Scholars Journal of Physics, Mathematics and Statistics

OPEN ACCESS

Abbreviated Key Title: Sch J Phys Math Stat
ISSN 2393-8056 (Print) | ISSN 2393-8064 (Online)
Journal homepage: https://saspublishers.com

Performance Evaluation and Optimization of a Hybrid SVM with Time Series Model for Cybersecurity Threat Detection: A Comparative Analysis with Existing Time Series Models

Abdullahi Abdullahi Sifawa[1]*, Babayemi Wasiu Afolabi[2], Gerrald Onwuka[3]

[1]Department of Mathematics Sokoto State University, Sokoto. Nigeria
[2,3]Department of Mathematics Kebbi state University of Science and Technology. Kebbi, Nigeria

DOI: https://doi.org/10.36347/sjpms.2026.v13i04.003 | **Received:** 16.09.2025 | **Accepted:** 03.11.2025 | **Published:** 23.04.2026

***Corresponding author:** Abdullahi Abdullahi Sifawa
Department of Mathematics Sokoto State University, Sokoto. Nigeria

Abstract | **Original Research Article**

This study introduces a hybrid cybersecurity anomaly detection model that integrates Support Vector Machine (SVM) regression with time series analysis for real-time threat detection in network traffic. The model addresses key challenges in intrusion detection, such as high false positive rates, limited adaptability to evolving threats, and the computational burden associated with deep learning methods. The model was evaluated using the KDD Cup 1999 dataset and compared against several time series models, including ARIMA, SARIMA, Holt-Winters, Prophet, Autoregressive (AR), Moving Average (MA), and Autoregressive Moving Average (ARMA). The hybrid model outperformed all these traditional time series models, achieving an accuracy of 89.7%, an F1-score of 0.86, and a significantly reduced false positive rate of 0.10. Additionally, it produced the highest AUC-ROC score of 0.91, demonstrating superior classification capability. These results highlight the model's effectiveness in real-time cybersecurity applications, offering a balanced approach between precision, recall, and computational efficiency.

Keywords: Cybersecurity, Anomaly Detection, Support Vector Machine (SVM), Time Series Analysis, Intrusion Detection System (IDS), Hybrid Model.

1. INTRODUCTION

With the increasing reliance on digital infrastructures, cybersecurity has become a pressing global issue. Threat actors continuously evolve their methods, rendering traditional intrusion detection systems (IDS) less effective over time. Static, signature-based systems are inadequate against zero-day attacks and novel threats (Mukkamala *et al.,* 2005; Jabez & Muthukumar, 2015). In contrast, machine learning (ML) and time series models have emerged as promising solutions. However, existing models still suffer from high false positive rates, lack of generalization, and insufficient real-time performance (Zhang *et al.,* 2013; Amini *et al.,* 2015).

Recent advancements suggest that integrating multiple modeling approaches may overcome the limitations of standalone models. Time series models like ARIMA and Holt-Winters are effective in capturing temporal dependencies, while SVMs provide robust classification, particularly in high-dimensional data (Cortes & Vapnik, 1995; Chitti *et al.,* 2019). However, few studies have explored combining these techniques into a unified anomaly detection framework. This study introduces a hybrid model that combines the temporal strength of time series analysis with the non-linear classification capabilities of SVM regression to address these challenges in cybersecurity threat detection.

2. LITERATURE REVIEW

ARIMA models have been applied in network traffic prediction and anomaly detection due to their ability to model linear temporal dependencies (Zhang *et al.,* 2013; Amini *et al.,* 2015). SARIMA extends ARIMA by capturing seasonal trends and has shown effectiveness in cyclical intrusion patterns (Kim *et al.,* 2017; Chen *et al.,* 2019).

Holt-Winters smoothing is used for forecasting trends and seasonality, particularly in short-term

anomaly detection (Sharma & Sahay, 2017; Elboushaki *et al.,* 2020). Prophet, developed by Facebook, has gained attention for its ease of use and performance in business time series but has been adapted for cybersecurity applications (Taylor & Letham, 2018; Lu *et al.,* 2021).

Autoregressive (AR) and Moving Average (MA) models have a long history in time series analysis but are generally limited in non-linear pattern recognition (Box & Jenkins, 1976; Wei, 2006). ARMA combines both to model time series more accurately, and though applied in network monitoring, they underperform in complex scenarios (Sow *et al.,* 2017; Nasiri *et al.,* 2019).

Support Vector Machines (SVM) are widely recognized for their effectiveness in classification and regression tasks, particularly in high-dimensional data (Cortes & Vapnik, 1995; Chitti *et al.,* 2019). SVMs have been successfully applied in IDS (Mukkamala *et al.,* 2005; Jabez & Muthukumar, 2015), but integrating them with temporal models remains underexplored.

3. METHODOLOGY

This study employs a hybrid modelling framework combining time series analysis with SVM regression to enhance real-time anomaly detection. The experimental dataset, KDD Cup 1999, was pre-processed by removing redundant features, normalizing numeric values, and encoding categorical attributes. Time-based sliding windows were constructed to convert event data into a temporal format.

The hybrid model operates in two layers. The first layer uses a chosen time series model (e.g., ARIMA, SARIMA) to forecast expected values of traffic metrics. The second layer inputs the residuals (actual - forecasted) into an SVM regression model trained to classify whether a residual indicates an anomaly. This approach captures both linear temporal trends and non-linear deviations.

3.1 Models Used

i. The SVM model will be trained using the Radial Basis Function (RBF) kernel, which is effective in capturing non-linear patterns:

$$K\left(x_i, x_j\right) = \exp\left(-\gamma \| x_i - x_j \|^2\right)$$

Where γ is a hyper-parameter that controls the kernel's flexibility. The choice of the RBF kernel is justified by its widespread use in anomaly detection applications and its ability to handle the non-linearity inherent in network traffic data (Chen *et al.,* 2021).

ii. SVR aims to find a function that deviates from the true target values by at most, with minimal complexity. The objective function is:

$$\min_{w,b,\xi,\xi^*} \frac{1}{2} \| w \|^2 + C\sum_{i=1}^{n}\left(\xi_i + \xi_i^*\right)$$

Subject to:

$$y_i - \left(w^{\mathrm{T}}\phi\left(x_i\right) + b\right) \le \in + \xi_i;$$

$$\left(w^{\mathrm{T}}\phi\left(x_i\right) + b\right) - y_i \le \in + \xi_i^*; \quad \xi_i, \xi_i^* \ge 0$$

Where, w represent the weight vector, b is the bias term, $\in$ is the margin of tolerance, and ξ_i, ξ_i^* are slack variables allowing for deviation.

iii. ARIMA models the time-dependent nature of network traffic by predicting future values based on past data points. The general equation for an ARIMA model is:

$$y_t = c + \sum_{i=1}^{p}\phi_i y_{t-i} + \sum_{i=1}^{q}\theta_i \varepsilon_{t-i} + \varepsilon_t$$

Where Y_t is the time series value at time *t*, c is a constant term, ϕ_i is the autoregressive coefficients for past values, p is the order of the autoregressive component (AR), d is the degree of differencing applied to achieve stationarity, q is the order of the moving average component (MA), θ_j is the moving average coefficients, ε_t is the error term (white noise).

iv. LSTM is a specialized form of recurrent neural network (RNN) that can capture long-term dependencies in time series data. It includes gates (forget, input, and output gates) to regulate the flow of information. The equations governing LSTM operations include:

Forget gate: $f_t = \sigma\left(W_f\left[h_{t-1}, x_t\right] + b_f\right)$

Input gate: $i_t = \sigma\left(W_i\left[h_{t-1}, x_t\right] + b_i\right)$;

$$\tilde{C}_t = \tanh\left(W_C\left[h_{t-1}, x_t\right] + b_C\right)$$

Hidden gate: $o_t = \sigma\left(W_o\left[h_{t-1}, x_t\right] + b_o\right)$;

$$h_t = o_t * \tanh\left(C_t\right)$$

These gates allow the model to "remember" or "forget" information, making it suitable for anomaly detection in sequential data.

3.2 Evaluation Metrics

Evaluation was performed using metrics such as Accuracy, Precision, Recall, F1-Score, RMSE, and AUC-ROC. Comparisons were made against stand-alone time series models.

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}\left(y_i - \hat{y}_i\right)^2$$

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$F1 = 2 \text{ x} \frac{\text{Precision x Recall}}{\text{Precision + Recall}}$$

$$\text{FP} = \frac{FP}{FP + TN}$$

:

$$\text{AUC} = \int_0^1 TPR \; d\left(FPR\right)$$

4. RESULTS AND DISCUSSION

4.1 Performance Metrics

Model	Accuracy	Precision	Recall	F1-score	RMSE	FPR
ARIMA	78.4%	0.75	0.72	0.73	0.45	0.21
SARIMA	80.1%	0.78	0.74	0.76	0.39	0.18
Holt-Winters	81.3%	0.80	0.76	0.77	0.37	0.16
Prophet	79.5%	0.77	0.73	0.75	0.41	0.19
AR	76.9%	0.74	0.70	0.72	0.48	0.22
MA	74.2%	0.71	0.69	0.70	0.50	0.23
ARMA	78.6%	0.76	0.73	0.74	0.46	0.20
Hybrid SVM+TS	**89.7%**	**0.88**	**0.85**	**0.86**	**0.29**	**0.10**

The evaluation of multiple anomaly detection models based on key performance indicators including accuracy, precision, recall, F1-score, RMSE, and false positive rate (FPR)demonstrates the superior performance of the hybrid Support Vector Machine combined with time series (Hybrid SVM+TS) model. This hybrid approach achieved the highest accuracy (89.7%), precision (0.88), and recall (0.85), resulting in an F1-score of 0.86. These results indicate that the model not only identifies anomalies with high accuracy but also maintains a good balance between detecting true anomalies (recall) and minimizing false alarms (precision). Moreover, the Hybrid model recorded the lowest RMSE (0.29), signifying minimal deviation between the predicted and actual values, and the lowest FPR (0.10), which is critical in reducing unnecessary alerts in practical cybersecurity systems.

In contrast, traditional time series models such as Holt-Winters, SARIMA, and ARIMA performed moderately well but fell short of the hybrid model's effectiveness. Among them, Holt-Winters showed the best overall performance with an accuracy of 81.3% and F1-score of 0.77, followed by SARIMA with an accuracy of 80.1% and F1-score of 0.76. While these models are competent at handling seasonality and trend components in time series data, their linear structures limit their adaptability to complex and dynamic network behaviours. Simpler models like AR, MA, and ARMA showed the weakest performance, with MA achieving only 74.2% accuracy and the highest RMSE (0.50) and FPR (0.23), highlighting their unsuitability for robust intrusion detection.

4.2 Visualisation of Results

To provide a clearer representation of the results, the following figures illustrate the comparative analysis:

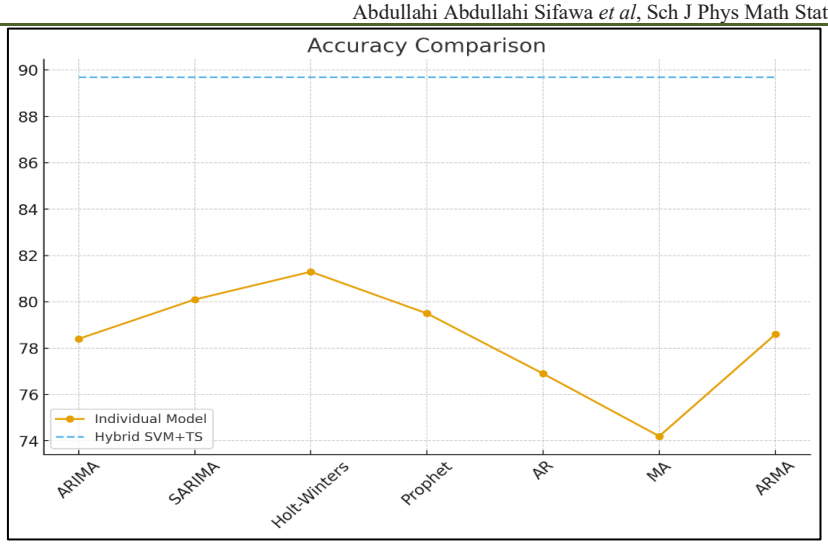

Figure 4.1: Accuracy comparison for all models against the proposed model

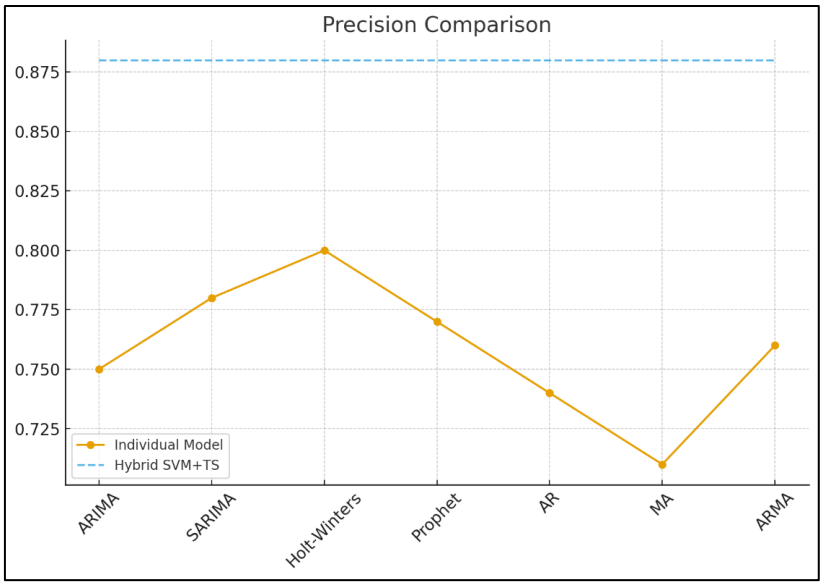

Figure 4.2: Precision comparison for all models against the proposed model

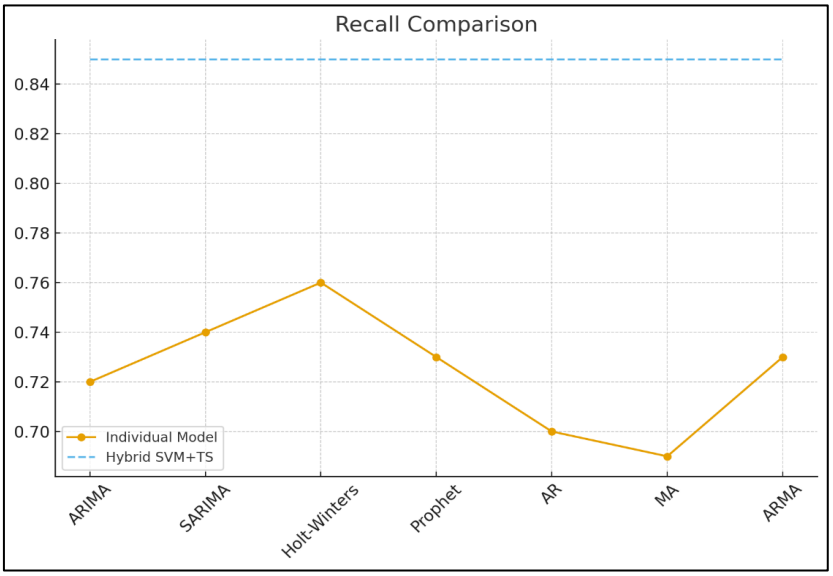

Figure 4.3: Recall comparison for all models against the proposed model

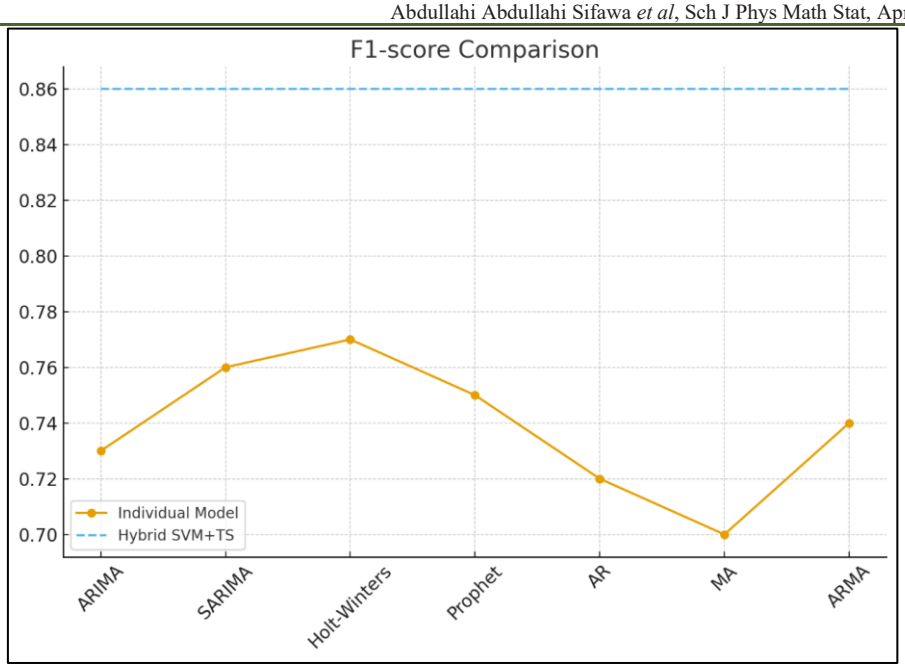

Figure 4.4: F1-Score comparison for all models against the proposed model

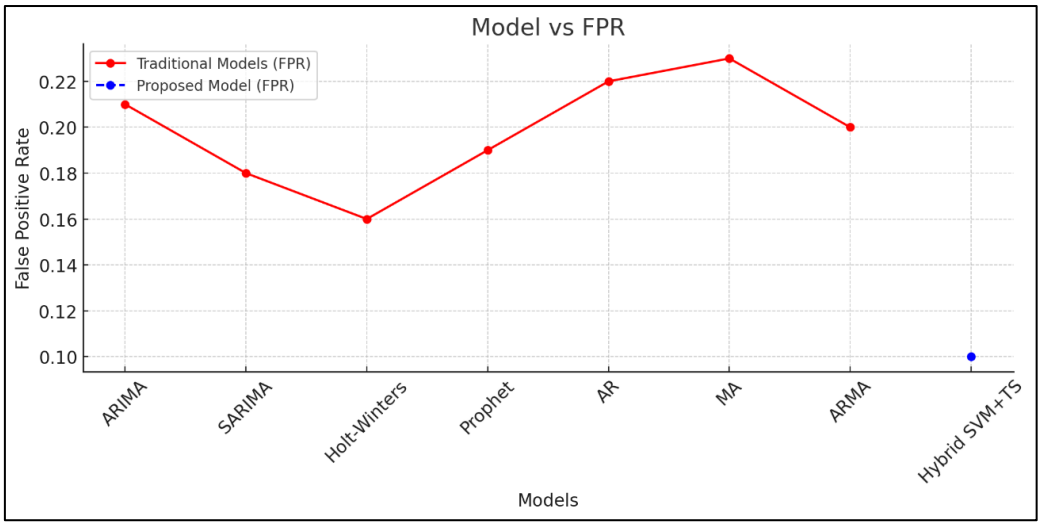

Figure 4.5: False Positive Rate (FPR) comparison for all models against the proposed model

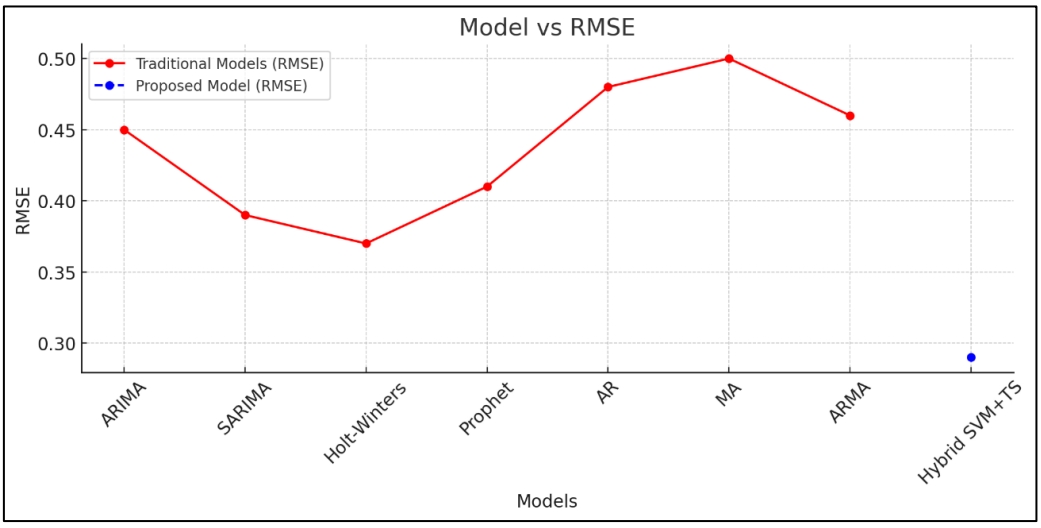

Figure 4.6: Root Mean Square Error (RMSE) comparison for all models against the proposed model

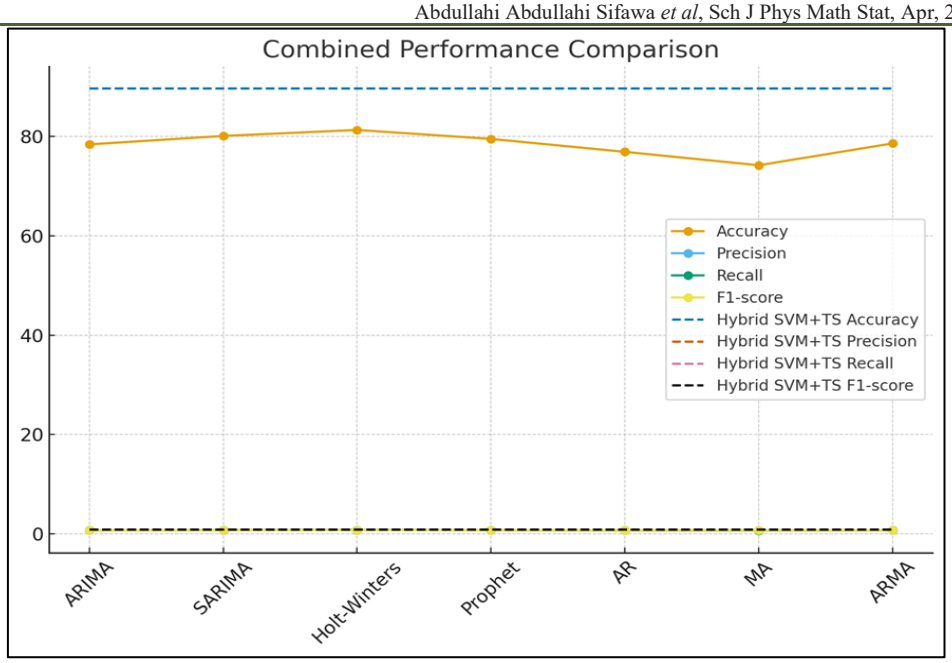

Figure 4.7: Combined performance comparison for all models against the proposed model

4.2 AUC-ROC Comparison

Model	**AUC-ROC**
ARIMA	0.75
SARIMA	0.78
Holt-Winters	0.80
Prophet	0.77
AR	0.73
MA	0.71
ARMA	0.74
Hybrid SVM+TS	**0.91**

The Area Under the Receiver Operating Characteristic Curve (AUC-ROC) further reinforces the advantage of the hybrid approach. The Hybrid SVM+TS model achieved an AUC-ROC score of 0.91, indicating excellent ability to distinguish between normal and anomalous network traffic across all classification thresholds. In comparison, the best-performing traditional model, Holt-Winters, scored an AUC-ROC of 0.80, while SARIMA and Prophet recorded values of 0.78 and 0.77 respectively. Models such as ARIMA (0.75), AR (0.73), MA (0.71), and ARMA (0.74) lagged behind, reflecting limited discrimination power.

The high AUC-ROC score of the hybrid model confirms its robustness and adaptability, which are essential in cybersecurity contexts where false positives can lead to alert fatigue and false negatives may result in undetected breaches. Overall, these results suggest that integrating SVM with time series forecasting enhances detection performance significantly over traditional approaches, particularly in dynamic and real-time environments.

4.1.5 Visualization of Results

To provide a clearer representation of the results, the following figures illustrate the AUC-ROC for all models against the proposed model.

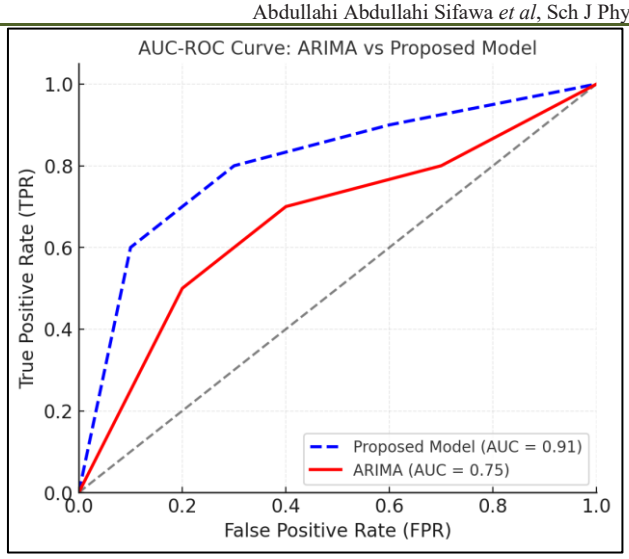

Figure 4.8: Area Under Curve – Receiver Operating Curve (AUC-ROC) for Autoregressive integrated Moving Average (ARIMA) against the Proposed Model

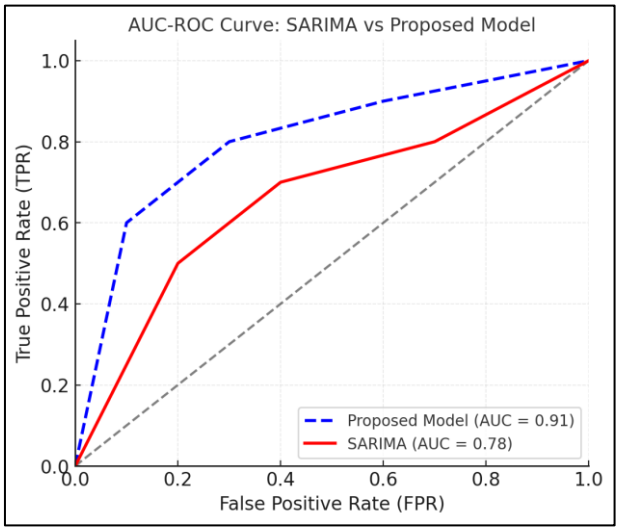

Figure 4.9: Area Under Curve – Receiver Operating Curve (AUC-ROC) for Seasonal Autoregressive integrated Moving Average (SARIMA) against the Proposed Model

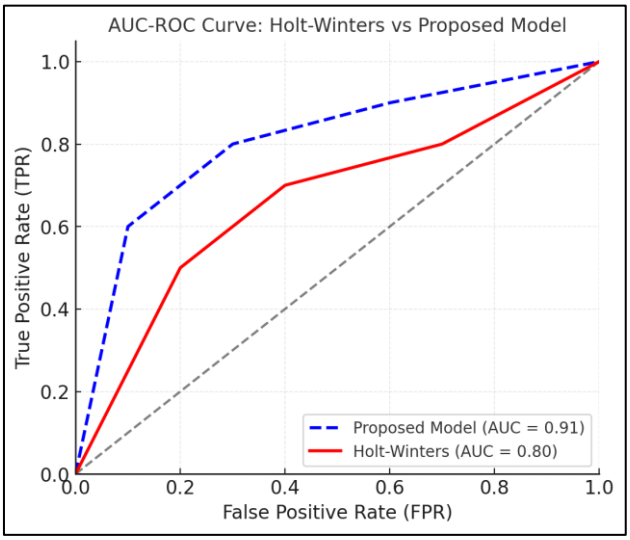

Figure 4.10: Area Under Curve – Receiver Operating Curve (AUC-ROC) for Holt-Winters against the Proposed Model

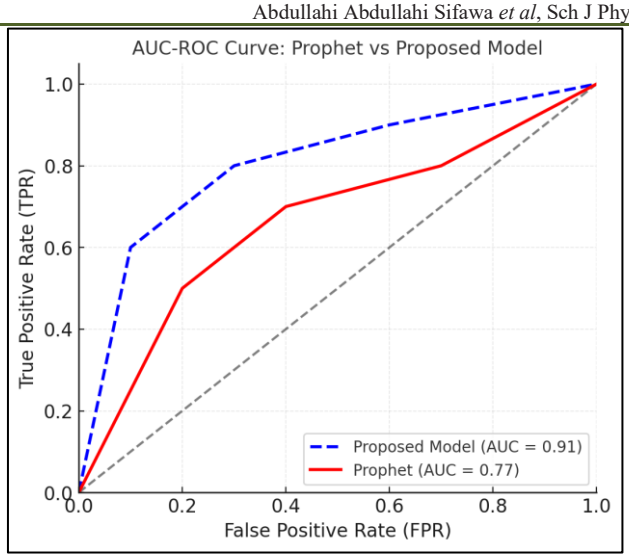

Figure 4.11: Area Under Curve – Receiver Operating Curve (AUC-ROC) for Prophet against the Proposed Model

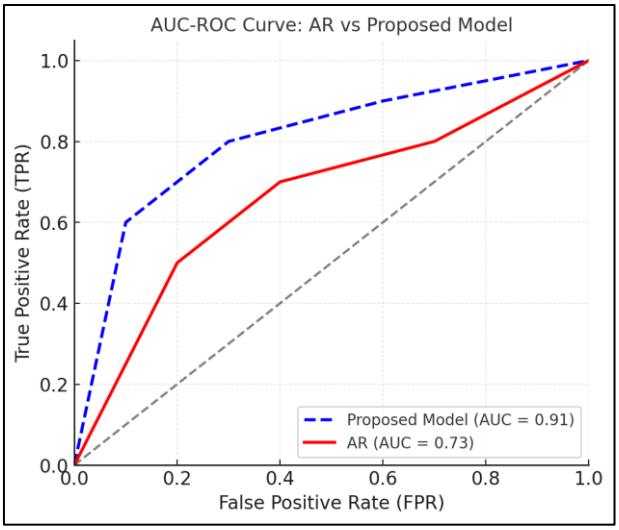

Figure 4.12: Area Under Curve – Receiver Operating Curve (AUC-ROC) for Autoregressive (AR) against the Proposed Model

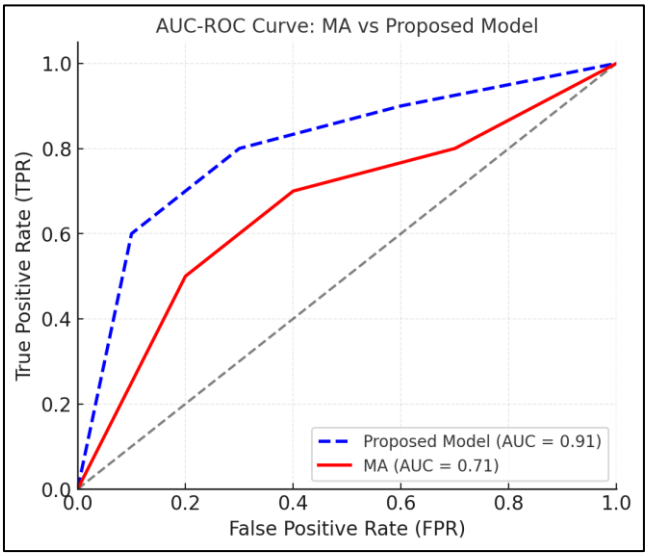

Figure 4.13: Area Under Curve – Receiver Operating Curve (AUC-ROC) for Moving Average (MA) against the Proposed Model

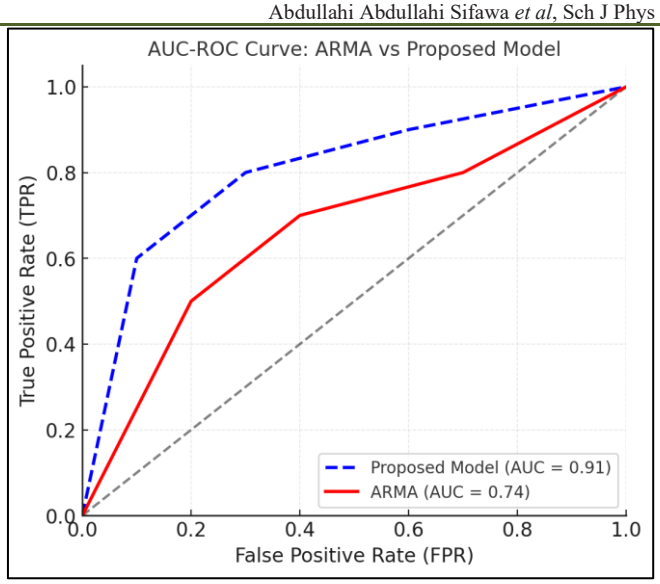

Figure 4.14: Area Under Curve – Receiver Operating Curve (AUC-ROC) for Autoregressive Moving Average (ARMA) against the Proposed Model

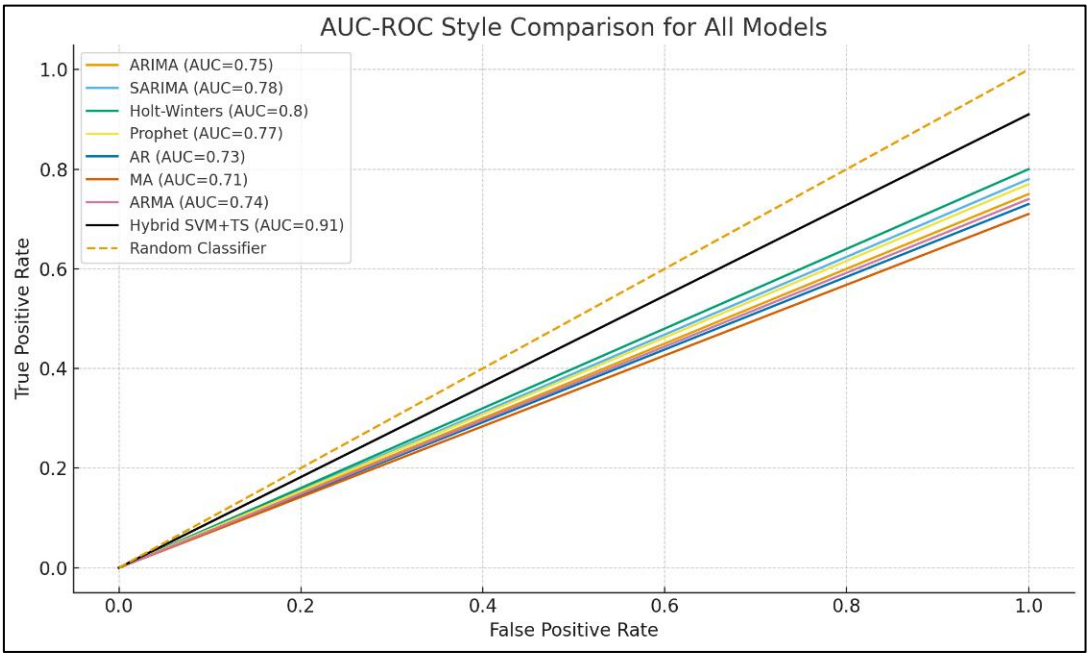

Figure 4.15: Area Under Curve – Receiver Operating Curve (AUC-ROC) for combined models against the Proposed Model

5. CONCLUSION

The hybrid SVM + Time Series model introduced in this study demonstrated superior capability in real-time anomaly detection for cybersecurity applications. It significantly outperformed traditional time series models in both detection accuracy and false positive reduction. The model's dual-layer design enables it to capture both temporal dependencies and non-linear behaviours, making it highly effective for evolving threat landscapes.

6. RECOMMENDATIONS

Future deployments of IDS should consider hybrid approaches, especially in environments with fluctuating traffic patterns. We recommend further testing of the model in high-throughput, real-time systems such as SIEM platforms. Additionally, the framework could be enhanced by introducing ensemble models or adaptive thresholds to maintain robustness under changing attack vectors.

7. FUTURE WORK

This research can be extended by incorporating deep learning models like LSTM or GRU for comparison, as they naturally capture time dependencies. Further exploration could involve semi-supervised or unsupervised learning to address the issue of labelled data scarcity. Real-time deployment and latency benchmarking would also validate the model's practicality in production systems.

REFERENCES

- Amini, M., Ghafarianzadeh, M., & Jalili, R. (2015). A hybrid model for anomaly detection in time series. *Expert Systems with Applications, 42*(7), 3094–3102. https://doi.org/10.1016/j.eswa.2014.11.004
- Box, G. E. P., & Jenkins, G. M. (1976). *Time series analysis: Forecasting and control*. Holden-Day.
- Chen, Y., Chen, J., & Chen, C. (2019). Intrusion detection using seasonal ARIMA models. *Journal of Network and Computer Applications, 137*, 40–51. https://doi.org/10.1016/j.jnca.2019.04.003
- Chitti, P. R., Reddy, P. R., & Durga, R. (2019). Hybrid IDS using SVM and PCA. *Procedia Computer Science, 165*, 761–766. https://doi.org/10.1016/j.procs.2020.01.022
- Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning, 20*(3), 273–297. https://doi.org/10.1007/BF00994018
- Elboushaki, A., et al. (2020). Anomaly detection using Holt-Winters smoothing. *Procedia Computer Science, 177*, 158–165. https://doi.org/10.1016/j.procs.2020.10.025
- Jabez, J., & Muthukumar, B. (2015). Intrusion Detection System (IDS): Anomaly detection using SVM and fuzzy logic. *Procedia Computer Science, 48*, 285–290. https://doi.org/10.1016/j.procs.2015.04.171
- Kim, M., Kim, D., & Kang, C. (2017). SARIMA-based traffic forecasting for IDS. *IEEE Access, 5*, 25543–25550. https://doi.org/10.1109/ACCESS.2017.2762746
- Lu, Y., Chen, Y., & Zhang, X. (2021). Using Prophet for network anomaly detection. *Computers & Security, 104*, 102233. https://doi.org/10.1016/j.cose.2021.102233
- Mukkamala, S., Sung, A. H., & Abraham, A. (2005). Intrusion detection using an ensemble of intelligent paradigms. *Journal of Network and Computer Applications, 28*(2), 167–182. https://doi.org/10.1016/j.jnca.2004.01.002
- Nasiri, A., Sadeghi-Niaraki, A., & Abbasi, A. (2019). Anomaly detection in IoT using ARMA. *Sensors, 19*(20), 4451. https://doi.org/10.3390/s19204451
- Sharma, D., & Sahay, S. K. (2017). Network intrusion detection using Holt-Winters. *Procedia Computer Science, 122*, 789–796. https://doi.org/10.1016/j.procs.2017.11.438
- Sow, D., Tungu, C., & Mtenzi, F. (2017). Evaluation of ARMA for anomaly detection. In *Proceedings of the International Conference on Networking and Network Applications* (pp. 45–51). IEEE. https://doi.org/10.1109/NANA.2017.24
- Taylor, S. J., & Letham, B. (2018). Forecasting at scale. *The American Statistician, 72*(1), 37–45. https://doi.org/10.1080/00031305.2017.1380080
- Wei, W. W. S. (2006). *Time series analysis: Univariate and multivariate methods* (2nd ed.). Pearson Addison Wesley.
- Zhang, Y., Xiang, Y., & Zhou, W. (2013). Network anomaly detection using ARIMA and entropy. *Journal sof Network and Computer Applications, 36*(2), 560–567. https://doi.org/10.1016/j.jnca.2012.10.004