Vol.15, Issue No 2, 2025

Harnessing Machine Learning Models for Cyber Attack Detection and Forecasting

[1] Baley Harshitha, [2] Katuri Hindu, [3] Badireddy Asha Deepika, [4] Ganta Paul Ronald, [5] Mr. K. S. H. Prasanna Kumar

[1,2,3,4] Students, Dept. of CSE, DNR College of Engineering & Technology, Balusumudi, Bhimavaram, India.

[5] Assistant Professor, Dept. of CSE, DNR College of Engineering & Technology, Balusumudi, Bhimavaram, India.

Abstract:

Every day, governments and their populations suffer enormous financial losses due to cybercrime, making it one of the most pressing global challenges. With the frequency of cyberattacks on the rise, it is more important than ever to track down the perpetrators and learn their methods. While it has always been difficult to detect and prevent cyberattacks, new developments in the field have brought security models and AI-based prediction tools that may help. There is a lot of research on crime prediction methods, but they may not be up to snuff when it comes to cybercrime and cyberattack tactics. Making use of real-world data to pinpoint when an attack happened and who was responsible is one way to tackle this issue. The offender's demographics, the nature of the offense, the extent of property damage, and the entry points for the attack are all part of this data set. Application procedures allow forensic investigators to get data from victims of cyberattacks. Cybercrime is analyzed using two models in this research study that utilizes machine learning techniques. The goal is to predict how attributes can help identify the method of cyber-attack and the criminal. The accuracy rates of eight distinct machine-learning algorithms were found to be comparable in this investigation. Out of all the cyber-attack methods that were tested, the Support Vector Machine (SVM) linear model had the highest accuracy rate. Important details about the kinds of assaults that victims may expect to encounter were revealed in the initial model. The most successful technique for detecting malevolent actors was logistic regression, which had a high success rate. Predictions about identification were the primary focus of the second model, which compared offender and victim attributes. According to our research, the chances of being a victim of cyberattacks go down as one's education and wealth go up. Because it will make cyber-attack detection easier and the fight against them more efficient, this proposed concept is highly anticipated for implementation by cybercrime departments.

Keywords: Machine learning algorithm, Cybercrime, SVM, Cyber-attacks.

1. Introduction:

A primary goal of machine learning is to extrapolate future outcomes from previously collected data. A subfield of AI known as "machine learning" (ML) allows computers to "learn" new tasks and information without human intervention. Creating computer programs that can adapt to new data is the main objective of machine learning. Expert algorithms are crucial to the training and prediction procedures. In order for an algorithm to make predictions about fresh test data, it is fed the training data. Machine learning may be broadly classified into three areas. There are three ways to group learning: monitored, unsupervised, and reinforced. Data must be labelled by a human before a software may utilize it for supervised learning. Learning without labels is known as unlabeled learning. It supplied the algorithm for learning. It is the responsibility of this process to classify the supplied data into groups. Last but not least, reinforcement learning evolves via dynamic interactions with its surroundings and the absorption of both positive and negative feedback. With Python, data scientists may use machine learning techniques to find patterns that reveal useful information. We may classify these algorithms as either supervised or unsupervised learning, depending on how they "learn" from the data in order to generate predictions. "Classification" is the process that assigns a label to a set of data points. Classes go by a few different names: goals, labels, and groupings. Making a rough estimate of a mapping function between continuous input variables (X) and discrete output variables (y) is an important part of predictive modeling in the classification discipline. One use of supervised learning in statistics and machine learning is classification, when a computer software learns to assign new

observations to preexisting categories using known patterns. Depending on its context, this data set may comprise either numeric values (such as the subject's gender or the email's spam status) or more complex categories of information. Problems with classification may arise in many areas, including document classification, biometric identification, speech recognition, and letter analysis.

2. Methodology:

Officers from the department who focus on the kind of crime that the public has reported are summoned. The unit's database has all of the necessary documentation for these statistics. The kind, manner, year, etc., of these crimes are meticulously documented by the police. They collect information, sort it into categories, run analysis, and create visual representations. Multiple simultaneous cyberattacks on the same target are only counted as a single incident. Look at the specifics of the incident, not the statistics, to see whether various approaches were used. While there are several recorded violations, cybercrime has gained significant attention as of late. Little has been done to stop cybercrime, despite the fact that it has caused immense material and moral damage. Since there has been little research on this topic in relation to concrete evidence in previous cybercrime investigations, it was selected as a focus. By analyzing the victim's data, the suggested model hopes to predict how likely it is that the victim would be a victim of crime. Law enforcement will also be able to better characterize cybercrime suspects, victims, and offenders, as well as better predict their actions. Additionally, the model will help in avoiding any unintended consequences. More targeted therapies will be possible thanks to the study's findings, which will also increase public awareness of hazards. We compiled this data set from actual cybercrime incidents that occurred in Elaz province between 2018 and 2022. Acquiring clean data and preparing it for analysis using machine learning algorithms was a difficult task. When the data was collected, every facet of cybercrime was investigated. Data science techniques were used to extract the unnecessary parts. In Figure 1, you can see the whole inventory of crimes, damages, assaults, and attack vectors that make up the dataset. Even better, you may sort the information on these four characteristics by color. Several modules in Python used this data to make predictions.

Figure 1: The number of cybercrimes or cyberattacks done by various methods in the datasets.

One of the main libraries used by the software, Matplotlib, together with NumPy and Pandas, allowed this application to display data. The article outlines the primary advantages of utilizing machine learning techniques, including the following: the ability to identify multiple patterns in both structured and unstructured data; the

capability to detect changing criminal strategies; the ability to extract complicated data relationships; and the possibility of producing outcomes that surpass human prediction.

The term "feature selection" describes the steps used to extract relevant and related information from a database. While preparing data for machine learning, it aids in space and time conservation. Training times may rise, leading to an increased error rate in the model and greater difficulty in interpreting it, if the attributes are not chosen properly. We have defined the features and elements of our dataset. Facts pertaining to real crimes are included in Table 1. Figure 2 displays the properties of the training data as well as the attributes in our dataset, including the median, maximum, and minimum values.

Table 1: Analysis on Crime Type

Item	Crime type
Crime	Debit/ Credit Card utilization; Information misuse; Hacking
Gender type	Male/ Female/ Other
Age	Below 27 years; 28-38 years age 39-51 years age factor
Income factor	Low/ Moderate/High
Job	Working / self -employ/ House wife/ retired person/ etc.
Marriage	Single / Couple
Education Qualification	Primary/ Higher/ Under graduate

Harming	Internet shopping without having proper knowledge. Money withdraws by unknown person
Attack	Misuse of ATM card/ Creditcard Social media accounting Digital data hacking Threatening mails Shopping in unauthorized website

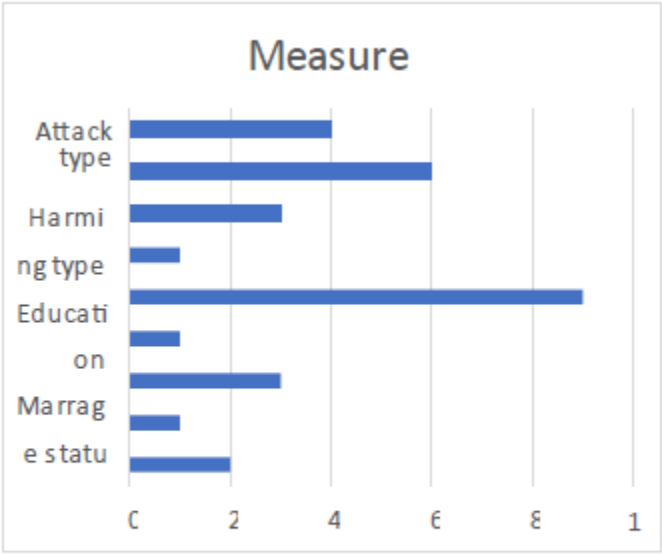


Figure 2: Measurement of actual crime

Standardization involves adjusting features so that they fit a normal distribution. Doing so should precede the use of any machine learning algorithms. Values between 1 and 10 were given to the columns to standardize the information and represent the range of data supplied. To maximize damage, aggressiveness, and attack methods, Python's Standard Scaler() was used. We trained using 80% of the data and tested with 20%. To forecast the assault tactic in the first model, we included details about the incident, the offender, the victim (gender, age, employment, income, marital status, degree of education), and the assault itself. In the second model, we sought to determine who was

responsible for the assault by looking at their age, gender, income, profession, marital status, degree of education, assault type, severity of injuries, and attack method.

3. Result with discussion:

In order to reduce crime and apprehend its perpetrators, the study's analysis of incidence data is satisfactory. One of the main goals of this research is to find ways to reduce criminal activity by analyzing collected data. Any new information or insights gained from the police investigations will be revealed in these findings. Machine learning approaches may analyze victim information, the mechanism of the cybercrime, and the likelihood of the perpetrator being recognized to determine whether the same cybercriminal was responsible for an attack. The victims of the cyber catastrophe in Elaz province have had their damages calculated using a variety of methodologies. We calculated the damages for each victim by adding together all the years in the dataset. Many attribute the decline in such incidents, especially after 2018, to the deterrent effect of regulations and awareness campaigns. As can be shown in Figure 3, the monetary damages caused by cyberattacks in Elaz are substantial. The aforementioned losses highlight the critical nature of assault approach and cyber security management.

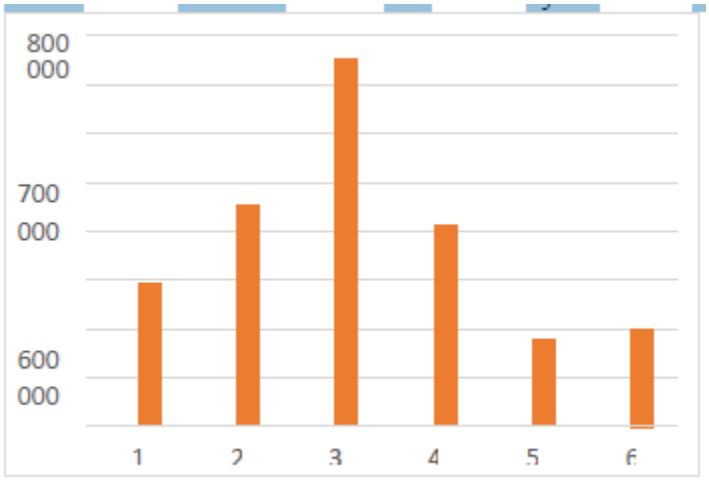


Figure 3: Economy damage by cyber attacks

This displays the output of several different algorithms, including SVM (Linear), XGBoost, DT, KNN, NB, RF, Logistic Regression, and SVM (Kernel). Could use Figure 4 as a reference to get the Pearson correlation coefficient. The strong correlations between almost all sets of data are evident in this correlation matrix.

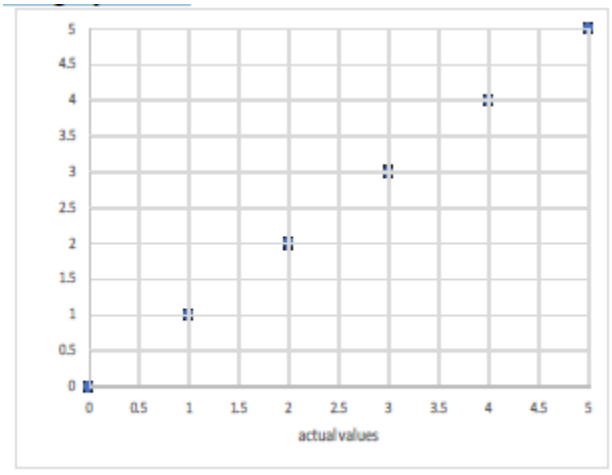
1	0.12	-0.26	-0.07	-0.19	0.0	0.41	0.44	0.25	0.03	0.08
0.12	1	0.23	0.13	0.23	-0.28	-0.03	0.24	-0.07	0.08	0.08
-0.26	-0.23	1	0.16	-0.31	0.49	0.04	-0.16	-0.06	-0.08	0.04
-0.07	-0.13	0.16	1	0.2	0.13	-0.34	0.09	0.04	0.08	0.04
0.2	0.23	-0.31	0.02	1	-0.35	-0.22	0.03	0.4	-0.01	-0.03
-0.19	-0.28	0.49	0.13	-0.35	1	-0.05	-0.19	0.01	-0.16	0.05
0.01	-0.05	0.07	-0.35	-0.26	-0.67	1	0.08	-0.08	0.05	-0.07
0.45	0.26	-0.16	0.01	0.25	-0.20	0.05	1	0.18	0.49	0.12
0.39	-0.07	-0.08	0.03	0.05	0.06	-0.06	0.19	1	-0.18	0.03
0.29	0.07	-0.04	-0.07	0.12	-0.19	0.08	0.49	-0.19	1	-0.23
0.05	0.05	0.06	0.13	-0.02	0.09	-0.05	0.12	0.05	-0.22	1

Figure 4: Confusion Matrix

Table 2: Model 1- Performance of Machine learning model

	Accuracy%	Precision%	Recall%	F1-score%
LR	94.12	95.25	94.23	95.2
KNN	90.5	72.56	77.25	73.12
SVML	96.12	96.22	96.25	96.55
SVMK	93.67	93.56	93.65	93.52
NB	82.55	82.54	82.54	82.64
DT	93.65	93.6	93.57	93.65
RF	95.89	95.88	95.84	95.68
XGBOOST	94.45	93.86	93.25	93.66

After training the dataset, we examined all feasible ways. Incorporate quality control and precision measures together. The F1 score, recall, accuracy, and precision were calculated by comparing the predicted values with the test data. The first model's prediction of the assault plan is provided in Table 2 along with its accuracy, precision, recall, and F1 score. When the numbers were crunched, SVML came out on top with the best prediction accuracy (95.55%). A narrow victory went to the SVML approach over the RF, LR, XGBoost, SVMK, DT, KNN, and NB algorithms. The success percentage was lowest in New Brunswick at 82.54%. Similar results were obtained by other algorithms as NB. Figure 5A shows the distribution graph of the real and predicted values, while Figure 5B shows the error matrix. The SVML method was used to make these predictions. When looking at the model's accuracy, recall, and F1 scores, the SVML technique was somewhat better than the competition. Results above 93% may be achieved with any of the following models: LR, SVMK, DT, RF, or XGBoost. The performance of each model was very comparable. The lowest-performing KNN and NB had scores that were nine percent below average. On the whole, the results produced by each algorithm met expectations. Based on these findings, it is feasible to use machine learning to forecast the trajectory of a cyberattack. Users will be able to anticipate which crimes an individual will face using data about that person, according to the proposed method. Be sure to include early warning systems groupings as well. When looking at the model's accuracy, recall, and F1 scores, the SVML technique was somewhat better than the competition. Results above 93% may be achieved with any of the following models: LR, SVMK, DT, RF, or XGBoost. The performance of each model was very comparable. Compared to the other algorithms, KNN and NB had a 10% lower score, indicating their poor performance. On the whole, the results produced by each algorithm met expectations. It was shown that machine learning may be used to forecast the trajectory of a cyberattack. By entering a person's traits into the suggested model (Table 2), one might anticipate the kind of crimes to which that individual would be vulnerable. It is also feasible to establish early warning systems for groups.



(A)

89	0	3	0	0	0
0	13	0	0	0	0
0	0	14	0	0	3
0	0	0	7	0	0
0	0	0	0	23	0
3	0	1	0	0	33

(B)

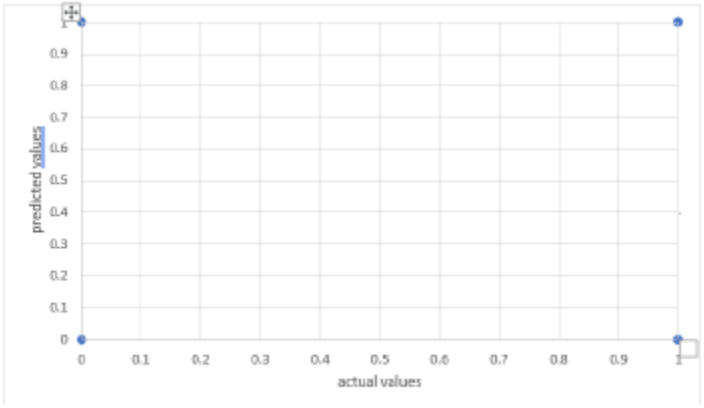
Figure 5: (A) 1st model comparison with actual values (B) Confusion matrix

Table 3: Model 2 performance in machine learning model

	Accuracy%	Precision%	Recall%	F1-score%
LR	66.52	61.25	61.23	60.56
KNN	65.23	57.46	57.88	57.14
SVML	65.66	66.81	65.85	64.89
SVMK	65.08	66.78	65.88	63.85
NB	63.15	58.29	58.32	56.24
DT	63.26	64.88	63.41	63.57
RF	64.25	64.55	64.26	63.21
XGBOOST	65.33	66.22	67.32	65.44

Table 3 displays the second model's prediction algorithms' accuracy, precision, recall, and F1 scores.

A number of methods were used to achieve accuracy: LR (66.52%), SVML (0.827%), KNN (1.44%), SVMK (1.39%), XGBoost (2.44%), RF (3.34%), and DT (3.34%). While NB had the poorest performance, the other algorithms were all rather close. Visualizations of the error matrix and the distribution graph of the actual and projected values generated by the SVML approach are shown in Figure 6A and Figure 6B, respectively. In spite of NB's poor performance, the other algorithms came quite close. Both the error matrix and the distribution graph of the actual and projected values produced by the SVML approach are shown in Figure 6A and 6B, respectively. Algorithm outputs have F1 scores, recall, and accuracy between 56% and 66%. The final product was not up to standard. We aimed to establish whether the same criminal was responsible for the crime by comparing known and unknown features of the attacker. But the findings of the model indicated that a new model should be built with more characteristics.



(A)

(A)

39	41
24	72

(B)

Figure 6: (A) Comparison error matrix (B) Confusion matrix

The size of the dataset is a constraint for the planned research project since it contains real data. We need temporal data in order to estimate time series. In a similar vein, precise estimates may help identify the perpetrator if the technical details of the attacks were recorded by the authorities.

Conclusion:

The authors of this article propose a method to detect and halt cyberattacks by combining data from past efforts with machine learning techniques. This model can predict who will be the victims and what kinds of attacks they will face. The methods used in machine learning are persuasive enough. Using linear SVMs is the way to go. At 61% accuracy, the model can predict which hacker would launch a cyberattack. Using a variety of AI approaches, I propose increasing this figure. Spreading knowledge about malware and social engineering assaults is of the utmost importance. There was a negative correlation between the victim's wealth and education level and the chance of a cyberattack. The primary goal of the research is to provide law enforcement with more efficient resources to combat cybercrime more aggressively. New tracking and warning systems for individuals with comparable qualities may be established by evaluating the traits of the assault victims that surfaced throughout our research.

References:

1. Bilen, Abdulkadir & Özer, Ahmet. (2021). Cyber-attack method and perpetrator prediction using machine learning algorithms. PeerJ Computer Science. 7. e475. 10.7717/peerj- cs.475.

2. Al-majed, Rasha & Ibrahim, Amer & Abualkishik, Abedallah & Mourad, Nahia & Almansour, Faris. (2022). Using machine learning algorithm for detect ion of cyber-at tacks in cyber physical systems. Periodicals of Engineering and Natural Sciences (PEN). 10. 261. 10.21533/pen.v10i3.3035.

3. Mazhar, T.; Irfan, H.M.; Khan, S.; Haq, I.; Ullah, I.; Iqbal, M.; Hamam, H. Analysis of Cyber Security At tacks and Its Solut ions for the Smart grid Using Machine Learning and Blockchain Methods. *Future Internet* **2023**, *15*, 83. ht tps://doi.org/10.3390/fi15020083

4. Sarker, I.H. Machine Learning for Intelligent Data Analysis and Automat ion in Cybersecurity: Current and Future Prospects. *Ann. Data. Sci.* (2022). ht tps://doi.org/10.1007/s40745-022-00444- 2

5. A. Alshehri, N. Khan, A. Alowayr and M. Yahya Alghamdi, "Cyberat tack detection framework using machine learning and user behavior analyt ics," *Computer Systems Science and Engineering*, vol. 44, no.2, pp. 1679–1689, 2023.

6. Amjad Rehman, Tanzila Saba, Muhammad Zeeshan Khan, Robertas Damaševičius, Saeed Ali Bahaj, "Internet - of-Things- Based Suspicious Act ivity Recognition Using Mult imodalit ies of Computer Vision for Smart City Security", *Security and Communication Networks*, vol. 2022, Article ID 8383461, 12 pages, 2022. ht tps://doi.org/10.1155/2022/8383461

7. Liu Qiang, Qu Xiaoli, Wang Dake, Abbas Jaffar, Mubeen Riaqa, Product Market Compet it ion and Firm Performance: Business Survival Through Innovat ion and Ent repreneurial Orientat ion Amid COVID-19 Financial Crisis, Front iers in Psychology, 12 , 2022, ISSN-1664-1078, 10.3389/fpsyg.2021.790923. URL=ht tps://www.frontiersin.org/articles/10.3389/fpsyg.2021. 790923

8. Ibor, A.E., Oladeji, F.A., Okunoye, O.B. *et al.* Conceptualisation of Cyberattack prediction with deep learning. *Cybersecur* **3**, 14 (2020). ht tps://doi.org/10.1186/s42400-020-00053-7

9. Yirui Wu, Dabao Wei, Jun Feng, "Network At tacks Detect ion Methods Based on Deep Learning Techniques: A Survey", *Security and Communication Networks*, vol. 2020, Art icle ID 8872923, 17 pages, 2020. ht tps://doi.org/10.1155/2020/8872923

10. Tehseen Mazhar, Hafiz Muhammad Irfan, Sunawar Khan, Inayatul Haq, Inam Ullah, Muhammad Iqbal, Habib Hamam, Analysis of Cyber Security At tacks and Its Solut ions for the Smart grid Using Machine Learning and Blockchain Methods,Future Internet , 10.3390/fi15020083, **15**, 2, (83), (2023).

11. McCarthy A, Ghadaf i E, Andriot is P and Legg P. (2023). Defending against adversarial machine learning at tacks using hierarchical learning. Journal of Informat ion Security and Applicat ions. **72**:C.

12. Ahsan, M.; Nygard, K.E.; Gomes, R.; Chowdhury, M.M.; Rifat, N.; Connolly, J.F. Machine Learning Techniques in Cybersecurity. Encyclopedia. Available online: ht tps://encyclopedia.pub/ent ry/25675 (accessed on 30 April 2023).

13. Kenfack, P.D.B., Mbakop, F.K. and Eyong-Ebai, E. (2021) Implementation of Machine Learning Method for the Detection and Prevention of Attack in Supervised Network. *Open Access Library Journal*, **8**, 1-25. doi: 10.4236/oalib.1108000.

14. Tewari, Shiv Hari, Data Science and Its Application in CyberSecurity (Cyber Security Data Science) (September 5, 2020). Data Science in Cyber Security and cyber threat intelligence: Sikos, Leslie F, Choo. Kim kwang. [Upcoming challenges in Cyber Security Data Science]. Security Analytics: Big Data Analyt ics for cybersecurity: A review of trends, techniques and tools: Tariq Mahmood , Uzma Afzal [Definition of Cyber, Available at SSRN: ht tps://ssrn.com/abstract=3687251

15. Zhao L, Zhu D, Shafik W, et al. Artificial intelligence analysis in cyber domain: A review. International Journal of Dist ributed Sensor Networks. 2022;18(4). doi:10.1177/15501329221084882

16. Narayan, Valliammal, and Barani Shaju. "Malware and Anomaly Detect ion Using Machine Learning and Deep Learning Methods." Research Anthology on Machine Learning Techniques, Methods, and Applications, edited by

Information Resources Management Associat ion, IGI Global, 2022, pp. 149-176. https://doi.org/10.4018/978-1-6684-6291-1.ch010

17. Ahmad Naim Irfan, Suriayat i Chuprat , Mohd Naz'ri Mahrin, Aswami Ariffin. (2022) Taxonomy of Cyber Threat Intelligence Framework. *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1295-1300.

18. Aksu, Dogukan, and M. Ali Aydin. "Detecting port scan attempts with comparative analysis of deep learning and support vector machine algorithms." *2018 International congress on big data, deep learning and fighting cyber terrorism (IBIGDELFT)*. IEEE, 2018.

19. Khuphiran, Panida, et al. "Performance comparison of machine learning models for DDoS at tacks detect ion." *2018 22nd International Computer Science and Engineering Conference (ICSEC)*. IEEE, 2018.

20. Arshey, M., and KS Angel Viji. "Thwart ing cyber crime and phishing at tacks with machine learning: a study." *2021 7th international conference on advanced computing and communication systems (ICACCS)*. Vol. 1. IEEE, 2021.

21. Shivlal Mewada, Anil Saroliya, N. Chandramouli, T. Rajasanthosh Kumar, M. Lakshmi, S. Suma Christal Mary, Mani Jayakumar, "Smart Diagnostic Expert System for Defect in Forging Process by Using Machine Learning Process", *Journal of Nanomaterials*, vol. 2022, Art icle ID 2567194, 8 pages, 2022. ht tps://doi.org/10.1155/2022/2567194

22. Rege, Manjeet , and Raymond Blanch K. Mbah. "Machine learning for cyber defense and at tack." *Data Analytics* 2018 (2018): 83.

23. P. Patro, R. Azhagumurugan, R. Sathya, K. Kumar, T. R. Kumar and M. V. S. Babu, "A hybrid approach est imates the real-t ime health state of a bearing by accelerated degradat ion tests, Machine learning," *2021 Second International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, Bengaluru, India, 2021, pp. 1-9, doi: 10.1109/ICSTCEE54422.2021.9708591.

24. Choudhary, Atul S., Pankaj P. Choudhary, and Shrikant Salve. "A Study On Various Cyber At tacks And A Proposed Intelligent System For Monitoring Such At tacks." *2018 3rd International Conference on Inventive Computation Technologies (ICICT)*. IEEE, 2018.

25. Kumari, Maya. "Applicat ion of Machine Learning and Deep Learning in Cybercrime Prevent ion—A Study." *Int. J. Trend Res. Dev* (2019): 1-4.

26. Saharkhizan, Mahdis, et al. "An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network t raffic." *IEEE Internet of Things Journal* 7.9 (2020): 8852- 8859.

27. Swaminathan, Aravind, et al. "Prediction of Cyber-at tacks and Criminality Using Machine Learning Algorithms." *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. IEEE, 2022.

28. NON, COMPENSATION OF MALICIOUS ATTACKS IN. "MACHINE LEARNING APPROACH FOR DETECTION, ESTIMATION AND COMPENSATION OF MALICIOUS
ATTACKS IN NON LINEAR CYBER CRIME PHYSICAL SYSTEMS." (2021).

29. Lilhore, Umesh Kumar, et al. "EHML: An Efficient Hybrid Machine Learning Model for Cyber Threat Forecasting in CPS." *2023 International Conference on Artificial Intelligence and
Smart Communication (AISC)*. IEEE, 2023.

30. Al-Abassi, Abdulrahman, et al. "An ensemble deep learningbased cyber-at tack detect ion in indust rial cont rol system." *IEEE Access* 8 (2020): 83965-83973.