FORECASTING CYBERCRIME IN INDIA AND CORRELATION OF CYBERCRIME THREATS WITH HEALTH SYSTEM DURING COVID-19 PANDEMIC

Abstract

Due to the rise of cybercrimes globally, the usage of Information and communication technology is bringing more complex issues and threats. In the current situation, the demand for internet usage has increased significantly and the activities of more people occur at home. So, large numbers of people are connected online for work and other network activities. Since the pandemic, cybercrime has increased in our country. This study is divided into two sections, first, we fit regression between the duration of non-pandemic and pandemic periods for the number of cybercrimes in India. In this section, we used a linear regression model and we observed the relation between pandemic and non-pandemic observations. In another paper, we investigated the future trends of cybercrime (Online fraud) through the Autoregressive Integrated Moving Average Model (ARIMA). Finally, we explore the vulnerability of cybercrime and its complex problems and the impact of cyber security threats on the National Health System during the pandemic.

Keywords: Cybercrime, Cyber security, Linear Regression model, ARIMA, Health system, Prediction.

Authors

R. Sasikumar
Department of Statistics
Manonmaniam Sundaranar University
Tirunelveli, Tamil Nadu, India.
sasikumarmsu@gmail.com

S. Indira
Department of Statistics
Manonmaniam Sundaranar University
Tirunelveli, Tamil Nadu, India.
indirasri91@gmail.com

P. Arriyamuthu
Department of Statistics
Manonmaniam Sundaranar University
Tirunelveli, Tamil Nadu, India.
arriyamth@gmail.com

I. INTRODUCTION

Recent research in cybercrime and security analysis has been centered on identifying threats, and vulnerabilities and providing suitable defense mechanisms to develop the robustness of online systems. With the improvement of communication technology, day-to-day cyber security has become very challenging. These crimes may use a variety of techniques from hacking to spreading inaccurate and deceptive material online. Also, it is known as "computer-related crime" which is an illegal behavior that involves a computer either as an instrument, a target (or) a means for perpetuating future crimes that come within the ambit of cybercrime (Chawki M, 2015). The time series of cyber-attacks recorded by a cyber-defense instrument known as honey pots, which passively monitor the incoming internet connections, is one of the cyber threats data (Zhan Z et.al, 2013). Long-range dependence (LRD) and extreme nonlinearity, among other phenomena, were investigated in these datasets and described the two separate statistical methods used for cyber incident and prediction (Sun N et.al, 2018). In the objective of detecting vulnerabilities, supervised machine learning methods including logistic regression, neural network, and random forest, have been proposed (Li Z et.al, 2016). (Ye N et.al, 2004) The performance of the Markov chain technique for detecting cyber-attacks was studied, and it was discovered that it is not always resilient depending on the window size.

(Yong Z et.al, 2007) Analyze the situation using the NSSA model. To assess the present network security situation, the evaluation uses a multi-perspective approach that includes descriptions of security attacks, vulnerabilities, and security services. (Zhang Q et.al, 2009) discussed the intent recognition problem in cyber security situation awareness through the hidden Markov model. (Liang W et.al, 2018) analyzed the hidden Markov model for predicting network security is ineffective. Therefore, a weighted hidden Markov model is developed to predict the security situation of a mobile network. (Chintal P et.al, 2018) analyzed the importance of data mining and machine learning, to use the linear regression model for the prediction of future cybercrime trends concerning Maharashtra state. (Fang X et.al, 2019) constructed a deep learning framework for predicting cyber-attack rates based on statistical methods. (Nagasubramaniyan G and Adithya Vikram Sakthivel, 2018) intends to propose a sufficient and effective multi-dimensional linear regression model for cybercrime prediction in India. (Rajadevi R et.al, 2020) predict the category of crime occurrence by using the multinomial logistic regression. Describe the major technologies, cyber-attacks, and cyber risks during the pandemic and security of health systems. (Meha Shah, 2020) Has the ARIMA model in machine learning techniques which is used on three parameters easy to estimate based on cyber-attack data. (Khawar Islam et al & Raza A, 2020) were used for forecasting the number of crimes in London based on time series techniques. Some techniques for testing the relationship between two variables and also discussed quantifies the strength of the linear relationship between a pair of variables (Khushbu Kumari & Yadav S, 2018). To forecast future crime trends, data mining techniques were applied. and then linear regression was trained by crime data of Bangladesh (Md. Abdul Awal et al, 2016). (Feba Babu & Sebastian K, 2018) Study on big data, Cyber Security, Types of cyber security threats and important challenges of cyber security, and Vulnerability prediction through statistical models. (Menaka Muthuppalaniappan & Stevenson K, 2021) illustrated the cyber security threats principles for healthcare organizations, resourcing and universities during Covid-19 pandemic.

II. MATERIALS AND METHODS

The study covers 28 states and 8 union territories of India. Data have been collected from the website of the National Crime Records Bureau (NCRB) for a period covering 2003 to 2020. The aim of this study is to analyse the data related to national online fraud. Then the two statistical models are developed on this data sequence. The Methods are divided into two sections (1) Linear regression Model, (2) ARIMA Model.

III. LINEAR REGRESSION MODEL

The model of linear regression was first introduced by Sir Francis Galton in 1894. This model is the quantified relation between the considered variables by fit a linear equation to observed data and also provide sufficient explanation of how the input observations affect the output observation. To analyze and the associated task for the data used to forecast the values of this model is applied to identify the current status of cybercrime. These algorithms to identify the cost coefficients and to minimize the error in computing the results. The equation of regression for funding predicted values as the mathematical form y= mx+c, which describes the best fit line for the relation between dependent (y) and independent (x). Here, predicts a variable y [Dependent variable / Target variable] as a linear function of another variable x [Independent variable/ Input variable]. In regression almost we fit data well with minimum error (or) cost value. The variables of the form $(x_1, y_1),(x_2, y_2),\ldots,(x_n, y_n)$ where $x_1 \in x$ and $y_1 \in y$. The form hypothesis function can be expressed as, $h_\theta(x) = \theta_0 + \theta_1 x_1 + \theta_2 x_2 + \ldots + \theta_n x_n \Rightarrow h_\theta(x) + \theta^T x$ where $\theta_0, \theta_1, \theta_2, \ldots, \theta_n$ are regression parameters. The cost (or) error function defined as,

$$J(\theta_0, \theta_1, \theta_2, \ldots\ldots \theta_n) = \frac{1}{2m} \sum_{i=1}^{m} (h_\theta(x^{(i)}) - y^{(i)})^2$$

The focus of linear regression almost fits the data sequence well with minimum error (or) cost function $J(\theta_0, \theta_1, \theta_2, \ldots, \theta_n)$ by computing $\theta_0, \theta_1, \theta_2, \ldots, \theta_n$, so that $h_\theta(x)$ close to y for (x, y) in training data. To fit the model uses the batch gradient descent algorithm. This concept is one way to minimize the error (or) cost value of θ_0 and θ_1. The algorithm as follows:

$$\theta_j := \theta_j - \alpha \frac{1}{2m} \sum_{i=1}^{m} (\theta^T x(x^{(i)}) - y^{(i)})^2$$

Where α be a learning rate. With every step of the algorithm, the parameters $\theta_0, \theta_1, \theta_2, \ldots, \theta_n$, come closer to the optimal values that will aim the minimize cost

$$J(\theta_0, \theta_1, \theta_2, \ldots, \theta_n).$$

IV. AUTO REGRESSIVE INTEGRATED MOVING AVERAGE MODEL

In our study, the ARIMA model is established for Cybercrime data. This model combines three processes, such as classified an "ARIMA (p, d, q)" model, where: p denotes the number of autoregressive terms, d denotes the number of no seasonal differences needed for stationary, and q denotes the number of moving averages. This model is used to predict future data in series based on the past value. The model is described as,

$$\phi(B)(1-B)^d Y_t = \theta(B)e_t$$

Where $\phi(B)$ and $\theta(B)$ are denote expressed as the Autoregressive and moving average characteristic polynomials estimated at B (Backward shift Operator). The following steps are used for the predictions of Cybercrime rates based on ARIMA.

- ***Identification of Model:*** We draw a graphical plot to understand the stationary in the data sequence. Stationary denote the existence of constant mean and variance.

- ***Model Evaluation:*** The ARIMA model has been used to select order p, d, q values to define model. We are calculating the autocorrelation function and partial autocorrelation function for ARIMA model parameters. This model evaluates also the intervention of determination of the time lag (p, q) for autocorrelation and moving average (i.e, AR and MA).

- ***Prediction:*** The select ARIMA (p, d, q) model is applied to predict values for the future trends and estimate the parameters such as Mean square error (MSE), Mean absolute Deviation (MAD), Percentage mean absolute deviation (PMAD) and mean absolute percentage error (MAPE). Explain the process of our study plan shown in figure 1

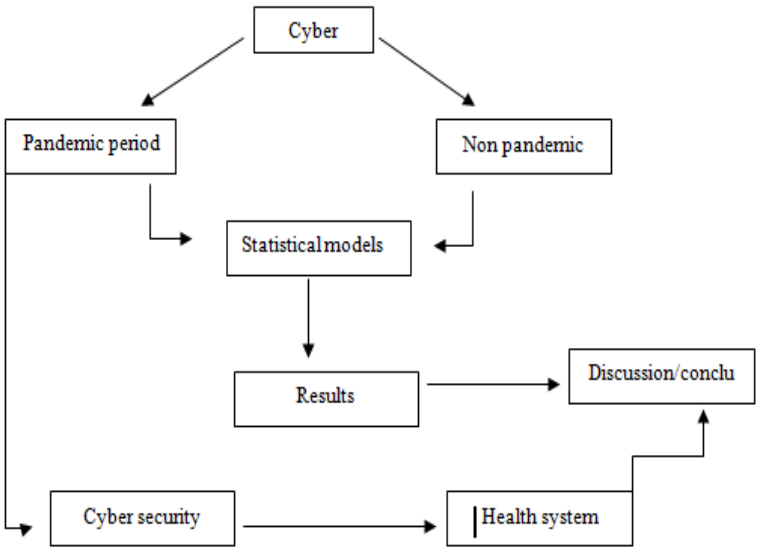

Figure 1: Shows the Process of Study Plan.

1. **Analysis and Results:** In this study, the linear regression model was presented for cybercrime data. Also, the ARIMA model was proposed to predict future trends.

2. **Results for Linear Regression Model :** We are computing the following measurement based on a linear regression model using Cybercrime reported during Non-pandemic (independent) and pandemic (dependent).

Table 1: Shows the Output for Linear Regression Model.

Model summary				
Model	R	R Square	Adjusted R^2	Std. error of the estimate
1	0.986[a]	0.972	0.971	526.340

Table 2: Shows the Analysis of Variance with P

ANOVA[a]						
Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	254031948.107	1	254031948.107	890.923.	0.000.[b]
	Residual	.000	26	.000		
	Total	254031948.107	27			

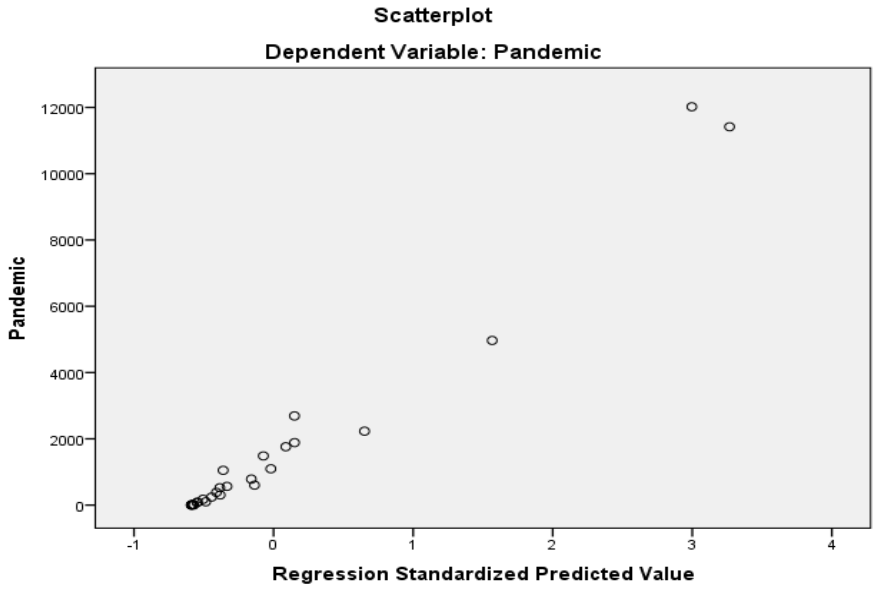

Figure 2: Scatter Plot of Pandemic Period

The null hypothesis, based on the above findings, is that there is no association between non-pandemic cybercrime reports and pandemic cybercrime records. Since the p- values are less than 0.05. Furthermore, we can observe from the R2 statistic that the models explain more than 97 percent of the values seen in the data sequence. and make the models quite accurate (i.e. this model a good fit for given data). Therefore, represent the regression equation as: $y = (71.98) + 1.77x$

V. PREDICTION FOR CYBERCRIME RATES USING ARIMA MODEL

The ARIMA model is utilized in this section to forecast future trends in cybercrime rates in India. This model is one of the statistical models for the forecast of time series analysis data. We are forecasting future trends of cybercrime rates in India using the ARIMA model. We choose of best fit ARIMA (2, 1, 2) model for cybercrime rates are performed to the properties of AIC and BIC. This model can be used for non-stationary time series data.

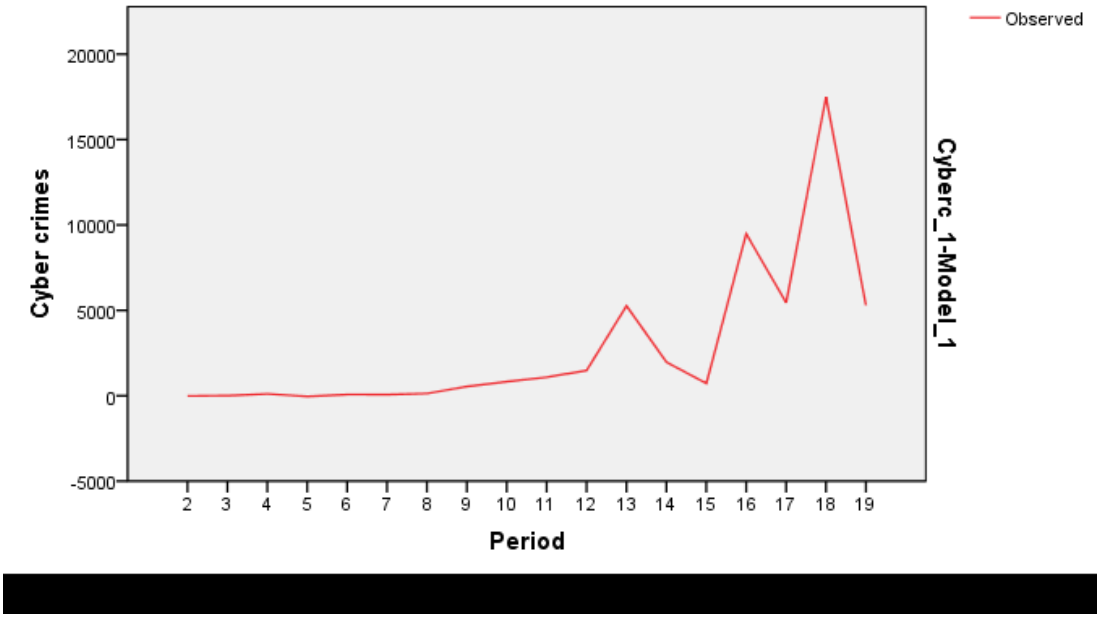

Figure 3: Shows The Line Plot of The First Order Differenced Sugarcane Production Data.

Table 3: Shows the Parameter Estimated for Cybercrime Rates Using ARIMA.

Model	Stationary R^2	R^2	RMSE	MAPE	MAE
ARIMA(2,1,2)	0.594	0.512	3734.446	784.413	2079.771

The above table displays the accuracy of the ARIMA model when it was used to the cybercrimes data. This model first classifies the data sequence into training and testing sets. The data sequence will then be used to this model with seasonality to set as TRUE. The select ARIMA model was used to predict future trends. Then we estimated the parameters such as Mean absolute error (MAE) and Mean absolute percentage error (MAPE).

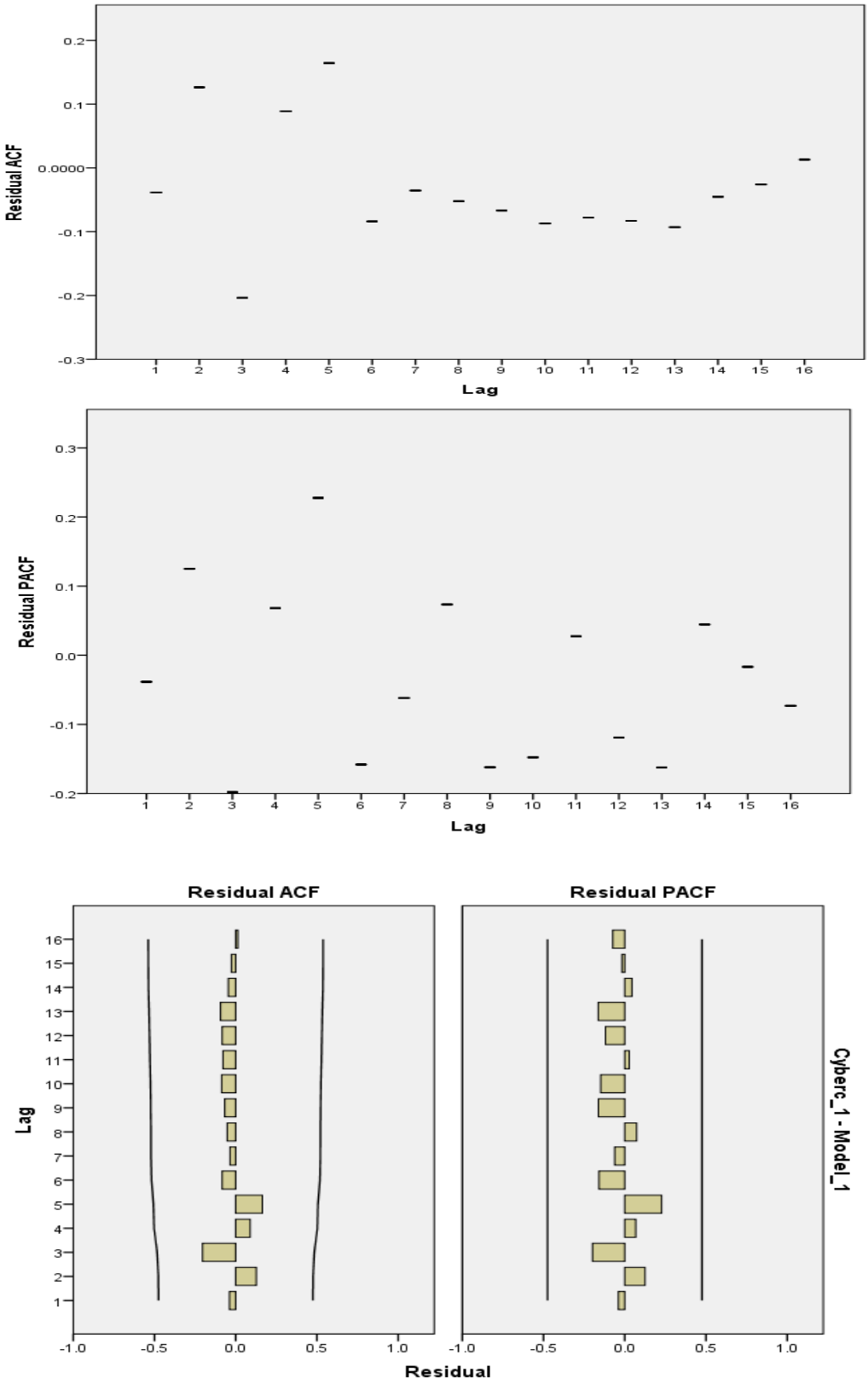

Figure 4: Shows the Auto Correlation Function (ACF) and Partial Auto Correlation Function (PACF) for the Model Fit.

We observe that the above Figure 4, the ACF and PACF are estimated; only 1st lag is outside the shaded portion. Hence, we fit autoregressive at two. Similarly, the first differencing of the partial autocorrelation function and 1st lag is coming out of the shaded region. Hence, we fit the moving average at two. Therefore we chose ARIMA (2, 1, 2) model to forecast future trends of cybercrime rates. The following figure shows that the Production for a period of up to three years by fitting ARIMA (2, 1, 2) model to our data.

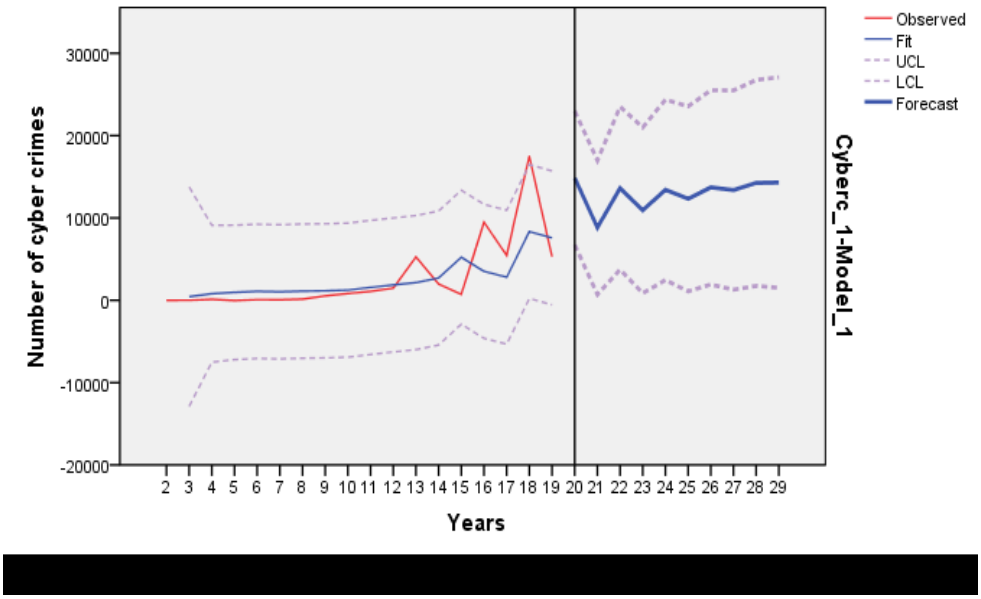

Figure 5: Shows the Graphical Representation of Observed and Forecasted for Cyber Crime Rates.

From this Figure 5, we suggest that the ARIMA (2, 1, 2) model is fitted to our data sequence and we observed that the cybercrime rates were forecasted. The results show the cybercrime rates are rising.

VI. IMPLICATIONS OF CYBER SECURITY THREATS ON NATIONAL HEALTH SYSTEM

In the world, developing and use of technology are rising day to day. At the same level, there's a rise the cyber security threats and privacy problems as well. These has been a high increase in the number of uses connecting working networks during pandemic. As a result of the situation's worsening benefits, malevolent authors become more active in attacking and hacking various platforms in order to promote financial gain and other bad interests. The number of malicious attackers and spam emails registered has increased. These intruders are focusing on individuals, government reports, and even the health system. The health industries are based on applications of Information Communication and Technology, which offer its users including doctors, nurses, physicians, and patients, a spacious range of medical services known as e-health systems. They are the most vulnerable and targeted systems in the event of a pandemic. If something goes wrong, it can result in a negative situation, such as the loss of valuable public lives. Any deadly cyber-attack will likely escalate the haggle currently faced by health administrations with resources. This section studied complex issues of Cyber Security on National Health systems, the several Cyber

security threats, and attitudes to technology effects vulnerability discussions The most important cyber security issues focused on software vulnerabilities. Organizations must maintain effective vulnerability management processes, which include analysis, identification, and reporting. Cyber security is mainly focused on protecting technologies, networks, computers, and programs from attack, damage or theft. The main aim of our study is to investigate the major issues of cyber security threats on the national health system is discussed. Malware, spam email, malicious websites, ransomware, malicious domains, business email compromise, and malicious are all cyber security issues. Mental health issues may increase vulnerability to Cyber security threats during the pandemic. While experiencing psychotic symptoms, some people with mental conditions may go online and also today's youth generation has a negative emotional impact from heavy usage of the network. These cyber security threats have a guide to a few serious privacy problems and concerns. Isolation, disruption of everyday lifestyle, financial hardship uncertainty, and continuous misinformation are also common psychological effects of the pandemic (Brooks SK et al, 2020). A history of mental health problems raises the risk of the psychotic symptoms of the pandemic (Lazzari C et al, 2020). During the pandemic, many people are filing invoices to obtain healthcare. Nearly half of Union States are concerned about preventing the virus in medical settings, such as hospitals and deferred medical care for persons with mental problems. (Kahl KG & Correll C. U, 2020). In people with more mental health problems, an absence of specific treatments may increase the chance of developing psychiatric symptoms. (Shinn AK & Viron M, 2020). Mental stress may increase the effects of cybercrime. Changes in daily routines and social isolation may disrupt coping techniques and reduce social communication in people with mental illnesses. (Costa M et al, 2020). The stochastic differential equations using Markov chain for the study of the problem of mean-square exponential stabilization in network system (Yuan C & Lygeros J, 2005). (Shukla et al, 2009) discussed all comparison studies in Internet traffic. The uses of technology and network systems are bringing more impacts and threats in terms of cyber security (Humayun M. et al, 2020). Table 5 displays some types of online fraud related to the pandemic and describes the descriptions.

S. No	***Categoriesof Cyber security threats***	***Descriptions***	**References**
1	Trojan horse	These viral threats will do something in the situation of a pandemic, stealing medical records and passwords by work keystrokes.	
2	Malicious spyware	These cybercriminals have seen pandemic as an opportunity to conduct attacks for monetary gain and to further their malicious goals.	
3	Spam emails	The attackers have always utilized these emails on a large scale to achieve their aims; for example, the end of the email address commonly ends with the institution's website, and individuals can verify whether they are interacting with the correct organization from there. The intruders apply an email such as	(Zhang, Q et.al, 2009), (Song X et.al, 2016), (McKinsey

		coronovirusfund@who.org	& Company,
4	Phishing	This is one of the most common cybercrimes. For example, a website offering fake vaccine reports for Pandemic.	2020), (TCS Worldwide, 2020)
5	Ransom ware	Cybercriminals are targeting public health facilities, hospitals, educational institutions, and other institutions in this attack. Human health systems are being affected by ransomware and resources such as the details of Covid-19 cases confidentiality and integrity are being compromised	
6	Mobile Threats	These include the deletion of mobile data and the leakage of account information on social media.	

VII. DISCUSSIONS

In this article, the cybercrime cases recorded were used for the time period covering 2002 to 2020. Since the pandemic, many people's daily activities have been connected to the internet for work, education, shopping, and surge in cybercrimes. So, first, we identified relation to the proposed logistic regression model. The data had been separated into pandemic and non-pandemic. The linear regression model can be fitted and the linear relationship between the pandemic periods has been analysed. From this, we can conclude that the maximum amounts of cybercrimes were recorded during the pandemic period. This is because the usage of networks during the pandemic is greatly increased. So the regression model is used to find the relationship between pandemic and non-pandemic. Whereas we calculated the R^2 statistic, we can identify that model explains more than 97 percent of the values observed in our data sets, creating the model accurately. Based on this future prediction can be made. Next, we used the ARIMA (2, 1, 2) model for the cybercrime data to predict the future trends which were based on different parameters simple to evaluate based on our data. Such as the corresponding mean square value and mean absolute percentage error values were estimated. Finally, we discussed the Cyber security threats impacts and changes to the National health system during the COVID-19 pandemic.

VIII. CONCLUSION AND FUTURE WORK

In this research study, we used linear regression model to propose a statistical model for investigating cybercrime. Also predicted based on the ARIMA model. We concluded that at the peak of the epidemic in our country, there was a clear and noticeable rise in cybercrime. Then we have identified the cyber security threats how to affect the health system. This research could help police investigation departments and law enforcement agencies forecast and prevent future crime in our country. For future studies, we focus on extending the methods by using other predictive and forecasting models in order to make a more comprehensive, integrated approach to the estimation of cybercrime and new threats.

REFERENCES

[1] Alghamdi, R. (2016). Hidden Markov models (HMMs) and security applications. *International Journal of Advanced Computer Science and Applications*, *7*(2), 39-47.
[2] Awal, M. A., Rabbi, J., Hossain, S. I., & Hashem, M. M. A. (2016, May). Using linear regression to forecast future trends in crime of Bangladesh. In *2016 5th International Conference on Informatics, Electronics and Vision (ICIEV)* (pp. 333-338). IEEE.
[3] Alexander, R. (2020). Using linear regression analysis and defense in depth to protect networks during the global corona pandemic. *Journal of Information Security*, *11*(04), 261.
[4] Babu, F., & Sebastian, K. (2018, August). A review on cybersecurity threats and statistical models. In *IOP Conference Series: Materials Science and Engineering* (Vol. 396, No. 1, p. 012029). IOP Publishing.
[5] Brooks, S. K., Webster, R. K., Smith, L. E., Woodland, L., Wessely, S., Greenberg, N., & Rubin, G. J. (2020). The psychological impact of quarantine and how to reduce it: rapid review of the evidence. *The lancet*, *395*(10227), 912-920.
[6] Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, digital forensics and jurisdiction* (Vol. 593). Springer.
[7] Chintal P, Gaikwad RJ, Deshmukh RR. Cybercrime analysis of Maharashtra state using gradient descent approach with linear regression. Int. J. Pure Appl. Math. 2018; 119(16):3537-42.
[8] Ch, R., Gadekallu, T. R., Abidi, M. H., & Al-Ahmari, A. (2020). Computational system to classify cybercrime offenses using machine learning. *Sustainability*, *12*(10), 4087.
[9] Costa, M., Pavlo, A., Reis, G., Ponte, K., & Davidson, L. (2020). COVID-19 concerns among persons with mental illness. *Psychiatric Services*, *71*(11), 1188-1190.
[10] Dr. G. Nagasubramaniyan, Adithya Vikram Sakthivel. A Linear Regression Model for the Prediction and Prevention of Cybercrimes in India. International Journal for Research in Applied Science & Engineering Technology.2018 April; 6(4):2149-2153.
[11] Deshmukh, S., Rade, R., & Kazi, D. (2019). Attacker behaviour profiling using stochastic ensemble of hidden markov models. *arXiv preprint arXiv:1905.11824*.
[12] Fang, X., Xu, M., Xu, S., & Zhao, P. (2019). A deep learning framework for predicting cyber-attacks rates. *EURASIP Journal on Information security*, *2019*(1), 1-11.
[13] Gu, J. (2020, August). An Effective Intrusion Detection Model Based on Pls-Logistic Regression with Feature Augmentation. In *China Cyber Security Annual Conference* (pp. 133-140). Springer, Singapore.
[14] Gero, S., Back, S., LaPrade, J., & Kim, J. (2021). Malware Infections in the US during the COVID-19 Pandemic: An Empirical Study. *International Journal of Cybersecurity Intelligence & Cybercrime*, *4*(2), 25-37.
[15] Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*(4), 3171-3189.
[16] Islam, K., & Raza, A. (2020). Forecasting crime using ARIMA model. *arXiv preprint arXiv:2003.08006*.
[17] Kumari, K., & Yadav, S. (2018). Linear regression analysis study. *Journal of the practice of Cardiovascular Sciences*, *4*(1), 33.
[18] Kahl, K. G., & Correll, C. U. (2020). Management of patients with severe mental illness during the coronavirus disease 2019 pandemic. *JAMA psychiatry*, *77*(9), 977-978.
[19] Kumar, P., Kalita, H., Patairiya, S., Sharma, Y. D., Nanda, C., Rani, M., & Bhagavathula, A. S. (2020). Forecasting the dynamics of COVID-19 pandemic in top 15 countries in April 2020: ARIMA model with machine learning approach. *MedRxiv*.
[20] Li, Z., Zou, D., Xu, S., Jin, H., Qi, H., & Hu, J. (2016, December). Vulpecker: an automated vulnerability detection system based on code similarity analysis. In *Proceedings of the 32nd Annual Conference on Computer Security Applications* (pp. 201-213).
[21] Liu, E. (2017). *Logistic Regression Model for Predicting Warning "Incident" Rates and Implications for the Common Vulnerability Scoring System* (Doctoral dissertation, The Ohio State University).
[22] Liang, W., Long, J., Chen, Z., Yan, X., Li, Y., Zhang, Q., & Li, K. C. (2018). A security situation prediction algorithm based on HMM in mobile network. *Wireless Communications and Mobile Computing*, *2018*.
[23] Lazzari, C., Shoka, A., Nusair, A., & Rabottini, M. (2020). Psychiatry in time of COVID-19 pandemic. *Psychiatria Danubina*, *32*(2), 229-235.
[24] Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior*, *35*(7), 581-591.

[25] Michael G. (2020). Knowledge based system for predicting cybercrime patterns using data mining techniques. Journal of Critical Reviews, 7(10):2043-53.
[26] McKinsey & Company, "COVID-19 Crisis Shifts Cyber security Priorities and Budgets." 2020. [Online]. Available: https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecuritypriorities-and-budgets#.
[27] Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1), mzaa117.
[28] R. Rajadevi, E. M. Roopa Devi, S. Vinoth Kumar. (2020) Prediction of Crime Occurrence using Multinomial Logistic Regression. International Journal of Innovative Technology and Exploring Engineering. Jan; 9(3):1432-1435.
[29] Shukla, D., Tiwari, V., & Kareem, P. A. (2009). All Comparison Analysis in Internet Traffic Sharing Using Markov Chain Model in Computer Networks. *Computer Science & Telecommunications*, *2009*(6).
[30] Song, X., Xiao, J., Deng, J., Kang, Q., Zhang, Y., & Xu, J. (2016). Time series analysis of influenza incidence in Chinese provinces from 2004 to 2011. *Medicine*, *95*(26).
[31] Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2018). Data-driven cybersecurity incident prediction: A survey. *IEEE communications surveys & tutorials*, *21*(2), 1744-1772.
[32] Saleh, M. (2019). A Proactive Approach for Detecting Ransomware based on Hidden Markov Model (HMM). *International Journal of Intelligent Computing Research*, *10*.
[33] Shinn, A. K., & Viron, M. (2020). Perspectives on the COVID-19 pandemic and individuals with serious mental illness. *The Journal of clinical psychiatry*, *81*(3), 14205.
[34] Singh, S., Parmar, K. S., Kumar, J., & Makkhan, S. J. S. (2020). Development of new hybrid model of discrete wavelet decomposition and autoregressive integrated moving average (ARIMA) models in application to one month forecast the casualties cases of COVID-19. *Chaos, Solitons & Fractals*, *135*, 109866.
[35] Shah M (2020). *Survey on Prediction of Cyber Intrusion with Time Series Analysis*.
[36] TCS Worldwide, "How COVID-19 is Dramatically Changing Cyber security." 2020. [Online]. Available: https:// www.tcs.com/perspectives/articles/how-covid-19-is-dramatically-changing-cybersecurity.
[37] Ye, N., Zhang, Y., & Borror, C. M. (2004). Robustness of the Markov-chain model for cyber-attack detection. *IEEE transactions on reliability*, *53*(1), 116-123.
[38] Yuan, C., & Lygeros, J. (2005). Stabilization of a class of stochastic differential equations with Markovian switching. *Systems & Control Letters*, *54*(9), 819-833.
[39] Yoo, S. (2007). Neural Network Model vs. SARIMA Model In Forecasting Korean Stock Price Index (KOSPI). *Issues in Information Systems*, (3).
[40] Yong, Z., Xiaobin, T., & Hongsheng, X. (2007, December). A novel approach to network security situation awareness based on multi-perspective analysis. In *2007 International Conference on Computational Intelligence and Security (CIS 2007)* (pp. 768-772). IEEE.
[41] Zhang, Q., Man, D., & Yang, W. (2009, November). Using HMM for intent recognition in cyber security situation awareness. In *2009 Second International Symposium on Knowledge Acquisition and Modeling* (Vol. 2, pp. 166-169). IEEE.
[42] Zhan, Z., Xu, M., & Xu, S. (2013). Characterizing honeypot-captured cyber-attacks: Statistical framework and case study. *IEEE Transactions on Information Forensics and Security*, *8*(11), 1775-1789.
[43] Zhang, L., Wang, L., Zheng, Y., Wang, K., Zhang, X., & Zheng, Y. (2017). Time prediction models for echinococcosis based on gray system theory and epidemic dynamics. *International journal of environmental research and public health*, *14*(3), 262.
[44] Zegeye, W. K., Dean, R. A., & Moazzami, F. (2019). Multi-layer hidden markov model based intrusion detection system. *Machine Learning and Knowledge Extraction*, *1*(1), 265-286.

