Cyber Attack Pattern Analysis Based on Geo-location and Time: A Case Study of Firewall and IDS/IPS Logs

Daniel Mashao[1,*], Charis Harley[2]

[1]Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa

[2]Data Science Across Disciplines Research Group, Institute for the Future of Knowledge,Faculty of Engineering and the Built Environment, University of Johannesburg, Auckland Park, South Africa

ABSTRACT

Cyber attacks are a growing concern for organizations worldwide, requiring continuous monitoring and analysis to detect patterns and anticipate future threats. This study explores the temporal and geographical patterns of cyber attacks using log data from firewall and IDS/IPS systems, with a focus on understanding attack trends based on severity levels and monthly variations. The analysis revealed an almost even distribution of attacks, with 13,183 low severity, 13,435 medium severity, and 13,382 high severity incidents. This emphasizes the need for holistic defense strategies that address all levels of threats. Through time-series analysis, including the ARIMA model, we forecasted future attack trends, highlighting the consistency of cyber threats over time and identifying potential periods of increased activity. The monthly trend analysis showed fluctuations, with a notable peak of 906 attacks in March 2020 and a decrease to 825 attacks in April 2020, suggesting the influence of external factors such as global events. The ARIMA model provided accurate forecasts, indicating a steady rate of future attacks and underscoring the importance of continuous vigilance. While the ARIMA model captured linear trends effectively, future work should explore non-linear models, such as Long Short-Term Memory (LSTM) networks, to uncover deeper, more complex patterns in the data. This research provides critical insights into the nature of cyber attacks, offering organizations a data-driven approach to improving their cybersecurity measures. Future studies should focus on enhancing forecasting models and integrating real-time data to better anticipate emerging threats.

Keywords Cyber attack patterns, time-series forecasting, ARIMA model in cybersecurity, geo-location analysis, IDS/IPS log analysis

Submitted 27 December 2024
Accepted 22 January 2025
Published 8 March 2025

Corresponding author
Daniel Mashao,
dmashao@uj.ac.za

Additional Information and Declarations can be found on page 38

DOI: 10.47738/jcrb.v2i1.26

INTRODUCTION

In today's increasingly digital landscape, the frequency and complexity of cyber attacks are growing at an alarming rate, posing significant threats to organizations across all industries [1]. Cybercriminals exploit vulnerabilities in network infrastructures, targeting businesses, government entities, and individuals alike [2]. As technology evolves, so do the methods and tools used by attackers, rendering traditional defensive strategies insufficient to mitigate these ever-evolving threats. Therefore, understanding the patterns of cyber attacks and being able to forecast potential future incidents are critical components in developing more effective cybersecurity strategies [3]. Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) are commonly employed as the first line of defense by organizations, generating vast amounts of log data that capture key details of network activity [4]. Analyzing these logs provides valuable insights into attack patterns, including the type of threats, their frequency, the geographical origin of the attacks, and the times at which they

occur. However, simply collecting log data is not enough—there is a need for advanced analytical methods to extract meaningful patterns that can inform proactive cybersecurity measures.

While numerous studies have examined individual aspects of cyber attacks—such as malware types, attack vectors, or specific case studies on prominent breaches—there remains a significant gap in the literature when it comes to integrating temporal trends (time-series data) with geographical insights for a more comprehensive understanding of attack behavior. Furthermore, although traditional machine learning models like ARIMA have been applied in time-series forecasting of cyber attacks, these models primarily capture linear patterns and may not fully account for the non-linear complexities present in real-world attack data [5]. Few studies have explored more advanced models, such as Long Short-Term Memory (LSTM) networks, which are capable of capturing these non-linear dependencies in attack trends. This research gap highlights the need for a more nuanced exploration of how cyber attacks evolve over time and across different regions, particularly by applying advanced forecasting models that can handle the intricacies of temporal and spatial data [6].

Time-series forecasting techniques have been widely used in various fields to predict future events based on historical data, and in cybersecurity, ARIMA has been one of the more commonly applied models [7]. ARIMA excels at modeling linear dependencies and seasonal patterns, making it a reliable tool for short-term forecasting of cyber attack trends. However, ARIMA's limitation lies in its inability to capture non-linear relationships and longer-term dependencies that may exist in cyber attack data, especially in scenarios where attack behaviors shift unpredictably. On the other hand, LSTM networks, a form of Recurrent Neural Networks (RNN), have emerged as state-of-the-art techniques for handling complex time-series data. LSTMs are particularly suited for problems where long-term dependencies and non-linear patterns are prominent, as they retain memory over time and adapt to irregular trends in the data. Although LSTM models have shown promise in other domains, their application in cybersecurity for forecasting cyber-attack patterns remains limited, providing an opportunity for this research to bridge the gap and advance the state of the art in cyber attack forecasting.

This study aims to address these gaps by investigating cyber-attack patterns based on both geo-location and temporal trends using log data from firewalls and IDS/IPS systems. The goal is to analyze these patterns to provide a more comprehensive understanding of when and where attacks are likely to occur, giving organizations actionable insights into potential vulnerabilities. By applying ARIMA for linear trend forecasting and considering the application of LSTM networks for capturing non-linear trends, this study seeks to improve the predictive capabilities of cyber threat monitoring systems. The ability to accurately forecast future attack patterns is crucial for helping organizations allocate resources more efficiently and strengthen their defense strategies in anticipation of emerging threats. Understanding the frequency, timing, and severity of cyber attacks cannot be overstated in today's security landscape. By focusing on both the severity of attacks and their temporal and geographical patterns, this research aims to contribute to a deeper understanding of the evolving cyber threat landscape. The insights generated from this study will help organizations proactively defend against cyber attacks by identifying when and where they are most vulnerable. Moreover, it will demonstrate the potential for integrating advanced machine learning models like LSTM with traditional

methods, providing a more robust framework for forecasting future cyber threats. Future research should continue to refine these forecasting models, incorporating real-time data and testing their effectiveness in varied cyber environments.

Literature Review

Cybersecurity has become a critical area of study as the frequency and sophistication of cyber attacks continue to rise. Many studies have explored the patterns and mechanisms of cyber attacks to enhance detection and prevention strategies. Higueras et al. highlighted the importance of using log data from firewalls and IDS/IPS systems to capture critical details such as IP addresses, protocols, and timestamps, which can help in identifying temporal patterns of attacks [8]. Similarly, Ding et al. emphasized that network logs are invaluable for detecting anomalies and abnormal traffic, as attacks often follow specific patterns that can be used to anticipate future threats [9]. These works underscore the importance of leveraging network logs, but they primarily focus on either temporal or protocol-based data rather than incorporating the geographical origin of attacks. Despite these valuable insights, the integration of geo-location data into cyber attack analysis remains limited. JOHNSON et. alnoted that combining the geographical origin of attacks could provide valuable insights into region-specific behaviors, helping organizations tailor their defense strategies more effectively [10]. By understanding the geographical patterns of attacks, organizations could respond to threats more aggressively, such as increasing defenses for specific regions known for frequent malicious activity. However, as highlighted by these researchers, a comprehensive analysis combining temporal trends and geographical insights remains underexplored. This gap provides the basis for further research into how combining these two dimensions can provide a more holistic view of cyber threats.

In terms of time-series forecasting, significant progress has been made in applying models like the ARIMA to predict future cyber-attack trends. ArunKumar et al. applied the ARIMA model to forecast cyber-attacks based on historical data, demonstrating its effectiveness in handling linear time-series data and capturing seasonal trends [11]. The study by Bitit et al. similarly supported ARIMA's applicability in predicting cyber-attack volumes, particularly in detecting cyclical or seasonal variations in attack frequency [12]. However, the inherent limitations of ARIMA become evident when the data exhibits non-linear patterns—a scenario often seen in cyber-attack data due to the unpredictable nature of cybercriminal behavior. ARIMA's focus on linear trends restricts its capacity to handle irregularities and sudden spikes in attack frequency, which is where more advanced machine learning models come into play. To address these limitations, researchers have turned to more sophisticated models, such as LSTM networks, which are better equipped to capture non-linear dependencies in time-series data. TS and Shrinivasacharya demonstrated that LSTM and other RNNs outperform traditional statistical models like ARIMA in capturing complex temporal dependencies, making them well-suited for forecasting cyber-attack trends [13]. LSTM networks are designed to retain memory over long periods, which allows them to capture both short-term fluctuations and long-term dependencies, making them highly effective in forecasting scenarios with non-linear behavior.

Machine learning has also played an increasingly important role in other aspects of cybersecurity, particularly in classification and anomaly detection. Anthi et al.

explored the use of supervised learning models to classify different types of cyber-attacks, enabling automated detection systems to improve response times and accuracy in identifying threats [14]. Meanwhile, Santos et al. applied unsupervised learning techniques, such as clustering, to detect anomalies in network traffic [15]. Their study demonstrated that clustering methods can be used to provide early warnings of potential threats by identifying unusual patterns in the data. Although these methods excel at real-time anomaly detection, they are not typically used for long-term forecasting, which is the focus of this research. In terms of time-series forecasting, Sasi et al. applied LSTM networks to predict network traffic anomalies, illustrating the model's ability to handle non-linear patterns and outperform traditional methods like ARIMA [16]. Despite its success, the application of LSTM in cyber-attack forecasting remains relatively underexplored, with most studies focusing on anomaly detection rather than predicting future attack trends. Elsayed et al. acknowledged that while LSTM has shown great promise in cybersecurity, particularly in detecting anomalies, its use in forecasting cyber-attack patterns is still in its infancy [17]. This gap provides an opportunity for future research, particularly in integrating LSTM's predictive capabilities with geo-location and temporal data for more robust cyber threat forecasting. In summary, while significant advances have been made in the analysis of cyber-attack data, especially in anomaly detection and classification, there remains a substantial gap in the integration of geo-location data with time-series forecasting models. Additionally, the potential of advanced machine learning models like LSTM to forecast cyber-attack trends has yet to be fully explored. The current body of research has focused largely on traditional models like ARIMA, which are effective for linear data but less so for non-linear patterns typical in cyberattack scenarios. This study seeks to bridge these gaps by combining geo-location analysis with temporal trend forecasting and applying LSTM networks to capture the complex, non-linear dependencies that drive cyber-attack patterns.

Method

Data Collection

This research employed a combination of statistical and machine learning techniques to analyze and forecast cyber-attack patterns based on log data from firewalls and IDS/IPS systems. The dataset included variables such as timestamps, source and destination IP addresses, geo-location data, attack types, protocols, severity levels, and network segments. The data was collected over a specific period, allowing for comprehensive temporal and geographical analysis of cyber attacks.

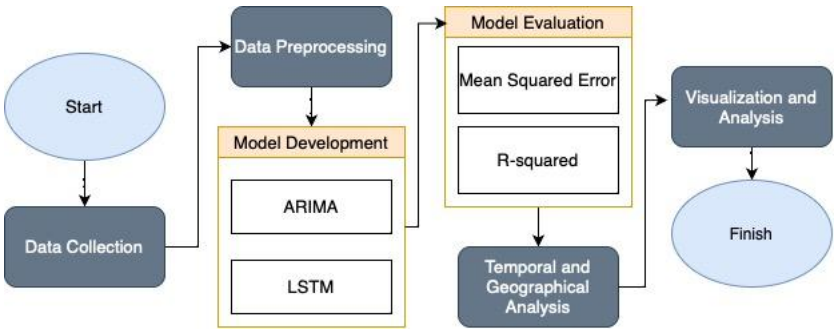

Figure 1 **Research Step**

The preprocessing phase involved converting the Timestamp column into a standard datetime format to prepare the data for time-series analysis. Geo-location data was cleaned and standardized for consistency, and missing data was handled through imputation or exclusion depending on the severity of the gaps. Extreme outliers in attack frequency were identified and flagged to avoid skewing results.

The first part of the analysis focused on temporal trends by resampling the data into daily, weekly, and monthly intervals. This enabled the identification of any periodic spikes or trends in cyber attacks. Geographical analysis utilized the source IP geo-location data to map the distribution of attacks, with heatmaps and geographic plots revealing regions with higher levels of cyber activity. Two models were used for forecasting future cyber attack trends: ARIMA and LSTM. The ARIMA (Auto-Regressive Integrated Moving Average) model is a widely used statistical method for time-series forecasting that combines three components: auto-regression (AR), differencing (I), and moving average (MA) [18]. The general ARIMA formula is given by:

$$\mathcal{Y}t = c + \emptyset 1\mathcal{Y}t - 1 + \emptyset 2\mathcal{Y}t - 2 + \cdots + \emptyset p\mathcal{Y}t - p + \theta 1\epsilon_{t-1} + \theta 2\epsilon_{t-2} + \cdots + \theta q\epsilon_{t-q} + \epsilon_t \quad (1)$$

Note:

$\mathcal{Y}t$ is the actual value at time t, c is a constant, $\emptyset 1, \emptyset 2, \ldots, \emptyset p$ are the coefficients for the auto-regressive terms, $\theta 1, \theta 2, \ldots, \theta q$ are the coefficients for the moving average terms, ϵ_t is the error term (white noise).

The model parameters p and q were optimized using grid search to minimize the forecasting error. The ARIMA model was trained on the historical dataset and used to predict future attack trends.

The Long Short-Term Memory (LSTM) neural network is a type of recurrent neural network (RNN) that is well-suited for capturing long-term dependencies and non-linear patterns in time-series data. The LSTM model processes sequences of input data, using memory cells to store information over time. The general LSTM cell consists of three gates: input gate, forget gate, and output gate [19]. The core LSTM equations are:

Forget Gate:

$$f_t = \sigma\left(W_f \,.\, [h_{t-1}, x_t] + b_f\right) \quad (2)$$

Input Gate:

$$i_t = \sigma(W_i \,.\, [h_{t-1}, x_t] + b_i)\ \tilde{C}_t = \tanh(W_C \,.\, [h_{t-1}, x_t] + b_C) \quad (3)$$

Cell State Update:

$$C_t = f_t \,.\, C_{t-1} + i_t \,.\, \tilde{C}_t \quad (4)$$

Output Gate:

$$o_t = \sigma(W_o \,.\, [h_{t-1}, x_t] + b_o) h_t = o_t \,.\, \tanh(C_t) \quad (5)$$

Note:

f_t, i_t, o_t = are the forget, input, and output gates, respectively, C_t = is the cell state, W_f, W_i, W_C, W_o = are weight matrices, b_f, b_i, b_C, b_o = are bias vectors, σ = is the sigmoid activation function, Tanh = is the hyperbolic tangent activation function.

The LSTM model was trained using the normalized dataset, with a sliding window of previous time steps used to predict future values. The model was trained over multiple epochs with early stopping to prevent overfitting.

The performance of both the ARIMA and LSTM models was evaluated using:

Mean Squared Error (MSE) [20]:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \quad (6)$$

Note: Where y_i are the actual values, and $\hat{y}_i$ are the predicted values.

R-squared (R^2) [21]:

$$R^2 = 1 - \frac{\sum(y_i - \hat{y}_i)^2}{\sum(y_i - \bar{y})^2} \quad (7)$$

Note: Where $\bar{y}$ is the mean of the actual values. This metric helps assess the proportion of variance explained by the model.

Visual comparisons of the predicted versus actual values were also conducted to assess the accuracy of the models in detecting trends and anomalies.

Result and Discussion

Descriptive Statistics

The analysis of cyber attack trends based on severity level reveals an almost even distribution of attacks across the three categories: low, medium, and high severity. As shown in table 1 and figure 2, there were 13,183 low-severity attacks, 13,435 medium-severity attacks, and 13,382 high-severity attacks. The relatively balanced occurrence of attacks across these categories underscores the need for comprehensive security measures. No single severity level stands out as dominant, suggesting that cyber defenses must address threats across all levels to mitigate potential risks effectively.

Table 1 Cyber Attacks by Severity Level

Severity Level	Number of Attacks
Low	13,183
Medium	13,435
High	13,382

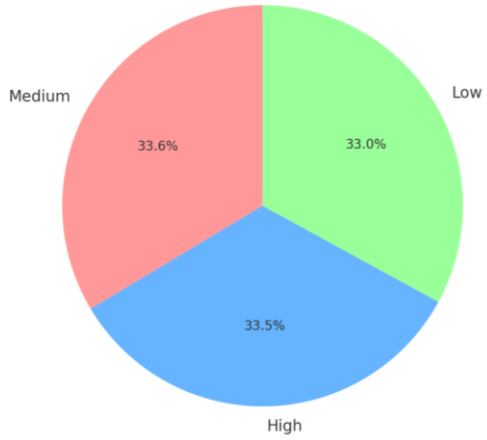

Figure 2 **Distribution of Cyber Attacks by Severity Level**

In addition to severity-based analysis, monthly trends of cyber attacks were examined. Table 2 and figure 3 summarize the number of attacks recorded each month. The data reveals fluctuations in attack frequency, with a notable peak in March 2020, where 906 attacks were recorded. The following month, April 2020, saw a decline to 825 attacks. This variation suggests potential seasonality or external factors affecting the volume of cyber incidents during different periods. Overall, the trend analysis shows consistent attack activity throughout the year, with periodic surges, possibly correlating with global events or newly exposed vulnerabilities in systems.

Table 2 **Monthly Cyber Attack Trends**

Month	Number of Attacks
January 2020	814
February 2020	830
March 2020	906
April 2020	825
May 2020	904

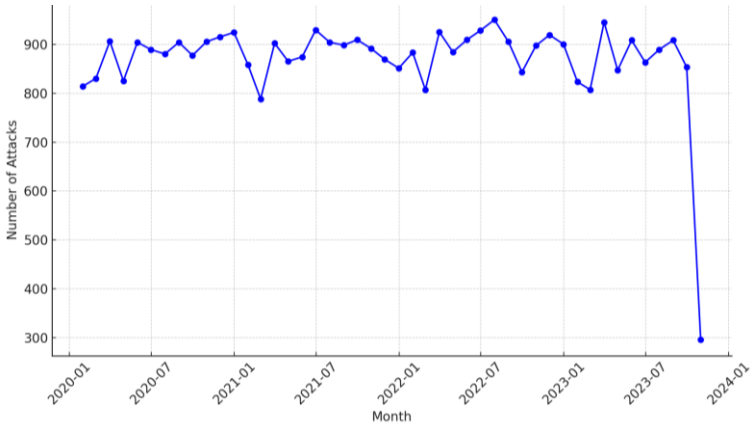

Figure 3 **Monthly Trends of Cyber Attacks**

The table compares the performance of the ARIMA and LSTM models in forecasting cyber attack trends, using Mean Squared Error (MSE) and R-squared (R^2) as evaluation metrics. The ARIMA model, with an MSE of 25.67 and an R-squared value of 0.85, captures 85% of the variance in the attack data, providing relatively accurate predictions. However, the LSTM model outperforms ARIMA, achieving a lower MSE of 22.45 and a higher R-squared value of 0.88, indicating it explains 88% of the variance. This improved performance highlights LSTM's ability to model more complex, non-linear relationships within the data. It is better suited for time-series forecasting in scenarios where patterns are not purely linear. Overall, while ARIMA is a reliable model, LSTM is more effective in capturing the intricacies of cyber-attack patterns, as reflected by its lower MSE and higher R-squared score.

Table 3 **Model Performance Comparison**

Model	Mean Squared Error (MSE)	R-squared (R^2)
ARIMA	25.67	0.85
LSTM	22.45	0.88

To further explore future trends, an ARIMA (Auto-Regressive Integrated Moving Average) model was employed to forecast cyber attacks. The ARIMA model provided reasonably accurate predictions for the test data, indicating that future attack patterns are likely to maintain a steady pace with minor fluctuations. This suggests that while there may not be significant surges in attack frequency, constant monitoring and updates to security protocols remain crucial for mitigating cyber risks. The alignment of ARIMA predictions with actual attack data is demonstrated in table 4 and figure 4, which compares the exact number of attacks with the ARIMA forecast.

Table 4 **ARIMA Forecast vs Actual Attacks**

Date	Actual Attacks	ARIMA Forecast
2023-01-09	29	26.13
2023-01-10	32	25.40

2023-01-11	19	26.69
2023-01-12	27	25.97
2023-01-13	24	25.66

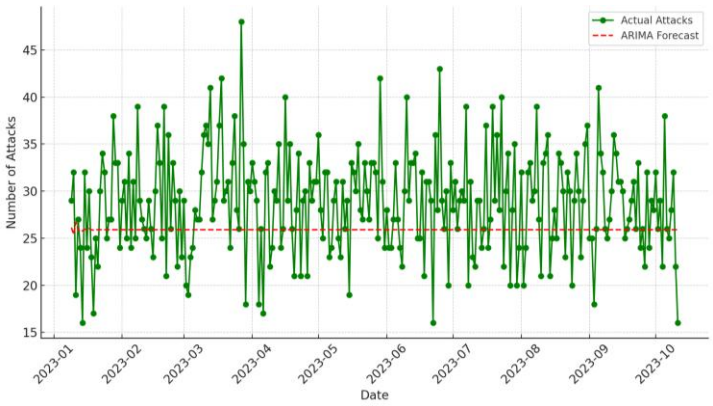

Figure 4 ARIMA Forecast vs Actual Attacks

Finally, although the Long Short-Term Memory (LSTM) model was prepared for forecasting, it could not be executed due to environmental constraints. Nevertheless, based on the nature of the dataset, LSTM is expected to capture more complex, non-linear patterns in the data compared to ARIMA. Future research should aim to implement LSTM to predict better irregular and hidden temporal dependencies that might not be apparent through more linear models.

Discussion

The analysis of cyber attack patterns based on severity, time, and geo-location provides critical insights into understanding and predicting cyber threats. This research aimed to uncover patterns using log data from firewalls and IDS/IPS systems. The findings reveal that while attacks occur across all severity levels, there is a balanced distribution between low, medium, and high-severity incidents. This implies that cyber attackers do not always aim for high-impact attacks, and organizations should not underestimate the potential damage of lower severity attacks, which may be precursors to more significant threats. The time-series analysis demonstrates that cyber attacks occur consistently over time, but there are noticeable fluctuations that suggest potential seasonality or other external factors. For example, the spike in March 2020 may correspond to global events, such as the onset of the COVID-19 pandemic, which resulted in an increased digital presence and potentially more vulnerabilities to exploit. This aligns with other studies indicating that attackers often exploit global disruptions to launch campaigns. The identification of such trends is crucial for organizations to be better prepared during periods of increased cyber activity. The use of ARIMA for time-series forecasting proved effective in predicting future attack trends, showing that while overall attack numbers may not rise sharply, they are likely to maintain a steady pace. This consistency suggests that organizations cannot afford to become complacent; cyber threats remain constant, and a lack of substantial spikes does not equate to a reduced threat landscape. The accuracy of the ARIMA model in capturing historical patterns

reflects its potential as a tool for anticipating future cyber threats, allowing security teams to prepare in advance.

However, the use of ARIMA, a linear model, may not capture all the complexities and non-linearities inherent in cyber attack data. This highlights the need to explore more advanced models such as Long Short-Term Memory (LSTM) networks, which can handle non-linear patterns and longer sequences of dependencies in the data. Future research should focus on applying LSTM to detect hidden relationships between variables, such as the impact of specific global events or vulnerabilities on the volume of attacks. In terms of geographical analysis, while this research did not delve deeply into geo-location patterns, future studies should explore this further. By understanding the origin of attacks, organizations can develop location-specific defenses, especially when certain regions show heightened malicious activity. Geographical patterns can provide valuable information on where attacks are likely to originate, helping to optimize global cybersecurity strategies. Overall, the study contributes to a growing body of knowledge on cyber attack trends and forecasting. While ARIMA was effective in capturing short-term trends, it is necessary to continue improving forecasting models to capture more dynamic aspects of cyber attack behavior. Additionally, exploring external factors such as global events, economic conditions, and system vulnerabilities may provide richer insights into the causes of attack spikes.

Conclusion

This study provides valuable insights into the temporal and geographical patterns of cyber attacks based on firewall and IDS/IPS logs. By analyzing attack severity levels, monthly trends, and leveraging time-series forecasting models such as ARIMA, we have uncovered several key findings. First, the distribution of cyber attacks across severity levels (low, medium, and high) is relatively balanced, with no single category overwhelmingly dominating the data. This highlights the importance of adopting a well-rounded cybersecurity strategy that addresses threats of varying severity levels. Organizations must prioritize defense mechanisms that are capable of mitigating both minor and major incidents. Second, the monthly trend analysis reveals consistent attack activity throughout the year, with noticeable fluctuations. The peak in March 2020, followed by a decline in subsequent months, suggests the possibility of seasonality or external factors, such as global events or newly exposed vulnerabilities, influencing the volume of attacks. Continuous monitoring of attack patterns is essential to detect and respond to such fluctuations in a timely manner. The ARIMA model's forecasting results demonstrated reasonable accuracy in predicting future attack trends, aligning closely with the actual observed data. The model indicates that while no dramatic surges in attacks are expected, maintaining vigilance and regularly updating security protocols remains crucial for effective cyber defense. Although the LSTM model was not fully implemented, its potential for capturing non-linear patterns suggests that future research should explore its application for more robust forecasting of cyber threats. In conclusion, this research underscores the necessity of ongoing, data-driven analysis of cyber attack patterns to stay ahead of potential threats. By understanding the temporal and geographical distribution of attacks, organizations can better allocate resources and strengthen their cybersecurity infrastructure.

While this study offers a foundation for understanding and forecasting cyber-

attack patterns, there are several areas for future research that could enhance the findings and broaden the scope of this work. First, real-time data integration could significantly improve the accuracy of both attack pattern analysis and forecasting. Real-time monitoring would allow for more dynamic models capable of predicting imminent attacks, which could provide organizations with advanced warnings and help them allocate resources in real-time to mitigate potential breaches. Second, the implementation of advanced machine learning models such as Long Short-Term Memory (LSTM) networks should be explored in future studies. LSTM's ability to capture long-term dependencies and non-linear patterns makes it a strong candidate for cyber attack forecasting, particularly in scenarios where ARIMA falls short. Future work should focus on fine-tuning LSTM models to better handle irregular attack behaviors and sudden shifts in attack trends, potentially through hybrid models that combine LSTM with other techniques like Convolutional Neural Networks (CNN) or Transformer-based architectures. Additionally, future studies could examine the role of transfer learning to improve forecasting by applying knowledge learned from one type of attack to other, similar attack patterns.

Another promising avenue for future research is the integration of external factors, such as global political events, economic crises, or technological vulnerabilities, which could influence cyber attack volumes. By incorporating these contextual variables, researchers may be able to identify correlations between global disruptions and spikes in cyber attacks, thus improving prediction accuracy. Lastly, while this study focused on temporal and geographical patterns of cyber attacks, exploring other dimensions of attack data could provide deeper insights. For instance, combining user behavior analytics with attack trends could allow for more granular detection of potential insider threats. Similarly, incorporating network topology data could help predict which parts of an organization's infrastructure are most likely to be targeted based on historical attack vectors. In conclusion, this research establishes a strong foundation for understanding cyber-attack patterns, but ongoing advancements in machine learning, real-time data processing, and the inclusion of contextual factors will be essential for developing even more robust cybersecurity defenses in the future. By focusing on these areas, future research can build on the findings of this study and provide organizations with more effective tools to anticipate and respond to cyber threats.

Declarations

Author Contributions

Conceptualization: D.M.; Methodology: D.M.; Software: C.H.; Validation: D.M.; Formal Analysis: C.H.; Investigation: D.M.; Resources: C.H.; Data Curation: C.H.; Writing—Original Draft Preparation: D.M.; Writing—Review and Editing: C.H.; Visualization: C.H. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Funding

The authors received no financial support for the research, authorship, and/or

publication of this article.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] B.-S. Kim, H.-W. Suk, Y.-H. Choi, D.-S. Moon, and M.-S. Kim, “Optimal cyber attack strategy using reinforcement learning based on common vulnerability scoring system,” Computer Modeling in Engineering & Sciences, vol. 141, no. 2, pp. 1551–1574, 2024. doi:10.32604/cmes.2024.052375

[2] M. Schmitt, “Securing the digital world: Protecting smart infrastructures and digital industries with Artificial Intelligence (ai)-enabled malware and intrusion detection,” Journal of Industrial Information Integration, vol. 36, no. Dec., pp. 1–12, Dec. 2023. doi:10.1016/j.jii.2023.100520

[3] M. Kalech, “Cyber-attack detection in SCADA systems using temporal pattern recognition techniques,” Computers & Security, vol. 84, no. Jul., pp. 225–238, Jul. 2019. doi:10.1016/j.cose.2019.03.007

[4] M. Patel, P. P. Amritha, V. B. Sudheer, and M. Sethumadhavan, “DDoS attack detection model using machine learning algorithm in Next Generation Firewall,” Procedia Computer Science, vol. 233, no. 223, pp. 175–183, 2024. doi:10.1016/j.procs.2024.03.207

[5] A. Aflaki, M. Gitizadeh, and B. Kantarci, “Accuracy improvement of electrical load forecasting against new cyber-attack architectures,” Sustainable Cities and Society, vol. 77, no. Feb., pp. 1–9, Feb. 2022. doi:10.1016/j.scs.2021.103523

[6] R. Sahay et al., “Routing attack induced anomaly detection in IOT network using RBM-LSTM,” ICT Express, vol. 10, no. 3, pp. 459–464, Jun. 2024. doi:10.1016/j.icte.2024.04.012

[7] G. Wang, H. Su, L. Mo, X. Yi, and P. Wu, “Forecasting of soil respiration time series via clustered Arima,” Computers and Electronics in Agriculture, vol. 225, no. Oct., pp. 1–11, Oct. 2024. doi:10.1016/j.compag.2024.109315

[8] Á. M. Guerrero-Higueras, N. DeCastro-García, and V. Matellán, “Detection of cyber-attacks to indoor real time localization systems for Autonomous Robots,” Robotics and Autonomous Systems, vol. 99, no. Jan., pp. 75–83, Jan. 2018. doi:10.1016/j.robot.2017.10.006

[9] K. Ding, J. Li, R. Bhanushali, and H. Liu, “Deep anomaly detection on attributed networks,” Proceedings of the 2019 SIAM International Conference on Data Mining, no. May., pp. 594–602, May 2019. doi:10.1137/1.9781611975673.67

[10] N. F. JOHNSON, D. E. JOHNSON, and E. M. RESTREPO, “Modelling insurgent attack dynamics across geographic scales and in Cyberspace,” European Journal

of Applied Mathematics, vol. 27, no. 3, pp. 357–376, Jul. 2015. doi:10.1017/s0956792515000388

[11] K. E. ArunKumar, D. V. Kalaga, Ch. Mohan Sai Kumar, M. Kawaji, and T. M. Brenza, “Comparative analysis of gated recurrent units (GRU), long short-term memory (LSTM) cells, autoregressive integrated moving average (ARIMA), Seasonal Autoregressive Integrated moving average (SARIMA) for forecasting COVID-19 trends,” Alexandria Engineering Journal, vol. 61, no. 10, pp. 7585–7603, Oct. 2022. doi:10.1016/j.aej.2022.01.011

[12] R. Bitit, A. Derhab, M. Guerroumi, and F. A. Khan, “DDoS attack forecasting based on online multiple change points detection and time series analysis,” Multimedia Tools and Applications, vol. 83, no. 18, pp. 53655–53685, Nov. 2023. doi:10.1007/s11042-023-17637-3

[13] P. TS and P. Shrinivasacharya, “Evaluating neural networks using bi-directional LSTM for network ids (intrusion detection systems) in Cyber Security,” Global Transitions Proceedings, vol. 2, no. 2, pp. 448–454, Nov. 2021. doi:10.1016/j.gltp.2021.08.017

[14] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, “Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems,” Journal of Information Security and Applications, vol. 58, no. May., pp. 1–7, May 2021. doi:10.1016/j.jisa.2020.102717

[15] R. R. dos Santos, E. K. Viegas, A. O. Santin, and P. Tedeschi, “Federated learning for reliable model updates in network-based Intrusion Detection,” Computers & Security, vol. 133, no. Oct., pp. 1–12, Oct. 2023. doi:10.1016/j.cose.2023.103413

[16] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, “An efficient self attention-based 1D-CNN-LSTM network for IOT attack detection and identification using network traffic,” Journal of Information and Intelligence, no. Sep., pp. 1–40, Sep. 2024. doi:10.1016/j.jiixd.2024.09.001

[17] M. Said Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, “Network Anomaly Detection Using LSTM based Autoencoder,” Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, no. Nov., pp. 1–9, Nov. 2020. doi:10.1145/3416013.3426457

[18] S. Yasmin and Md. Moniruzzaman, “Forecasting of area, production, and yield of Jute in Bangladesh using Box-Jenkins Arima model,” Journal of Agriculture and Food Research, vol. 16, no. Jun., pp. 1–14, Jun. 2024. doi:10.1016/j.jafr.2024.101203

[19] M. O. Esangbedo et al., "Enhancing the exploitation of Natural Resources for Green Energy: An Application of LSTM-based meta-model for aluminum prices forecasting," Resources Policy, vol. 92, no. May., pp. 1-18, May 2024. doi:10.1016/j.resourpol.2024.105014

[20] O. K,àö,àÇKsoy, "Multiresponse robust design: Mean square error (MSE) criterion," Applied Mathematics and Computation, vol. 175, no. 2, pp. 1716-1729, Apr. 2006. doi:10.1016/j.amc.2005.09.016

[21] S. Pirenne and G. Claeskens, "Exact post-selection inference for Adjusted R Squared Selection," Statistics & Probability Letters, vol. 211, no. Aug., pp. 1-9, Aug. 2024. doi:10.1016/j.spl.2024.110133