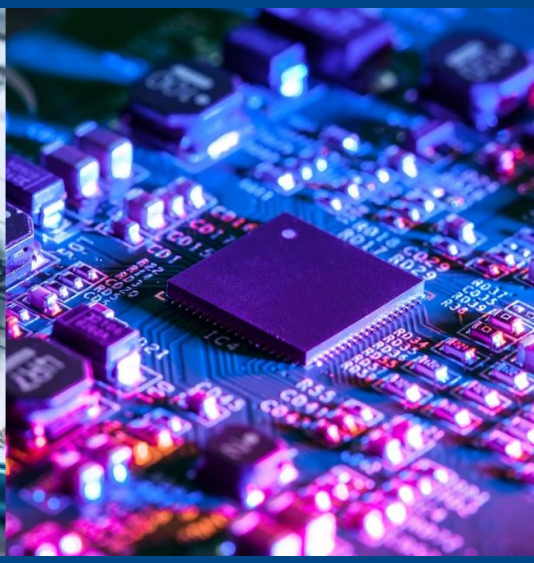
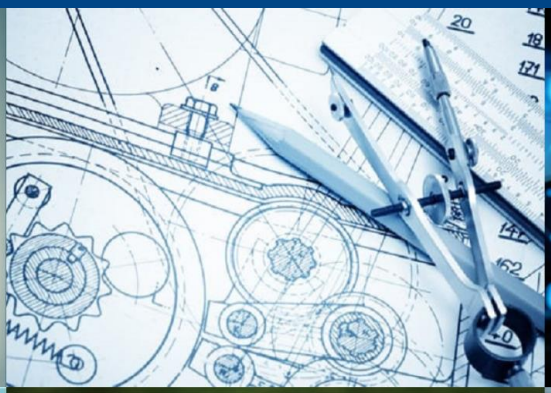
ISSN: 2582-7219

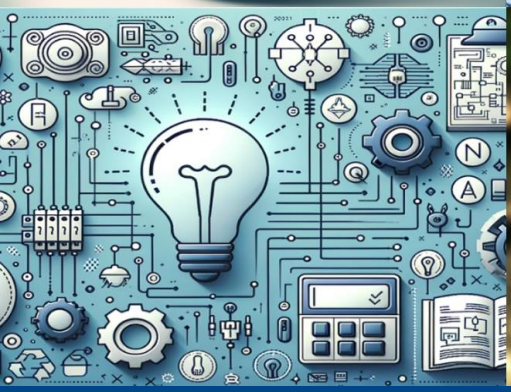




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 3, March 2025**

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803252

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Network Monitoring System to Detect Cyber Attacks using Forensic Tools and Algorithm

Dr. D.J. Samatha Naidu, K. Lakshmi Kanth

Professor, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, India

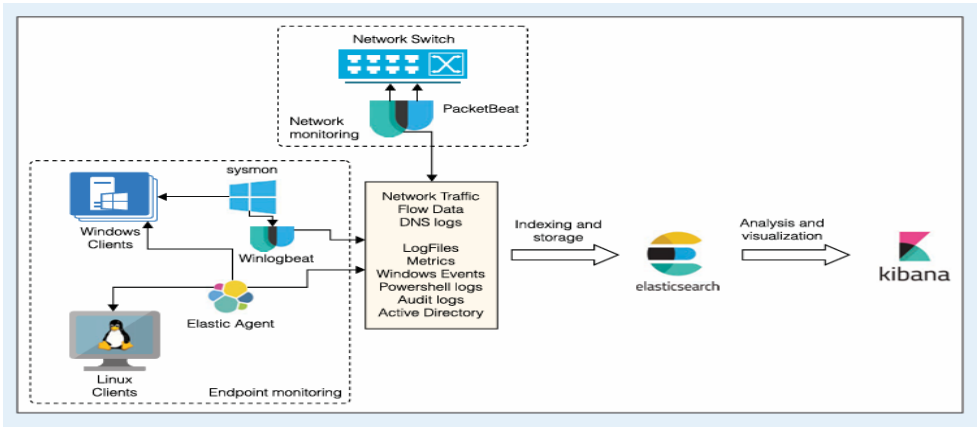
PG Student, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, India

ABSTRACT: The recent years have pushed the limits of digital transformation for organizations and institutions, occurring rapidly and at an unprecedented scale. This swift transition has led to a rise in cyber attacks and cybercrime. This paper aims to develop a system for detecting cyberattacks using data from a controlled cyber range environment. The system uses machine learning to identify patterns and anomalies in network behavior, enabling proactive detection and mitigation of cyber threats. The proposed system leverages the ELK-Stack for log collection, processing, and correlation to detect security incidents. It incorporates network and host-based measurements to provide a comprehensive view of the infrastructure. The system demonstrates effectiveness in log management and cyber incident detection.

KEYWORDS : Machine Learning, Cyber range, ELK-Stack(Elasticsearch, Logstash, Kibana) , Anomaly Detection.

I. INTRODUCTION

The digital age has transformed how organizations operate, with online platforms now essential for various activities, including banking, government services, commerce, and education. This shift towards digital transformation has occurred rapidly and at an unprecedented scale. Consequently, there has been a rise in cyberattacks and cybercrime. To address the growing threat of cyberattacks, this paper focuses on developing a system for their detection. The system leverages machine learning techniques to identify patterns and anomalies in network behavior, using data from a controlled cyber range environment. The research also emphasizes the importance of Security Information and Event Management (SIEM) systems, highlighting the use of the ELK-Stack (Elasticsearch, Logstash, and Kibana) for log collection, processing, and correlation.



ig. 1. ELK-Stack workflow for monitoring.

II.LITERATURE REVIEW

1. Introduction to Cyber Range and Its Role in Cybersecurity

A cyber range is a simulated environment designed to replicate real-world cyber threats and networks, offering a safe space for testing, training, and improving cybersecurity strategies. These environments help develop and assess various

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

defense mechanisms against cyberattacks. Cyber ranges are particularly valuable in the realm of machine learning (ML), as they offer a controlled environment where algorithms can be trained on attack data, helping to enhance their detection capabilities.

2. Cyber Attack Detection: An Overview

Detecting cyberattacks is a complex challenge due to the evolving nature of threat landscapes. Traditional defense systems rely heavily on signature-based methods, but attackers constantly evolve tactics to avoid detection. In recent years, anomaly detection and behavioral analysis using machine learning have emerged as more effective techniques to detect novel attacks. The need for continuous improvement in detecting cyber threats has led to the integration of measurement-based learning, where systems can learn from data generated in cyber range environments. Measurement learning involves using quantitative metrics derived from system behavior, traffic data, or logs to identify patterns or anomalies indicative of cyberattacks.

3. Machine Learning Approaches to Cyber Attack Detection

Several machine learning techniques have been employed to detect cyberattacks. These can be broadly classified into:

- **Supervised Learning**: Involves training a model on labeled data to identify known attacks. Algorithms like decision trees, support vector machines (SVM), and neural networks have been widely applied. These methods are effective when labeled attack data from cyber range environments are available, as they help models generalize to unseen threats.
- **Unsupervised Learning:** Often used when labeled data is sparse or unavailable. Clustering techniques such as k-means, and anomaly detection methods like autoencoders, are typically employed. Unsupervised learning algorithms can identify unknown attack patterns by detecting outliers or abnormal behavior, which is often the case in novel or zero-day attacks.
- **Reinforcement Learning:** Used for developing adaptive defense systems that learn to respond to evolving threats based on feedback from their actions. This approach is still relatively nascent but shows promise for real-time attack detection and response.

Measurement learning, particularly in unsupervised and semi-supervised paradigms, can help refine these models by feeding them with dynamic, real-world data generated within the cyber range, thus enhancing the system's ability to detect emerging threats.

4. Cyber Range Data and Measurement Techniques

Cyber ranges provide valuable data that can be leveraged for detecting cyberattacks. These data points typically include network traffic logs, system performance metrics, firewall logs, and intrusion detection system (IDS) alerts. In the context of measurement learning, the goal is to identify critical features that can serve as indicators of malicious activity. Some measurement techniques commonly used in cyber ranges include:

- **Network Traffic Analysis**: Cyber ranges simulate real network traffic, including both benign and malicious interactions. By measuring metrics like packet flow, connection patterns, and traffic volume, ML algorithms can learn to distinguish normal from abnormal behavior.
- **System Behavior Metrics**: Monitoring system behavior, such as CPU utilization, memory usage, and file access patterns, provides key insights into potential attacks like denial-of-service (DoS) or privilege escalation.
- **Anomaly-based Detection**: The cyber range generates large volumes of data, including both normal and malicious events, which can be used to train models to identify anomalous behaviors. For example, a sudden increase in traffic to a specific server or abnormal login patterns may trigger an alert.
- **Feature Engineering**: Effective feature extraction is crucial to improving model accuracy. The process involves selecting relevant metrics from the available data (e.g., packet size, protocol type, number of failed login attempts) to represent a given attack.

5. Recent Developments in Machine Learning and Cyber Range Integration

Several recent studies have highlighted the growing importance of integrating cyber range environments with machine learning techniques to improve cyberattack detection:

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **A Hybrid Machine Learning Approach**: A study by Ahmed et al. (2023) proposed combining supervised and unsupervised learning models to detect cyberattacks. They used a cyber range to generate labeled and unlabeled data, and the hybrid model outperformed traditional methods by adapting to evolving attack vectors.
- **Deep Learning for Intrusion Detection**: Deep learning models, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have shown great promise for intrusion detection. These models can process large amounts of sequential data (like network traffic over time) and identify complex attack patterns that simpler algorithms may miss. A key challenge is ensuring that these models are trained on sufficient and diverse datasets, which cyber ranges can provide.
- **Automated Attack Scenario Generation**: A key trend in recent literature is the use of cyber ranges to generate synthetic attack scenarios, which can be used to train machine learning models more effectively. For instance, generated scenarios could involve multiple types of attacks (e.g., malware, DDoS, phishing) occurring simultaneously, providing a more comprehensive dataset for the model to learn from.
- **Explainability in Machine Learning Models:** In cybersecurity, it is essential not just to detect an attack but also to understand how the model reached its conclusion. Recent research has focused on integrating explainability with detection algorithms to improve transparency and trust in ML models used in cyber range environments.

6. Challenges and Future Directions

While measurement learning from cyber ranges has shown promise in cyberattack detection, several challenges remain:

- **Data Quality and Quantity**: High-quality, labeled data is crucial for training accurate models. Cyber ranges often generate vast amounts of data, but ensuring that this data is representative of real-world attacks and is appropriately labeled can be challenging.
- **Scalability:** As cyberattacks become more sophisticated, models trained on a specific range or set of attacks may struggle to generalize to new, unseen threats. Continuous data generation and model retraining are needed to ensure detection systems stay effective.
- **Adversarial Attacks**: The rise of adversarial machine learning, where attackers intentionally craft input data to deceive models, is another significant concern. Ensuring robustness against adversarial attacks is a key area of research.
- **Integration with Existing Systems:** Deploying machine learning models in real-world systems requires integration with existing infrastructure, including security tools and incident response systems. Ensuring that models perform effectively in operational environments, not just in the controlled setting of a cyber range, remains an ongoing challenge.

III. METHODOLOGY OF PROPOSED SURVEY

Programming improvement of life cycle (SDLC) is a movement of stages that give an average understanding of the item assembling process. How the item will be perceived and made from the business understanding and necessities elicitation stage to change over these business contemplations and requirements into limits and features until its utilization and movement to achieve the business needs. The extraordinary computer developer should have adequate data on the most capable technique to pick the SDLC model considering the endeavor setting and the business requirements.

Thus, it may be normal to pick the right SDLC model as shown by the specific concerns and necessities of the endeavor to ensure its flourishing. I composed one more on the most proficient method to pick the right SDLC, it can follow this connection more data. Besides, to dive more deeply into programming life testing and SDLC stages follow the connections featured here. It will investigate the various kinds of SDLC models and the benefits and disservices of everyone and when to utilize them. That can imagine SDLC models as devices that can be used to convey product projects. Thus, knowing and seeing each model and when to utilize it, the benefits and drawbacks of everyone is essential to know which one is appropriate for the undertaking setting.

Types of Software developing life cycles (SDLC)

- Waterfall Model
- V-Shaped Model

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Evolutionary Prototyping Model
- Spiral Method (SDM)
- Iterative and Incremental Method
- Agile development

IV. CONCLUSION AND FUTURE WORK

The integration of measurement learning from cyber range environments with machine learning techniques offers a promising approach to improving cyberattack detection. Cyber ranges provide a valuable resource for generating large, diverse datasets that can be used to train machine learning models to detect both known and novel attacks. Despite challenges related to data quality, scalability, and adversarial attacks, ongoing advancements in hybrid machine learning approaches, deep learning, and model explainability are likely to improve the effectiveness of attack detection systems. The article proposes an efficient real-time deep learning based framework to automate the process of monitoring the social distancing via object detection and tracking approaches, where each individual is identified in the real-time with the 9 help of bounding boxes. The generated bounding boxes aid in identifying the clusters or groups of people satisfying the closeness property computed with the help of pairwise vectorized approach. The number of violations are confirmed by computing the number of groups formed and violation index term computed as the ratio of the number of people to the number of groups. The extensive trials were conducted with popular state-of-the-art object detection models: Faster RCNN, SSD, and YOLO v3, where YOLO v3 illustrated the efficient performance with balanced FPS and mAP score. Since this approach is highly sensitive to the spatial location of the camera, the same approach can be fine tuned to better adjust with the corresponding field of view..

REFERENCES

[1] "Global status report on road safety 2015", World Health Organization, 2019. [Online]. Available: http://www.who.int/ violence_injury _prevention /road_safety_status/20 15/en/. [Accessed: 07- Mar- 2019].

[2] Prabakar, S., et al. "An enhanced accident detection and victim status indicating system: Prototype." India Conference (INDICON), 2012 Annual IEEE. IEEE, 2012.

[3] "Lexus Enform", Lexus, 2019. [Online]. Available: https://www.lexus.com/enform. [Accessed: 07- Mar- 2019].

[4] "OnStar Safety and Security Services", Onstar.com, 2019. [Online]. Available: https://www.onstar.com/us/en/services/safety-security/. [Accessed: 07- Mar- 2019].

[5] "SOSmart automatic car crash detection and notification app", SOSmart automatic car crash detection app, 2019. [Online]. Available: http://www.sosmartapp.com. [Accessed: 07- Mar- 2019].

[6] C. Kockan, “Communication between vehicles” PhD thesis, Istanbul Technical University, 2008

[7] Zeng, Yuanyuan, Deshi Li, and Athanasios V. Vasilakos. "Opportunistic fleets for road event detection in vehicular sensor networks." Wireless Networks 22.2 (2016): 503-521.

[8] Szegedy, Christian, et al. "Rethinking the inception architecture for computer vision." Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.

[9] Szegedy, Christian, et al. "Going deeper with convolutions." Proceedings of the IEEE conference on computer vision and pattern recognition. 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com