ {Maximum iterations}
$\alpha \leftarrow 0.5$ {Step size factor for following leader}
$\beta \leftarrow 0.3$ {Step size factor for exploiting best solution}
$\gamma \leftarrow 0.2$ {Step size factor for randomness}
Define Objective Function
$f(x)$ = minimize $\{f1(x), f2(x), \ldots, fm(x)\}$
Initialize population
population ← initialize population(N)
Evaluate initial fitness
fitness_values ← evaluate population(*population*, *f*)
for t ← 1 to *T* do
    Sort population based on fitness
    sorted_population, *sorted_fitness* ← sort population(*population*, *fitness_values*)
    for i ← 0 to *N* − 1 **do**

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

```
    if i == 0 then
      Leader zebra update
      population[i] ← update_leader (population[i], sorted population[0], α, β, γ, f )
    else
      Follower zebra update
      population[i] ← update_follower (population[i], sorted_population[i], α, β, γ, f )
    end if
  end for
  Evaluate new fitness values
  fitness_values ← evaluate population (population, f )
  Optional: Adjust step size factors dynamically
  adjust_step_size(α, β, γ, fitness_values)
  Check for convergence (optional)
  if has_converged (fitness_values) then
    Break
  end if
end for
Return the best solution
best_solution ← get_best_solution (population)
```

The Improved Zebra Optimization Algorithm (IZOA) is a metaheuristic optimization approach based on zebra social dynamics and movement patterns. It represents zebras as candidate solutions that are iteratively refined to find the best solution. The algorithm employs a population of zebras, with leader zebras guiding followers based on fitness, and movement influenced by parameters alpha (α), beta (β), and gamma (γ). Alpha determines the step size for exploring new regions, beta influences the use of known solutions, and gamma introduces randomness to prevent local optima. Setting these parameters correctly is critical for striking the right balance between exploration, exploitation, and diversity. The population size (N) and maximum iterations (T) are determined by the complexity of the problem and the computational resources available. Alpha, beta, and gamma are typically set within a range (for example, 0.1 to 1.0) and dynamically adjusted in response to preliminary results and performance evaluations.

RESULT AND DISCUSSION

The study used the CICIDS2018 dataset, which was produced by the Cybersecurity Institute of Canada (CIC) and is available on Kaggle. It provides labelled network traffic data that is important for cybersecurity research. Significant features including protocol types, destination ports, flow durations, packet counts, sizes, and statistical metrics are included. The development of efficient threat detection and mitigation techniques in network security is made possible by this dataset.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

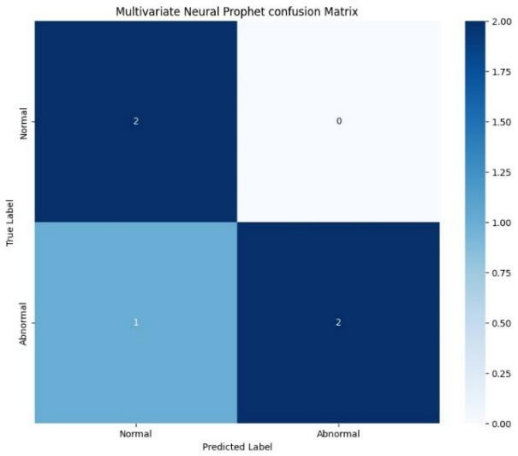

Figure 2. Confusion Matrix of Multivariate neural Prophet

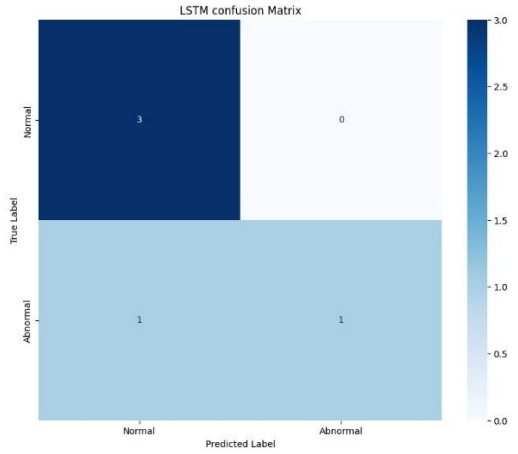

Figure 3. Confusion Matrix of LSTM

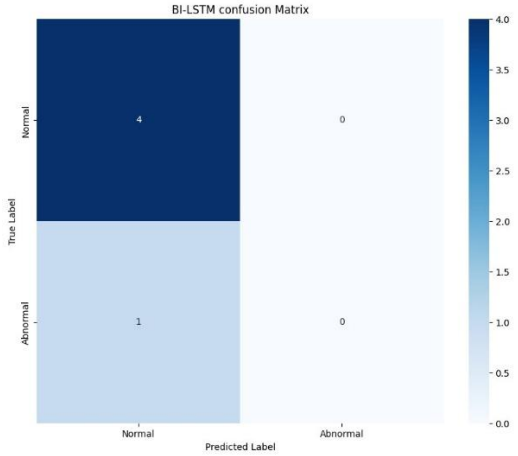

Figure 4. Confusion Matrix of BI-LSTM

The above given confusion matrix [Figure-2, Figure-3, Figure-4] for the classification task by using Multivariate Neural Prophet model, LSTM, and Bi-LSTM. The diagonal cells of the matrix represent the

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

number of samples that were successfully categorized. The off-diagonal cells represent the number of samples that were incorrectly categorized. The following outcomes are shown by the Multivariate Neural Prophet model provides well-balanced classification results. The model successfully recognized two abnormal instances as abnormal (true positives) and two normal cases as normal (true negatives), with one false negative resulting from an abnormal case being mistakenly predicted as normal, and no false positives. The Long Short-Term Memory (LSTM) model successfully categorized three normal instances as normal and one abnormal case as abnormal, demonstrating strong performance in normal prediction. However, it misclassified one abnormal case as normal (false negative) and produced no false positives. The LSTM model works well in normal instances, but its capacity to identify anomalies is restricted. The (BI-LSTM) model also performs well in predicting normal instances, with four true negatives and zero false positives. But it did not accurately detect any abnormal instances (0 true positives) and misclassified one abnormal case as normal (false negative). This demonstrates that the BI-LSTM excels in normal predictions but is less successful in spotting anomalies. In overall, the MPN model beats the LSTM and BI-LSTM models by correctly predicting both normal and abnormal instances with low misclassifications, resulting in the best overall accuracy.

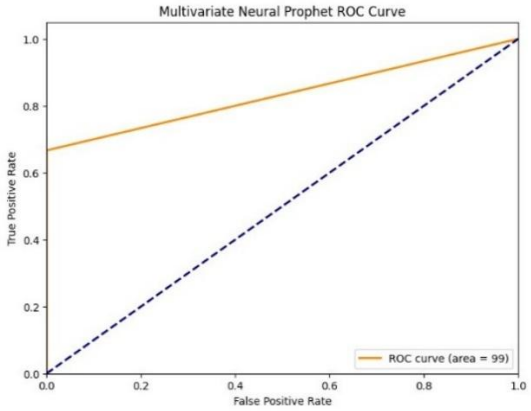

Figure 5. ROC Curve of Multivariate neural Prophet

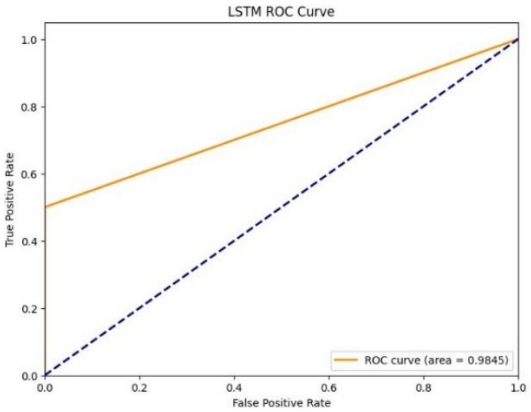

Figure 3. ROC Curve of LSTM

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

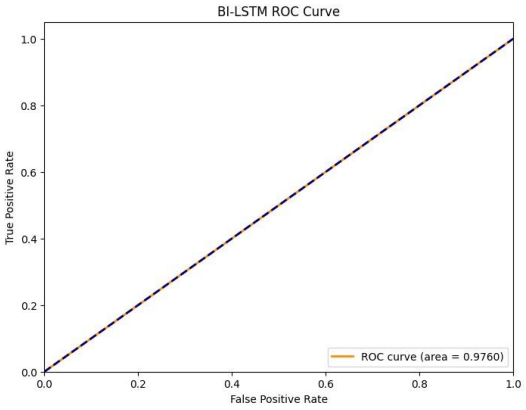

Figure 4. ROC Curve of BI-LSTM

A comprehensive overview [Figure-5, Figure-6, Figure-7] of the classification performance of the models that have been evaluated for the prediction of normal and abnormal instances is provided by the ROC curves. It is important to note that multivariate neural prophet model excels over the other models and has the maximum level of accuracy. A trajectory that approaches the top left corner with a high true positive rate for correctly categorized positive examples and remains close to the bottom right corner, indicating a low rate of inaccurately recognized negative instances, is depicted in the multivariate neural prophet ROC curve. The Area score of the multivariate neural prophet model is remarkable, surpassing that of other models such as LSTM, and Bi-LSTM. These are the precise area values for multivariate neural prophet model (Area = 0.99), LSTM (Area = 0.9845), Bi-LSTM (Area = 0.9760). These numerical comparisons demonstrate that multivariate neural prophet model performs better than other approaches.

Table 1. Performance Metrics

Models	Accuracy	Precision	Recall	F1-Score
Multivariate Neural Prophet	0.899	0.98	0.899	0.854
LSTM	0.831	0.85	0.831	0.78
Bi-LSTM	0.801	0.64	0.801	0.711

The Multivariate Neural Prophet model is better to the other models in terms of critical performance metrics [Table-1], which is why it is the example that is the most appropriate for the content that has been supplied. It achieves an accuracy of 0.899, which implies that it successfully predicts almost 89.9% of the occurrences, which suggests that it has a good overall performance. This shows that it has a high overall performance. In terms of its positive predictions, the model has a high degree of reliability, as it correctly identifies 98% of the occurrences that it predicts as being positive. The fact that it has an accuracy of 0.98 demonstrates that it is quite trustworthy. As shown by the recall rate of 0.899, the model is able to accurately identify 89.9% of the true positive instances. This recall rate ensures that the majority of cases that are relevant are discovered. The F1-Score for 0.854, which achieves a harmony between accuracy and remember, is more evidence that the model is effective. This score provides further evidence that the model is good. The LSTM model, on the other hand, displays a lower level of performance, with a precision of 0.831, an exact amount of 0.85, a reminder of 0.831, as well as an F1-Score of 0.780. This is in contrast to the Bi-LSTM model, which displays a lower level of performance, precisely when it comes to 0.801, an exact amount of 0.64, a reminder of 0.801, as well as an F1-Score of 2.71. Regarding this particular subject matter, the Multivariate Neural Prophet model is the alternative that is both the most dependable and the most effective that can be obtained.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

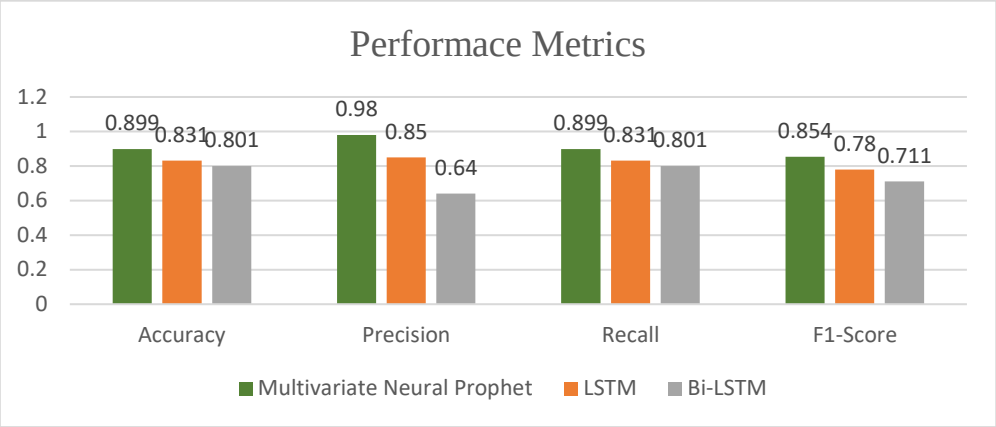

Figure 8. Comparison between Proposed and existing models

Figure 8 compares the performance of the proposed Multivariate Neural Prophet model to the current LSTM and Bi-LSTM models. The image clearly shows that the Multivariate Neural Prophet model surpasses the LSTM and Bi-LSTM models in every statistic, including accuracy, precision, recall, and F1-score. The MPN's exceptional performance is shown by its great accuracy and precision, as well as a good recall and balanced F1-score. While the LSTM model is useful, it falls short of MPN in terms of accuracy and F1 score. The Bi-LSTM model, although competitive in recall, has major shortcomings in precision and overall accuracy, resulting in the lowest F1-score. This comparison demonstrates the Multivariate Neural Prophet model outperforms the LSTM and Bi-LSTM models in classification tasks.

DISCUSSION

This research tested three advanced models Multivariate Neural Prophet, LSTM, and BI-LSTM on the CICIDS2018 dataset to identify network traffic anomalies. The Multivariate Neural Prophet model categorized network activity as normal or abnormal with one that best accuracy and reliability. This model balanced threat detection with false alarm reduction, which is essential for real cybersecurity applications, making it the best. However, although the LSTM model performed well, it missed several abnormalities, which might be problematic in real-world circumstances where even one undiscovered danger can have major effects. Despite its complex design, the BI-LSTM model performed poorly in this investigation. It had trouble detecting aberrant network traffic, suggesting that complexity may not necessarily improve anomaly detection. Multivariate Neural Prophet model's outstanding performance makes it suitable for network security applications, providing dependable threat detection. This research shows that the LSTM model has promise, while the BI-LSTM model is less successful, highlighting the necessity for cautious network security model selection. Future study might refine these models or explore other network threat detection methods.

CONCLUSION

While cloud computing has many benefits, security issues including threats and illegal access exist. Machine learning improves the efficacy of intrusion detection systems (IDS), which are essential for resolving these problems. The secret to real-time monitoring is anomaly detection. The necessity for contemporary datasets like CIC-IDS2018 is highlighted by the fact that current research often uses out-of-date datasets. Additional research into time series approaches, sophisticated models such as auto encoders, and strategies to reduce false positives is also necessary. Performance and resource efficiency may be improved by incorporating models such as the Facebook Prophet and optimizing models like the Zebra algorithm. Closing these vulnerabilities may greatly enhance cloud security and increase the efficacy and efficiency of IDS. A solid method for enhancing cloud security may be found by fusing an enhanced Zebra algorithm with a multivariate neural Prophet model.

REFERENCES

[1] A. K. Shukla and A. Sharma, "Cloud Base Intrusion Detection System using Convolutional and Supervised Machine Learning," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-5, doi: 10.1109/ISCON57294.2023.10112007.
[2] A. K. Shukla and A. Sharma, "Classification and Mitigation of DDOS attacks Based on Self-Organizing Map and Support Vector Machine," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-5, doi: 10.1109/ISCON57294.2023.10111988.
[3] A. K. Shukla and A. Sharma, "Distributed Attacks Classification Based on Radical Basis Function and Particle Swarm Optimization In Hypervisor Layer," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-4, doi: 10.1109/ISCON57294.2023.10112162.
[4] G. Mahalakshmi, S. Sridevi, and S. Rajaram, "A survey on forecasting of time series data," in 2016 International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE'16), 2016, pp. 1–8. doi: 10.1109/ICCTIDE.2016.7725358.
[5] A. K. Shukla and A. Sharma, "Reduce false intrusion alerts by using PSO feature selection in NSL-KDD dataset," 8th International Conference on Computing in Engineering and Technology (ICCET 2023), Hybrid Conference, Patna, India, 2023, pp. 226-231, doi: 10.1049/icp.2023.1495.
[6] A. K. Shukla and A. Sharma, "Cloud Data Security by Hybrid Machine Learning and Cryptosystem Approach", Int J Intell Syst Appl Eng, vol. 12, no. 2s, pp. 01–14, Oct. 2023.
[7] J. L. Leevy and T. M. Khoshgoftaar, "A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data," J. Big Data, vol. 7, no. 1, p. 104, 2020, doi: 10.1186/s40537-020-00382-x.
[8] D. Al-Fraihat, M. Alzaidi, and M. Joy, "Why do consumers adopt smart voice assistants for shopping purposes? A perspective from complexity theory," Intell. Syst. with Appl., vol. 18, p. 200230, 2023, doi: https://doi.org/10.1016/j.iswa.2023.200230.
[9] Y. O. Sharrab, M. Alsmirat, B. Hawashin, and N. Sarhan, "Machine learning-based energy consumption modeling and comparing of H.264 and Google VP8 encoders," Int. J. Electr. Comput. Eng., vol. 11, no. 2, pp. 1303–1310, 2021, doi: 10.11591/ijece.v11i2.pp1303-1310.
[10] A. Alsarhan, A.-R. Al-Ghuwairi, I. T. Almalkawi, M. Alauthman, and A. Al-Dubai, "Machine Learning-Driven Optimization for Intrusion Detection in Smart Vehicular Networks," Wirel. Pers. Commun., vol. 117, no. 4, pp. 3129–3152, 2021, doi: 10.1007/s11277-020-07797-y.
[11] Y. Peng, "Research of Network Intrusion Detection system based on snort and NTOP," 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, Chongqing, China, 2012, pp. 2764-2768, doi: 10.1109/FSKD.2012.6233822.
[12] B. Cui, Z. Liu, and L. Wang, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage," vol. 6, no. 1, pp. 1–13, 2015, doi: 10.1109/TC.2015.2389959.
[13] M. Cui, D. Han and J. Wang, "An Efficient and Safe Road Condition Monitoring Authentication Scheme Based on Fog Computing," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9076-9084, Oct. 2019, doi: 10.1109/JIOT.2019.2927497.
[14] Su, Jian, et al. "Redundant rule Detection for Software-Defined Networking". (2020, June 30). KSII Transactions on Internet and Information Systems. Korean Society for Internet Information (KSII). https://doi.org/10.3837/tiis.2020.06.022.
[15] C. Orlikowski, R. Hein, and E. Wittbrodt, "Port-based approach to distributed transfer function method," vol. 672, pp. 671–672, 2009, doi: 10.1002/pamm.200910305.
[16] Y. Dai, F. Gieseke, S. Oehmcke, Y. Wu and K. Barnard, "Attentional Feature Fusion," 2021 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 2021, pp. 3559-3568, doi: 10.1109/WACV48630.2021.00360.
[17] K. He, X. Zhang, S. Ren, and J. Sun, "Spatial Pyramid Pooling in Deep Convolutional Networks for Visual Recognition," vol. 8828, no. c, pp. 1–14, 2015, doi: 10.1109/TPAMI.2015.2389824.
[18] K. Fotiadou, T. Velivassaki, A. Voulkidis, D. Skias, S. Tsekeridou, and T. Zahariadis, "Network Traffic Anomaly Detection via Deep Learning," pp. 1–17, 2021. doi: 10.3390/info12050215
[19] Y. P. Faniband and S. M. Shaahid, "Univariate Time Series Prediction of Wind speed with a case study of Yanbu, Saudi Arabia," Int. J. Adv. Trends Comput. Sci. Eng., vol. 10, no. 1, pp. 257–264, 2021, doi: 10.30534/ijatcse/2021/361012021.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[20] D. K. Barupal and O. Fiehn, "Generating the blood exposome database using a comprehensive text mining and database fusion approach," Environ. Health Perspect., vol. 127, no. 9, pp. 2825–2830, 2019, doi: 10.1289/EHP4713.
[21] A. Dixit and S. Jain, "Effect of stationarity on traditional machine learning models: Time series analysis," in Proceedings of the 2021 Thirteenth International Conference on Contemporary Computing, in IC3-2021. New York, NY, USA: Association for Computing Machinery, 2021, pp. 303–308. doi: 10.1145/3474124.3474167.