IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

TIME SERIES ANALYSIS ANDFORECASTING OF CYBERSECURITY INCIDENTS IN INDIA USING MONTHLY SECONDARY DATA

Dr. Pooja R. Patil
Assistant professor, School of Computing and Technology,
PTVA's Mulund College of Commerce (Autonomous),
Mulund, Mumbai, Maharashtra.

DECLARATION

This research paper is an original work based on secondary data collected from publicly available government sources. The study has been conducted for academic and research purposes.

ABSTRACT

The rapid growth of digital technologies has significantly increased the risk of cybersecurity incidents worldwide. In India, the expansion of internet penetration, digital payment systems, cloud services, and online platforms has led to a notable rise in cyber-related threats. In this context, understanding the temporal behavior of cybersecurity incidents is essential for effective monitoring and policy formulation. This study presents a time series analysis and forecasting of cybersecurity incidents in India using monthly secondary data.

The primary objectives of the study are to analyze trends in cybersecurity incidents, examine possible seasonal variations, and develop a forecasting model for future incident levels. The dataset consists of 42 monthly observations collected from official government sources, including cybersecurity and crime-related reports. The data were analyzed using statistical techniques such as descriptive statistics, linear trend regression, One-Way Analysis of Variance (ANOVA), and Simple Exponential Smoothing.

The regression analysis indicates that there is no statistically significant linear trend in cybersecurity incidents over the study period. Similarly, the ANOVA results reveal that there is no significant seasonal variation across different months. The forecasting model based on Simple Exponential Smoothing suggests relatively stable future incident levels, although the widening confidence intervals indicate increasing uncertainty in long-term predictions.

Overall, the findings suggest that cybersecurity incidents in India exhibit irregular fluctuations rather than stable trend or seasonal patterns. This implies that cyber threats are influenced by dynamic and external factors rather than predictable temporal structures. The study highlights the importance of continuous cybersecurity monitoring, adaptive response strategies, and proactive preparedness to mitigate cyber risks in an evolving digital environment.

Keywords: Cybersecurity, Time Series Analysis, Forecasting, Simple Exponential Smoothing, Secondary Data, India

1. INTRODUCTION

Digital technologies have become an essential part of modern society and economic activities. The widespread use of online banking, e-commerce, cloud computing, mobile applications, and digital communication has significantly increased dependence on information technology systems. Although technological advancements have improved efficiency and accessibility, they have also introduced new cybersecurity risks and vulnerabilities.

Cybersecurity incidents such as phishing, malware attacks, ransomware, identity theft, financial fraud, and data breaches have increased rapidly across the world. India has experienced substantial growth in internet users and digital financial services in recent years, leading to greater exposure to cyber threats. As digitalization expands, cybersecurity has become a critical concern for governments, businesses, and individuals.

Statistical analysis of cybersecurity incidents is important for understanding incident behavior and developing preventive measures. Time series analysis helps in identifying patterns, fluctuations, and future movements in time-based data. Forecasting cybersecurity incidents can support better cybersecurity planning and preparedness.

The present study focuses on analyzing and forecasting cybersecurity incidents in India using monthly secondary data collected from official government sources. Statistical techniques including regression analysis, ANOVA, and Simple Exponential Smoothing are applied to study trend patterns, seasonal variation, and future predictions.

- **RESEARCH GAP**

Previous studies have primarily focused on machine learning techniques and technical intrusion detection systems. Limited research has applied statistical time series methods to monthly cybersecurity incident data in the Indian context. This study addresses this gap through trend analysis, seasonal analysis, and forecasting using statistical techniques.

- **SIGNIFICANCE OF THE STUDY**

The study is important because cybersecurity incidents are growing concerns for governments, businesses, and individuals. Statistical analysis and forecasting of cybersecurity incidents can assist policymakers and organizations in understanding cyber threat behavior and improving cybersecurity preparedness.

2. REVIEW OF LITERATURE

Cybersecurity has become an important area of research due to increasing cyber threats and growing digital dependency. Several researchers have studied cybercrime patterns, forecasting methods, and cybersecurity management using statistical and analytical techniques.

Sharma and Gupta (2020) reported that rapid digitalization and increased internet usage have contributed to the growth of cybercrime incidents in India. Their study emphasized the importance of cybersecurity awareness and preventive strategies.

Kumar and Singh (2021) analyzed cybersecurity incidents in India and identified phishing attacks and online financial fraud as major concerns. The study highlighted the need for continuous cybersecurity monitoring.

Verma et al. (2021) applied time series techniques for analyzing cyberattack trends and suggested that forecasting models can improve cybersecurity preparedness.

Patel and Shah (2022) examined forecasting methods for cybersecurity incidents and highlighted the usefulness of statistical forecasting techniques in identifying potential future cyber threats.

Rao and Iyer (2022) observed that cybersecurity incidents often exhibit irregular fluctuations due to changing attack strategies, technological developments, and policy interventions.

Existing literature indicates that forecasting and statistical analysis play an important role in cybersecurity planning. However, most studies have focused on machine learning approaches and intrusion detection systems, with limited application of statistical time series methods to monthly cybersecurity incident data in the Indian context. This study addresses this gap through statistical time series analysis and forecasting of cybersecurity incidents in India.

Time series analysis has been widely applied in forecasting domains such as stock markets, healthcare, weather prediction, and cybersecurity. Methods such as exponential smoothing and ARIMA models are commonly used for short-term forecasting of time-dependent data.

Overall, previous studies highlight that cybersecurity data often exhibit irregular fluctuations due to evolving attack strategies, technological changes, and policy interventions. Therefore, forecasting models are essential for improving cybersecurity preparedness and decision-making.

3. RESEARCH METHODOLOGY

3.1 Objectives of the Study

1. To analyze the monthly trend of cybersecurity incidents in India using secondary data.
2. To examine the growth pattern and seasonal variations in cybersecurity incidents.
3. To develop a forecasting model for predicting future cybersecurity incidents in India.
4. To provide suggestions for improving cybersecurity preparedness based on the findings of the study.

3.2 Hypotheses of the Study

H01: There is no significant trend in monthly cybersecurity incidents in India.
H11: There is a significant trend in monthly cybersecurity incidents in India.
H02: There are no significant seasonal variations in cybersecurity incidents in India.
H12: There are significant seasonal variations in cybersecurity incidents in India.

3.3 Sources of Data

The study is based entirely on secondary data collected from official government sources related to cybersecurity incidents in India.

Major Sources Used

- Indian Computer Emergency Response Team (CERT-In)
- National Crime Records Bureau (NCRB)
- Data.gov.in
- Reserve Bank of India (RBI) reports on digital fraud and cybersecurity

The data consisted of monthly cybersecurity incident observations obtained from publicly available reports and datasets.

3.4 Period of Study

The study uses 42 monthly observations covering the study period from 2019 to 2022.

Dataset Description

Variable	Description
Time	Monthly observation number
Month-Year	Monthly period of observation
Incidents	Number of cybersecurity incidents reported

The dataset was converted into time series format for statistical analysis and forecasting.

3.5 STATISTICAL TOOLS USED

The following statistical techniques were applied:

- Descriptive Statistics
- Linear Trend Regression
- One-Way ANOVA
- Simple Exponential Smoothing
- Graphical Analysis

4. DATA ANALYSIS AND INTERPRETATION

4.1 Descriptive Analysis

Monthly cybersecurity incident data were analyzed using descriptive statistics. The data showed fluctuations in cybersecurity incidents across different months during the study period.

Table 4.1 Descriptive Statistics

Statistic	Value
Mean	10.57
Median	10
Standard Deviation	5.20
Minimum	2
Maximum	24
Observations	42

Interpretation

The descriptive statistics indicate moderate variability in cybersecurity incidents during the study period. The difference between minimum and maximum values suggests fluctuations in monthly incident levels. The graphical analysis indicated irregular movement in cybersecurity incidents without a consistent upward or downward pattern.

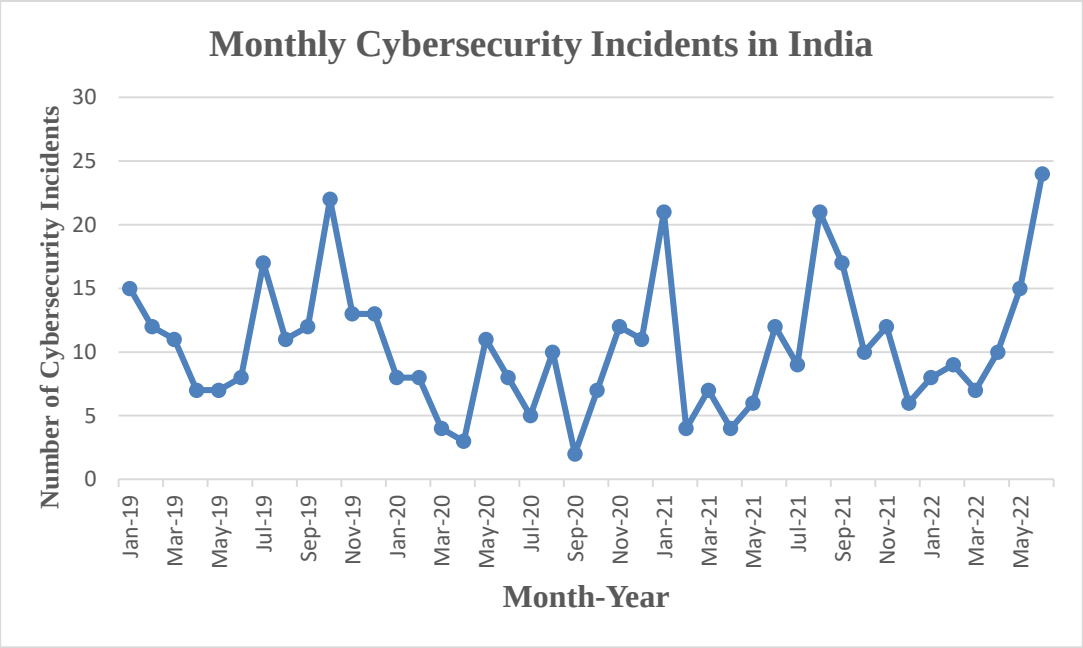

Figure 1: Monthly Cybersecurity Incidents in India

Figure 2: Forecast of Cybersecurity Incidents

Figure 1 shows the monthly cybersecurity incidents in India during the study period. The graph indicates irregular fluctuations in incident levels across different months. No consistent upward or downward trend was observed in the data.

4.2 Trend Analysis

Linear regression analysis was applied to examine the presence of a significant trend in cybersecurity incidents.

The regression model used was:

$Y_t = a + bt + et$

Where:

Y_t = Cybersecurity incidents

t = Time variable

a = Intercept

b = Trend coefficient

Table 4.2.1 Regression Output Summary

Particulars	**Value**
Multiple R	0.0575
R Square	0.0033
Adjusted R Square	-0.0216
Standard Error	5.2553
Observations	42

Table 4.2.2 ANOVA Results

Source	F Value	Significance F
Regression	0.1329	0.7173

Table 4.2.3 Coefficient Results

Variable	Coefficient	P-value
Intercept	9.9280	0.0000
Time Variable	0.0244	0.7173

Interpretation

The regression analysis revealed that the p-value associated with the time variable was greater than 0.05. Therefore, the null hypothesis was accepted. The results indicate that no statistically significant trend existed in monthly cybersecurity incidents during the study period.

Seasonal Variation Analysis

One-Way ANOVA was applied to examine whether cybersecurity incidents differed significantly across different months.

Table 4.2.4 ANOVA Summary

Source of Variation	SS	df	MS	F	P-value
Between Groups	262.1548	11	23.8323	0.8449	0.5993
Within Groups	846.2500	30	28.2083		

Interpretation

The ANOVA results indicated that the p-value was greater than 0.05. Therefore, the null hypothesis was accepted. The findings suggest that there was no statistically significant seasonal variation in cybersecurity incidents across different months.

4.3 Forecasting Analysis

Since the trend and seasonality components were not statistically significant, Simple Exponential Smoothing was used for forecasting future cybersecurity incidents.

Forecast results indicated relatively stable incident levels in future periods. However, confidence intervals widened gradually over time, indicating increasing uncertainty in long-term predictions.

Table 4.3.1Forecast Values

Time Period	Forecast	Lower Confidence Bound	Upper Confidence Bound
43	24.02	13.44	34.61
44	24.05	13.13	34.97
45	24.07	12.84	35.31
46	24.10	12.55	35.65
47	24.12	12.26	35.98
48	24.15	11.98	36.31

Interpretation

The forecast results indicate relatively stable future cybersecurity incident levels. The gradual widening of confidence intervals suggests increasing uncertainty in future periods.

Forecast Interpretation

The forecast graph showed that future cybersecurity incidents are expected to remain relatively stable around recent observed levels. The widening confidence intervals indicate uncertainty associated with long-term forecasting.

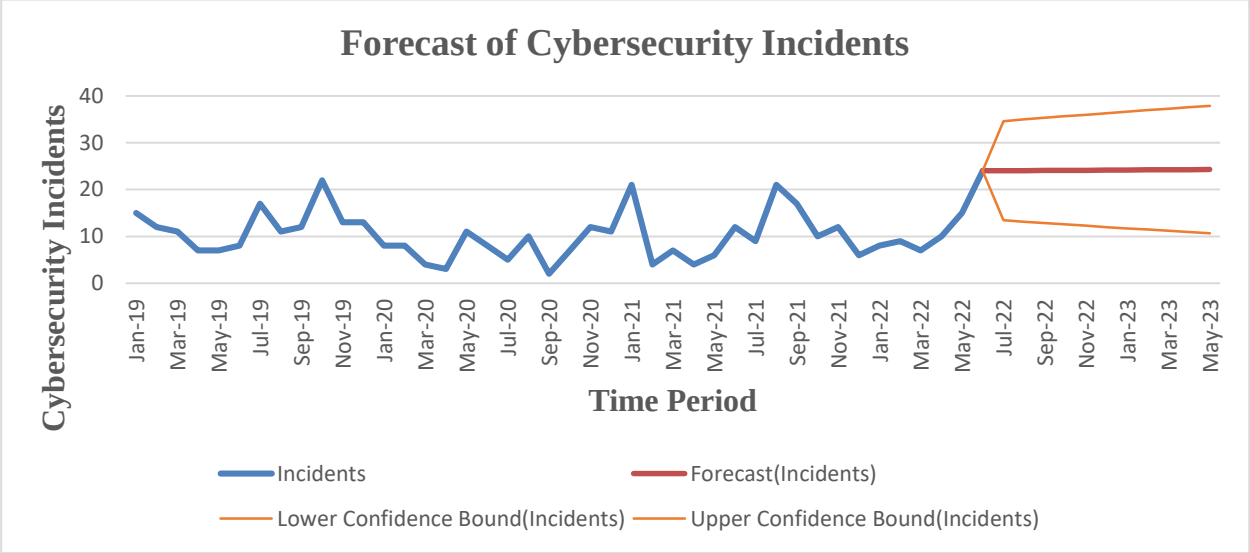

Figure 2: Forecast of Cybersecurity Incidents

Figure 2 presents the forecasted cybersecurity incidents using the Simple Exponential Smoothing method. The forecast values remain relatively stable over future periods, while the widening confidence intervals indicate increasing uncertainty in long-term predictions.

5. FINDINGS OF THE STUDY

Monthly cybersecurity incidents in India showed irregular fluctuations during the study period.
Linear regression analysis indicated that no statistically significant trend existed in cybersecurity incidents.
One-Way ANOVA results showed no significant seasonal variation across months.
Forecasting analysis using Simple Exponential Smoothing indicated relatively stable future cybersecurity incident levels.
Confidence intervals widened in future forecast periods, indicating increasing uncertainty in long-term predictions.
Cybersecurity incidents appear to be influenced by irregular external factors rather than stable temporal patterns.

6. CONCLUSION

The present study examined cybersecurity incidents in India using time series analysis and forecasting techniques based on monthly secondary data. The findings revealed that cybersecurity incidents did not exhibit significant linear trend or seasonal variation during the study period. The data showed irregular fluctuations, indicating that cybersecurity incidents are dynamic and influenced by multiple external factors.
Forecasting analysis using Simple Exponential Smoothing suggested relatively stable future cybersecurity incident levels, although uncertainty increased for long-term predictions. The results emphasize the importance of continuous cybersecurity monitoring, preparedness, and adaptive security strategies.
The study contributes to the growing literature on cybersecurity analytics in India and demonstrates the usefulness of statistical time series techniques in cybersecurity research.

7. SCOPE FOR FUTURE RESEARCH

Future studies may apply advanced machine learning and deep learning forecasting techniques.
Larger datasets with longer time periods may improve prediction accuracy.
Category-wise analysis of cybercrime incidents can be conducted.
Comparative studies between different countries may provide broader insights.
Real-time cybersecurity monitoring and predictive analytics may be explored.

8. SUGGESTIONS

Government agencies should strengthen cybersecurity awareness and preparedness programs.
Organizations should continuously monitor cybersecurity threats and vulnerabilities.
Advanced cybersecurity analytics and real-time monitoring systems should be implemented.
Regular cybersecurity audits and employee training programs should be conducted.
Future research may use larger datasets and advanced forecasting models for improved prediction accuracy.

9. LIMITATIONS OF THE STUDY

The study is based on secondary data only.
The dataset consisted of only 42 monthly observations.
Advanced machine learning models were not applied due to dataset limitations.
The study focused only on overall cybersecurity incidents and not specific attack categories.

10. REFERENCES

[1] Indian Computer Emergency Response Team (CERT-In), “Cyber Security Incident Reports,” 2023.
[2] National Crime Records Bureau, *Crime in India Report*, 2022.
[3] Reserve Bank of India, *Annual Report on Banking Frauds and Cybersecurity*, 2022.
[4] D. N. Gujarati, *Basic Econometrics*, 5th ed. New York, USA: McGraw-Hill Education, 2015.
[5] D. C. Montgomery, C. L. Jennings, and M. Kulahci, *Introduction to Time Series Analysis and Forecasting*. Wiley, 2015.
[6] C. Chatfield, *The Analysis of Time Series: An Introduction*. CRC Press, 2016.
[7] R. J. Hyndman and G. Athanasopoulos, *Forecasting: Principles and Practice*. OTexts, 2018.
[8] R. Sharma and A. Gupta, “Cybercrime trends in India: Challenges and preventive measures,” *International Journal of Cyber Studies*, vol. 12, no. 2, pp. 45–58, 2020.

[9] P. Kumar and V. Singh, "Analysis of cybersecurity incidents in India using statistical methods," *Journal of Information Security*, vol. 8, no. 1, pp. 23–34, 2021.
[10] H. Patel and M. Shah, "Forecasting cyber threats using time series techniques," *International Journal of Data Analytics*, vol. 10, no. 3, pp. 88–101, 2022.