IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 11, November 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211033 |

Analyze and Forecast the Cyber Attack Detection Process using Machine Learning Techniques

Prof. Ashwini Kamble , Siddhi Shinde, Rishikesh Pokale, Arbaz Tamboli, Sharikh Shaikh

Department of Computer Science and Engineering, K.J. College of Engineering and Management Research, Pune, India

ABSTRACT : The increasing complexity of cyber threats poses significant challenges to organizations' security infrastructure. As a result, the development of effective cyber attack detection processes is crucial in safeguarding digital assets and sensitive information. This paper aims to provide an analysis of the current state of cyber attack detection and forecast its evolution with the integration of machine learning techniques. In this study, we start by reviewing the existing cyber attack detection methods and technologies, highlighting their limitations and vulnerabilities. We then delve into the potential benefits of applying machine learning to this process, such as improving accuracy, reducing false positives, and enabling real-time threat detection. Furthermore, we discuss the various machine learning techniques commonly used in cyber attack detection, including supervised learning, unsupervised learning, and deep learning methods. We evaluate the strengths and weaknesses of each technique, providing insights into their suitability for specific detection scenarios.

KEYWORDS: Cyber Attack, Machine Learning, Machine Learning Models

I. INTRODUCTION

In an increasingly interconnected and digitized world, the proliferation of cyber threats has become a critical concern for individuals, organizations, and governments alike. Cyber attacks can disrupt operations, compromise sensitive data, and even threaten national security. To combat this growing threat landscape, the integration of machine learning techniques into the cyber attack detection process has gained significant attention. Machine learning offers the ability to analyze vast amounts of data, identify patterns, and make informed decisions in real-time, thereby enhancing the efficacy of cyber defense strategies.

II. LITERATURE SURVEY

1.Paper Name: Cyber Attack Detection Model (CADM) Based on Machine Learning Approach
Author: Fahima Hossain, Marzana Akter and Mohammed Nasir Uddin
Abstract : A reliable Cyber Attack Detection Model (CADM) is a system that works as safeguard for the users of modern technological devices and assistant for the operators of networks. The research paper aims to develop a CADM for analyzing the network data patterns to classify cyber-attacks. CADM finds out attack wise detection accuracy using ensemble classification method. LASSO has been used to extract important features. It can work with large datasets and it has more visualization capability. Gradient Boosting and Random Forest algorithms have been used for classification of network traffic data to build an ensemble method.

2.Paper Name: A Novel Cyber-attack Detection Approach based on Kernel Extreme Learning Machine using FR-Conjugate Gradient
Author: Jun Li, Hao Jiang, Yaobing L
Abstract : Billions of devices have been developed with communication technology especially cyber technology, which provides great convenience for our lives. However, they also have produced some huge information security risks. The detection algorithm of traditional intrusion detection system (IDS) usually has a poor generalization and inefficient performance, that is to say it is not able to identify new attack types and deal with training data set with huge samples.

3.Paper Name: Streamed Incremental Learning for Cyber Attack Classification using Machine Learning
Author: Veeramanickam M.R.M, Vikas Khullar*

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211033 |

Abstract : Cyber-security is unavoidable in present days due to the security importance of each and every digital device part of a global network among millions of computing nodes. Industry 4.0 created much more impact on the automation of industrial micro functionalities to the manufacturing level, with more sensitive data to handle at every stage of organization, then security features of such platform are more important for a complete smooth working environment. This article will elaborate more on an understanding of Incremental learning with data analysis of huge Cyber-attack detection datasets which consist of Adware, Ransomware, SMS malware, scareware, Benign..etc. Incremental learning refers to a group of scalable various algorithms that as the ability to learn in terms of sequentially and can continuously update their models from huge infinite data streams. This working model helps to understand by adopting dynamic learning for varying incoming data inputs based on huge dataset inputs with scalable learning models of algorithms without discarding learned model outcomes

4.Paper Name: Load forecast anomaly detection under cyber attacks using a novel approach **Author:** Anshul Agarwal
Abstract : In order to make essential and practical choices about the demand and supply of energy, power grid operators rely on load prediction data. Consequently, effective load forecasting is critical to achieving economic benefits. Cyberattacked load prediction data may mislead power grid operators into making unwarranted choices about the distribution of electricity. This research has given a unique methodology for the detection and identification of cyber assaults on the electric grid's load prediction data. It has two stages. In the first phase, a benchmark is generated using historical real load data and an unsupervised machine learning model. The categorization of cyber threats using supervised machine learning models is the second phase. Finally, ensemble approaches are used to construct a novel hybrid model.

5.Paper Name: Intelligent Detection System for Multi-Step CyberAttack Based on Machine Learni
Author: Khattab M. Ali Alheeti, Abdulkareem Alzahrani
Abstract: Cyber-attacks involve stifling processes and activities, conciliating data, or restricting data access by carefully modifying computer systems and networks with malware. There has been a significant increase in these types of attacks over time. Due to the rise in complexity and structure, advanced defensive methods are needed. In the face of growing security threats, traditional methods of identifying cyberattacks are ineffective. In this paper, the intelligent of intrusion a detection system is suggested. Moreover, the suggested system attempts to evaluate the capability of the k-nearest neighbour's algorithm (KNN) in terms of distinguishing between authentic and tampered data. A reliable dataset named the Multi-Step Cyber-Attack Dataset (MSCAD) is utilized to determine the behavior Among the new sorts of attacks.

6.paper Name: Attack Forecast and Prediction
Author: Florian Klaus Kaisera , Tobias Budiga , Elisabeth Goebela
Abstract: Cyber-security has emerged as one of the most pressing issues for society with actors trying to use offensive capabilities and those who try to leverage on defensive capabilities to secure their assets or knowledge. However, in cyber-space attackers oftentimes have a significant first mover advantage leading to a dynamic cat and mouse game with defenders. Cyber Threat Intelligence (CTI) on past attacks bears potentials that can be used by means of predictive analytics to minimize the attackers first mover advantage. Yet, attack prediction is not an established means and automation levels are low. Within this work, we present Attack Forecast and Prediction which is based on MITRE Adversarial Tactics, Techniques and Common Knowledge (ATTCK). consists of three modules representing different analytical procedures which are clustering, time series analysis, and genetic algorithms.

7. Paper Name: Machine Learning Based Cyber Attacks Targeting on Controlled Information: A Survey
Author: YUANTIAN MIAO, CHAO CHEN
Abstract: Stealing attack against controlled information, along with the increasing number of information leakage incidents, has become an emerging cyber security threat in recent years. Due to the booming development and deployment of advanced analytics solutions, novel stealing attacks utilize machine learning (ML) algorithms to achieve high success rate and cause a lot of damage. Detecting and defending against such attacks is challenging and urgent so that governments, organizations, and individuals should attach great importance to the ML-based stealing attacks. This survey presents the recent advances in this new type of attack and corresponding countermeasures. The ML-based stealing attack is reviewed in perspectives of three categories of targeted controlled information, including controlled user activities, controlled ML model-related information, and controlled authentication information. Recent publications are summarized to generalize an overarching attack methodology and to derive the limitations and future directions of ML-based stealing attacks.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211033 |

8.Paper Name: Efficient Cyber Attack Detection in Industrial Control Systems Using Lightweight Neural Networks and PCA
Author: Moshe Kravchik and Asaf Shabtai
Abstract: A number of attack detection methods have been proposed, however they are characterized by a low detection rate, a substantial false positive rate, or are system specific. In this paper, we study an attack detection method based on simple and lightweight neural networks, namely, 1D convolutions and autoencoders. We apply these networks to both the time and frequency domains of the collected data and discuss pros and cons of each approach. We evaluate the suggested method on three popular public datasets and achieve detection rates matching or exceeding previously published detection results, while featuring small footprint, short training and detection times, and generality. We also demonstrate the effectiveness of PCA, which, given proper data preprocessing and feature selection, can provide high attack detection scores in many settings.

9.Paper Name: Cyber-attack detection in network traffic using machine learning
Author: Khalid Almulla
Abstract: Rapid shifting by government sectors and companies to provide their services and products over the internet, has immensely increased internet usage by individuals. Through extranets to network services or corporate networks used for personal purposes, computer hackers can lead to financial losses and manpower/time consumption. Therefore, it is vital to take all necessary measures to minimize losses by detecting attacks preemptively. Due to learning algorithms in cyberspace security challenges, deep learning-based cyber defense has lately become a hot topic. Penetration testing, malware categorization and identification, spam filtering, and spoofing detection are just a few of the key concerns in cyber defense that were tackled using Machine Learning (ML) approaches (Somme, 2020).

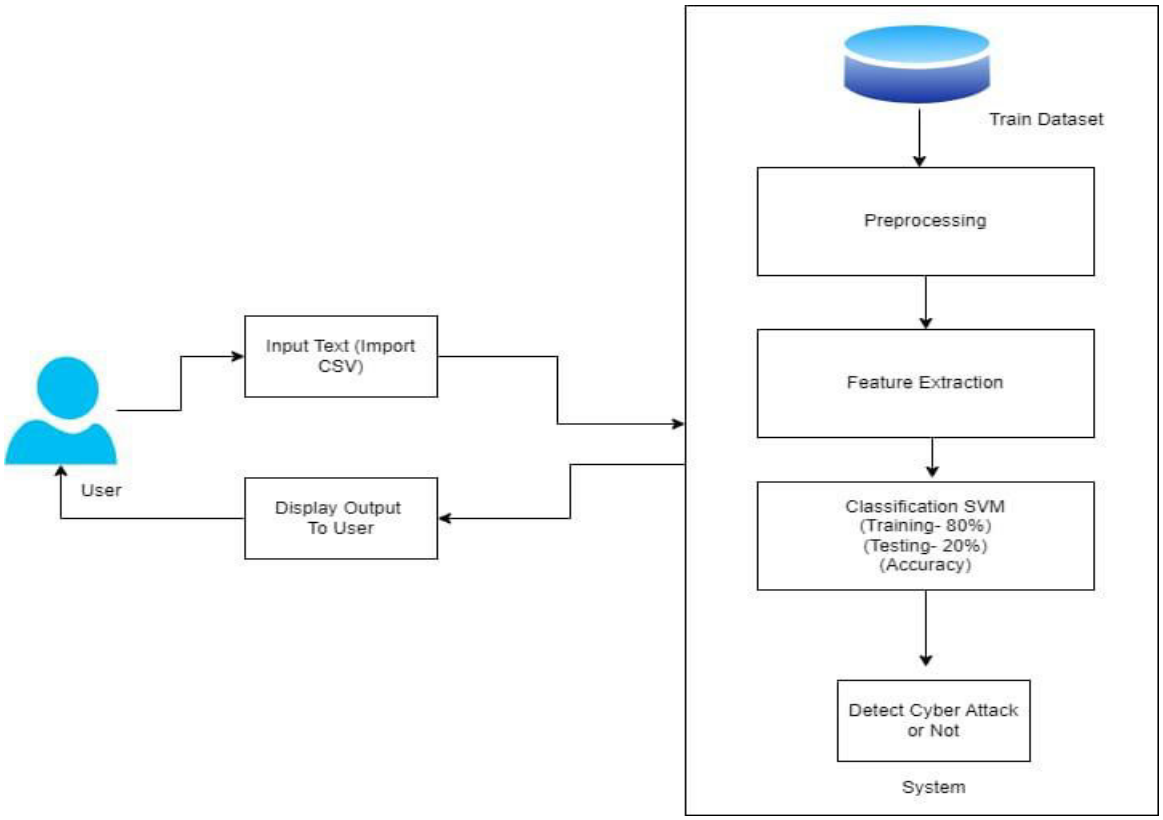
10. Paper Name: PREDICTION OF CYBER ATTACKS USING MACHINE LEARNING ALGORITHMS **Author:** S. Arumai Shiney, P.Jayasri Archana Devi
Abstract: One of the world's biggest issues nowadays is cyber-attacks. Every day, they wreak serious economic harm to both persons and nations. Cybercrime is also on the rise along with cyber-attacks. Understanding attack tactics and identifying cybercrime perpetrators are crucial in the fight against crime and criminals. Cyber-attack detection and prevention are challenging undertakings. Yet, academics have lately developed security models and made predictions using artificial intelligence techniques to solve these issues. There are many ways for predicting crimes that can be found in the literature. On the other hand, they struggle to foresee the strategies used in cybercrime and cyber-attacks. By using actual data to pinpoint an assault and its perpetrator, this issue can be solved. The information includes the kind of crime, the perpetrator's gender, the damage, and the attack techniques.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211033 |

III.SYSTEM ARCHITECTURE



- Module

• Admin

• In this module ,the Admin has to log in by using valid user name and password. After login successful he can do some operations such as View All Users and Authorize, View All E-Commerce Website and Authorize, View All Products and Reviews, View All Products Early Reviews, View All Keyword Search Details, View All Products Search Ratio, View All Keyword Search Results, View All Product Review Rank Results.

• View and Authorize Users

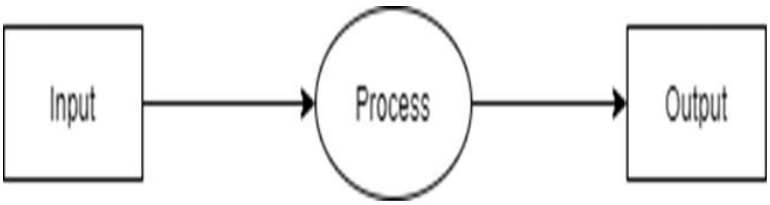
• In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

• End User

• In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will best or to the database. After registration successful, he has to login by using authorized user name and password.

Data Flow Diagram

In Data Flow Diagram ,we Show that flow of data in our system in DFD0 we show that base DFD in which rectangle present input as well as output and circle show our system, In DFD1 we show actual input and actual output of system input of our system is text or image and output is rum or detected like wise in DFD 2 we present operation of user as well as admin.

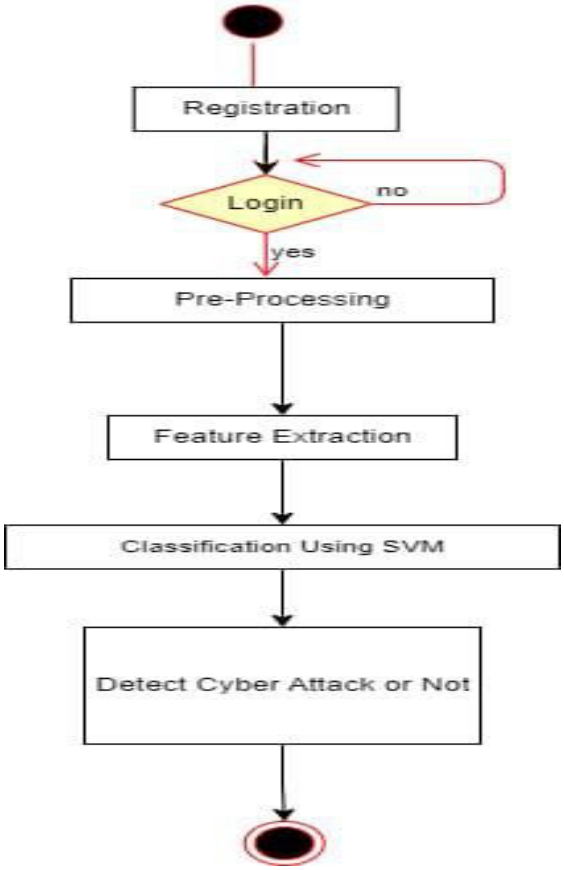


|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211033 |

Activity Diagram:



IV.CONCLUSION

In conclusion, the use of machine learning techniques in the cyber attack detection process is essential for combating an ever-evolving landscape of threats. While it offers significant advantages, it is not a silver bullet, and human expertise and continuous adaptation are equally important. Looking ahead, machine learning will continue to play a crucial role in enhancing cyber security, but it must be used in conjunction with other security measures to effectively protect digital assets. Refining anomaly detection techniques is crucial. Future work should focus on developing more sophisticated anomaly detection algorithms that can adapt to the changing nature of cyber threats. Developing advanced behavioural profiling models for users, devices, and applications will be vital. These models can help in identifying deviations from normal behavior, even in the presence of zero-day attacks. Research in adversarial machine learning is critical. As cyber attackers become more sophisticated, they can manipulate machine learning models.

REFERENCES

1 Wenye Wang, Zhou Lu, Cyber security in the Smart Grid: Survey and challenges, Computer Networks, Volume 57, Issue 5, 2013, Pages 1344-1371, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2012.12.017

2 P. Datta, S. N. Panda and S. Bajaj, ”Data Analysis of Cyber Security for Women in Haryana,” 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020, pp. 763-767, doi: 10.1109/ICRITO48877.2020.9197788.

3 R. A. Kemmerer, ”Cyber security,” 25th International Conference on Software Engineering, 2003. Proceedings., 2003, pp. 705-715, doi: 10.1109/ICSE.2003.1201257.

4 Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet 2021, 13, 39. https://doi.org/10.3390/fi13020039

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211033 |

5 Yihua Liao, V.Rao Vemuri, Use of K-Nearest Neighbor classifier for intrusion detection' in the Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, August 2002, Computers Security, Volume 21, Issue 5,2002, Pages 439-448.

6 M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things (Netherlands), vol. 7, p. 100059, 2019, doi: 10.1016/j.iot.2019.100059.

7 M. S. Bouhlel and S. Rovetta, Med Salim Bouhlel Proceedings of the 8th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications, vol. 1. 2018.

8 Mouna Jouini, Latifa Ben Arfa Rabai, Anis Ben Aissa, Classification of Security Threats in Information Systems, Procedia Computer Science, Volume 32, 2014, Pages 489-496, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2014.05.452.

9 D. Chu, L. -Z. Liao, M. K. -P. Ng and X. Wang, "Incremental Linear Discriminant Analysis: A Fast Algorithm and Comparisons," in IEEE Transactions on Neural Networks and Learning Systems, vol. 26, no. 11, pp. 2716-2735, Nov. 2015, doi: 10.1109/TNNLS.2015.2391201.

10 M.R.M. VeeraManickam, M. Mohanapriya, B.K. Pandey, et al. MapReduce framework based cluster architecture for academic student's performance prediction using cumulative dragonfly based neural network, Cluster Comput., 22 (2019), pp. 1259- 1275, 10.1007/s10586-017-1553-5

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details