Enhancing Cybersecurity through Machine Learning-driven Anomaly Detection Systems

By ***Dr Emily Chen, Prof. Chien-Ming, Dr Steve Lockey, Dr Hassan Khosravi & Dr Nell Baghaei***

Professor, University of Queensland, Gatton Campus, Gatton, QLD, Australia

1. Introduction to Cybersecurity and Anomaly Detection

Detecting anomalies inherent in a dataset is a critical task in many areas. Since anomalies can be attributed to defects in systems and examples of 0day attacks, discovering abnormal samples has become an important issue in a burgeoning number of domains. Although many ML algorithms produce satisfactory performance levels when labeling normal and abnormal samples is simple, if designing such a label is difficult, these models require numerous labeled samples to accomplish an accurate normal-abnormal characterization of the features inherent in a data collection.

In this work, cybersecurity is enhanced by automating the design of Machine Learning (ML) anomaly detection systems to protect the systems from never-before-seen (0day) attacks. There are two strategies that this project follows to accomplish this objective. Firstly, new strategies for expanding the usage of labels to provide more information for the designed anomaly detection system are developed by creating an innovative representation of the features. Secondly, Multiple Instance Learning (MIL) is extended to a more generalized setting called Transformation-based Multiple Instance Learning (TMMIL) for designing ML algorithms to perform well with more training data.

Cybersecurity deals with protecting systems connected to the web from attacks by hackers or terrorists. However, most existing cybersecurity techniques make use of signatures for detecting attacks. If a hacker crafts a new strike, after the hacker performs the strike, the trend of the strike is studied and signatures are then available to the general public so that the strike can be detected in the future.

2. Fundamentals of Machine Learning in Cybersecurity

In a soft human-controlled society such as military, industrial, financial, and business enterprises, the velocity at which security threats and cyberattacks are now occurring is alarming. The continuous information technology advancements, where criminal elements use the cyber domain to manifest their criminal behavior of thefts, ransom, and dimensions of national security attacks, have made the environment cautious and alerted. AI technologies and advanced cybersecurity (in a joint endeavor) offer a unique opportunity for a joint solution to improve the understanding of information and the tools to better cope with the emerging threats. Artificial intelligence (AI) methods in general and machine learning (ML) techniques in particular offer efficient tools for addressing some important challenges in cybersecurity. The first step might be to establish risk and develop a strategy for managing that risk to counter the continuous security threats. In such an environment where the risks occur in terms of data and security, the application of machine learning, being one of the general AI techniques, needs to manage uncertainties by learning the model from the data.

This introductory chapter is dedicated to the basic concept of using advanced machine learning, ML-driven algorithms and systems to enhance cybersecurity. It starts with an introductory discussion on the cybersecurity challenges and initiatives of enhancing it through advanced AI technologies, mainly machine learning. Then, the fundamentals of machine learning are discussed as these systems serve as the core engine inside ML-driven cybersecurity models for detecting cyberattacks. A brief discussion on some defense approaches which are based on a cross between AI, machine learning, and cybersecurity is presented here. Finally, the key challenges being faced by the ML-driven cyber systems are discussed.

3. Types of Anomalies in Cybersecurity

Digital systems of all types of scale and complexity in general can experience many types of abnormal behavior that deviate significantly from the normal, expected behavior. These varying types of abnormal behavior can be referred to as anomalies. We define ten main types of anomalies with respective business impact, with respect to cybersecurity. Spam, impersonation, theft of data, and corruption of the availability of services constitute some examples of detectable anomalies. Additionally, a few such as abuse of resources, insider trading, sabotage, and service discovery or process reconnaissance are generally closely linked to attacks that spearhead a compromising campaign. We had found these types of abnormal behavior, or known and expected business threats, through scientific analysis of digital forensic evidence and conversations with organizations that defended their assets from these business compromises.

In this paper, we introduce a new capability-driven framework for enhancing the performance of anomaly detection systems by the facilitated use of domain-specific training data. The elements of our solution are driven by explained domain properties that are used to define the limits for the design and deployment of anomaly detection solutions.

Cybersecurity has been an active research area for privacy and reliability concerns in big data management. Such concerns have been extended to machine learning (ML) and deep learning (DL) systems that are used in anomaly detection and threat intelligence. One main challenge is the ability of ML and DL models to interpret data and accurately provide normal/abnormal behavior in different domains. To date, there has been little attention paid to the performance of ML/DL systems in arid environments or under unreliable data sets to make them operational safely and securely.

4. Challenges in Traditional Anomaly Detection Systems

Traditionally, anomaly detection systems have primarily adopted rule-based systems, which handcraft rules that can classify observed data as normal or abnormal. While such traditional methods have proven to be effective in certain domains, they show limitations for network traffic data, which is generally high-dimensional and contains complex interconnections between different features. Furthermore, intrusion detection systems which rely on single-class classification models such as the one-class support vector machine, which only flags problems from a known class, may not capture the changing behaviors of threats as they evolve over time. Currently, available networks often handle diverse types of applications, resulting in complex data interactions and making the detection of abnormalities especially challenging. As a result, intrusion detection systems should not be effective solely on known classes of problems, but should also be able to detect network abnormalities that propagate over time. This motivates the need for a more sophisticated or robust one-class classifier, which can easily capture the most complex one-class problems posed by evolving network phenomena.

Anomaly detection systems play a critical role in monitoring and identifying breaches or cyberattacks in enterprises. Failure to react to the signs of these breaches exposes organizations to many insecurities, including loss of control over their network infrastructure, substantial data loss, data theft, fraud, privacy violations, and a tarnished organizational reputation. Therefore, enterprises require strong and reliable security measures in place to detect and rapidly eliminate such online threats. The presence of reliable security mechanisms will not only prevent financial loss and negative implications on their hard-earned reputation, but also ensure clients that their information is stored securely and safely, thereby increasing the customers' trust in the organizations. However, creating effective security mechanisms for enterprise network systems can be quite challenging, especially for detecting abnormal activities that are not intrinsically straightforward to capture and classify. The growing complexity and sophistication of cyberattacks also make their detection increasingly difficult.

5. The Role of Machine Learning in Enhancing Anomaly Detection

Machine learning algorithms, in general, can be broadly classified into several types, such as supervised, unsupervised, semi-supervised, and reinforcement learning. An unsupervised learning framework in which algorithms learn to group pieces of information that are similar to each other is particularly well-suited to the task of anomaly detection. There are, however, several challenges associated with applying machine learning to detect anomalies and cybersecurity-related events. In order to develop a successful machine-learning model for anomaly detection, the user will have to perform a multi-step process. First, considerable effort has to be expended to collect, clean, and prepare the input data. Second, the model must be trained and validated using the input data in conjunction with a set of labels that accurately identify anomaly or event type. Finally, the model's performance in detecting previously unseen anomalies must be regularly monitored and reassessed over time.

Anomaly detection leverages machine learning, a branch of artificial intelligence, to learn and identify the behaviors in a system, service, network, or process that deviate from established norms. The detection of such anomalies, which may suggest the presence of malware or a cyber-attack, or indicate system compromise or compliance violations, is achieved through the analysis of various types of data. In today's increasingly connected digital ecosystem, anomaly detection is a critical aspect of cybersecurity risk mitigation. As government agencies, private sector companies and organizations, and critical infrastructures that form the backbone of our economy, continue to accelerate their digital transformation, the integration of machine learning into their information and communication technology (ICT) systems can create unique business advantages.

6. Supervised Learning Approaches for Anomaly Detection

In the context of network communications and configuration files, potential contributors have begun to explore machine-learning methods. It is important to emphasize that the fundamentals of these techniques have existed for decades, but could not be axiomatically put into use until recently. List 3.1 presents a number of relevant machine learning techniques with rudimental contemplation for anomaly detection. Fuzzy logic, Bayesian networks, decision trees, neural networks, support vector machines (SVM), and clustering form the list of the most employed methods. Over the next few sections, cloud environment anomaly identification using machine learning approaches such as SVM, one-class SVM, and clustering are thoroughly discussed in the context of past research. The research by Menaga et al. (2022) incorporates a hybrid strategy for extracting and classifying domain feature-level opinions, as explained in their multi-stage process.

Consequently, anomaly detection in unsupervised settings is avoided to avert model drift. However, until all potential anomalies are unearthed, the precise validation of the system is unapproachable. Supervised techniques, because they are crafted to deal with particular anomalies, execute better than unsupervised methods. Nevertheless, there must be an amount of labeled data in order to utilize the supervised methods. This is a handicap for deploying supervised techniques. Without the labeled data for specified anomalies, a manual process must be used to label the anomalies which slows down the system's update process. Perhaps the two most common anomaly detection systems are SVM and one-class SVM. The one-class SVM is widely used because it reconfigures the SVM for anomaly detection without requiring labeled normal data for assistance. Rather than matching data with a hyperplane, this method executes a structural search for data points and determines whether they fall inside a trained hypersphere covering the set of normal data points. If a data point gets misplaced outside the hypersphere, it is determined to be an anomaly.

7. Unsupervised Learning Approaches for Anomaly Detection

When using unsupervised learning, the tradeoff between false positives and false negatives is set by the threshold. A higher threshold (setting for a more stringent requirement for the input to pass as regular, e.g. more than 5 standard errors from the mean) results in more false negatives, thus making it harder for legitimate intruder actions to pass as normal behavior, but runs the risk of high false positives as legitimate user behaviors may be identified as anomalies. Sometimes, models are combined with supervised or rule-based logic to better specify the types of actions that are considered anomalous. With such models, the threshold becomes less sensitive because the supervised section helps refine the model to specify the types of anomalous activities for which the model was not originally trained to detect. Such clustering approaches, similar to semi-supervised learning, leverage both the density estimation-like nature of unsupervised learning combined with the error correction capabilities of supervised learning. The supervised section is used to correct the cluster assignments from the unsupervised approach while boosting the confidence of both normal or anomalous assignments that may result from the unsupervised model.

Unsupervised learning describes models that use inputs that do not have a corresponding output like classification or regression; instead, these models expect the input data to have a certain pattern or regularities like clustering or density estimation. This makes unsupervised learning ideal for anomaly detection tasks in cybersecurity because they are not dependent on labeled data. It is the primary approach used to detect the bulk of the anomalies in these operating systems. We group unsupervised models used for anomaly detection into the probability-based, distances-based, and reconstruction-error based groups of anomaly detection solutions. Most of these methods use Mahalanobis distance, which works well for a large volume of high-dimensional data. Density estimation is used to solve anomaly detection using modeling.

8. Semi-Supervised Learning Approaches for Anomaly Detection

The major advances in the state of the art for anomaly detection are obtained by leveraging some slight degree of supervision. This chapter demonstrates a trend from completely to semi-supervised methods for anomaly detection, even up to supervised learning too, in order to make better use of the increasingly complex resources available for building expert systems. We present the main theoretical frameworks that lie in between supervised and unsupervised learning, and include examples of widely used algorithms that are part of these frameworks. While part of this chapter is dedicated to category-bridging techniques that use features derived from the low-dimensional embedding of crowdsourced theorems according to the brain, the main contribution of the chapter is the discussion of four semi-supervised learning frameworks that offer a natural combination of the benefits of unsupervised and supervised learning.

In the previous sections, we have examined several issues in unsupervised detection and proposed new algorithms to solve these problems. Our discussion is based on information already available in labeled and unlabeled data. However, in many realistic scenarios, the amount of labeled data available is often expensive to obtain or extremely small. Moreover, the cost related to the labeling process can be prohibitively high in terms of both time and resources. Even for traditional supervised learning settings, labeled data often does not generalize well to future data or remains insufficient for detecting fine-grained attacks. For instance, an attack is a zero-day threat, which is known as new and advanced attacks for which no signature is available. Similarly, an attack may exhibit symptoms or soft signatures that only become recognizable after the attack has spread for some time.

9. Hybrid Learning Approaches for Anomaly Detection

Several other studies have not considered any interactions among various threads. Although there are no collaboration approaches among tasks in such studies, the best training model supported by the model and task's performance outcome was chosen during training. Even though the design of these hybrid learning approaches can be extensively diverse, few novel interactions are observed among subtasks in applicative models. Nonetheless, most of these hybrid learning approaches demonstrate encouraging results in detecting network-based and host-based attacks using public datasets.

Hybrid learning approaches have also been proposed in the multi-model deep learning architecture termed DeepSupport. In this architecture, more traditional machine learning is trained to detect the anomalous SYN and ACK segments, while deep learning models are trained to detect anomalous RST segments. One symbolic model, NSN, and one deep learning architecture, sub-based Deep Neural Network (DNN), were also combined with sub-models embedded in the detection mechanism to enhance detection performance. Hybrid learning-based frameworks, named ANODE, have also been proposed with relatively effective self-ensemble mechanisms where symbolic models and the deep model detect network-based and host-based attack types. In the hybrid model, all threads emanate from the same task and combine at the end to create a new submodel. After the end of the process, the most appropriate choices should be identified. However, only the best sensitive submodel from the combination approach is utilized in the inference stage (inertia on the same experimental set). Experience has demonstrated the existence of compatibility among various threads; thus, the longest initial relationship among threads was applied as the final tie.

10. Deep Learning Techniques for Anomaly Detection

Deep learning is a sub-field of machine learning using neural networks comprising a multi-level hierarchy. The behavior derived from highly abstract representations of raw data has applications in many problem domains such as natural language processing, robotics, social network filtering, search engines, and so forth. Deep learning is being increasingly used for cybersecurity tasks such as malware detection, malware analysis, phishing detection, and so forth. The reason is that deep learning algorithms are continually evolving such that they can now process diverse types of data, including unstructured data, generating meaningful features, and constantly enhancing the various symbolic and subsymbolic representations learned in different types of tasks.

Deep learning techniques have become increasingly prevalent for both network and endpoint anomalies. This chapter reviews deep learning approaches such as autoencoders, recursive neural networks, convolutional neural networks, deep belief networks, denoising autoencoders, and recurrent neural networks. Their applications to different types of data such as binary data, textual data, numerical data, and sensor data are discussed. Finally, the chapter concludes with a discussion on different metrics employed in deep learning for enabling a progressive improvement in anomaly detection.

11. Evaluation Metrics for Anomaly Detection Systems

This is the most straightforward definition of discriminating between two overlapping classes with a kernel function. In anomaly detection, the task is to decide where the decision boundary should be. If the user does not cache the output of the anomaly detection process, then an (unsupervised) method must be used to establish a threshold. The erroneous decisions that are produced by any learning algorithm, which is used to design a controller in cybersecurity, may cause a system to go out of control or that may compromise the physical integrity of the system. The most common example of an incorrect decision is a false alarm, in which the algorithm labels a non-forged signature as a forged one. The entire idea behind designing a CDHO is to find good features to get a good separation in a linear PCP.

Almost all anomaly detection algorithms require a decision threshold above which to classify examples as anomalies. The decision threshold regulates the number of false alarms and misses. Its value depends on the rule's characteristics, the cost of false detection, and the cost of missing discernible change. Under such settings, the criterion for optimizing class assignments in an anomaly detection system is: 1. Minimize the false alarms, i.e., normal instances labeled as anomalies. 2. Minimize the misses, i.e., anomaly instances labeled as normal.

12. Real-world Applications of Machine Learning-driven Anomaly Detection

We presented an updated list of real-world applications of machine learning-driven anomaly detection in enterprise environments and correspondingly added new components as highlighted. Particularly, our recent deployment of independent anomaly detection systems has inspired us to contribute back to the community with a unified model, which equips with the capability in the following applications. They are collectively few steps towards generational and operationalized anomaly detection continuing from the past. Innovative notions behind the development of new anomaly detection systems are largely based on accumulated data mining expertise, security-rich enterprise information systems as data sources, and the feasibility of participating in viable projects. We recognize that the lessons which are learned from the development of lightweight cyberinfrastructure and cheap and quick computational resources could not be traded for breakthroughs made by testing early empirical observations in real-world applications. We would welcome feedbacks which might inspire us to revisit our ideas at the right places and moments for one to produce lasting dividends.

The success of the anomaly detection research in the academic space has started to see real-world applications in enterprise environments. In this chapter, we will share detailed accounts of a number of applications of machine learning-driven anomaly detection in the information security domain. These use cases range from detection of general security and perceived security anomalies derived from the textual and graphical representation of the security logs, to modeling and detection of network-scanning anomalies/signatures, to modeling and detection of unauthorized activities and personalities exploiting the cyberinfrastructure, to discovering regular occurrences of events demand the best with the help of machine learning-driven data mining algorithms, and to identifying racy email threads using reputation-derived doppelgangers. The anomaly detection systems resulted from the application of machine learning algorithms can be used in real-world security surveillance systems to monitor and to protect the cyber infrastructures effectively.

13. Case Studies in Cybersecurity using Machine Learning

Mobile apps are picking up popularity in app stores majority of which target smartphones and tablets that are powered by the Android operating system. The widespread use and mushrooming growth of the Android application (app) market are, unfortunately, beginning to attract cybercriminals. Malware writers are using app market as a backdrop for spreading their malicious software or malapps. Providing a mild annoyance at one end of the scale to exploitation aimed at frustrating the competitors at another, malapps cover a wide spectrum of mischief. With the malapp authors employing advanced malware delivery techniques and malware obfuscation mechanisms; not surprisingly, the numbers of Android malware continue to rise. The salient question becomes: How to filter malapps (or, identify benign apps) during the app review process? More generally, the question reduces to distinguishing benign behavior from malicious (or, non-benign) behavior. There are two significant observations about the app market predicated on the answer to the question.

This chapter presents two case studies that address specific cybersecurity objectives using machine learning. Section 13.1 addresses automated and optimized filtering of Android apps. Techniques developed here enable smartphone owners to fine-tune app stores and keep malware apps from being installed. Central to the experiments in Section 13.1 is the problem of the flexibility of relevant machine learning method. Section 13.2 exploits the flexibility feature of machine learning to fuse security information present in both text and semantics of web documents. The system through the combination of machine learning, malware fingerprints and semantics provides layers of defense beyond the system using the machine learning only.

14. Ethical and Privacy Considerations in Anomaly Detection Systems

Despite being analyzed from several points of view, very few researches underline the great challenge that the characteristics of machine learning-driven anomaly detection systems pose for patent systems. In the following section, we underline the main ethical and privacy issues current in all anomaly detection systems. However, this general part is not exhaustive, so the topics it does not contain of the general ethical and privacy implications can be reflected in the machine learning-driven ones as well. Then, we identify some valid ethical bases for regulating qualitative anomaly detection systems. We suggest as a premise that some categories of humans and entities are deserving legitimate interests including discriminatory actions against anomalies. Finally, we sketch the main features of a patent system capable of ensuring that these ethical premises are fulfilled, where the unfavorable ethical consequences are avoided, where the legitimate social moral values, and where the cooperation in knowledge flows flourishes.

This paper has two main objectives: one is to provide a scientific background and an introductory guideline for professionals who aim to solve cybersecurity problems related to high volumes of data through machine learning technologies, and two is to suggest to different actors working in the field of patent law some legal and political actions which would encourage and enhance research in this discipline, and cultural exchanges, industrial flows, and transparent commercialization. As in any technological development, anomalies have been perceived as both a problem and an opportunity which poses a risk and a potential advantage for security and law enforcement, and these counteracting perceptions might originate tense social debates around the characteristics and effects as well as the appropriate way to govern their coding and creating process.

15. Future Trends and Directions in Machine Learning-driven Anomaly Detection

With the significant criticality of the resultant security functions provided by anomalies in the routinely vast sets of data collected from systems, the decision-making process can be computationally complex within the communication network or framework. Additionally, the potential inclusion of additional information to the data can also introduce privacy challenges into the security task. The aggregated data composed of individual data items may be privacy-sensitive. Recently, ML has shown itself to be a powerful tool in data-rich environments, meaning that such data-driven mechanisms are now revealing themselves to be potentially very useful for AD systems. Consequently, ML-driven AD has the potential to assure the trustworthiness of such systems by improving the insight of what is normal, anomalous, novel, surprising, and of value within a community.

15.1 Security and Privacy in ML-driven Anomaly Detection

Machine learning (ML)-driven AD systems are an essential building block for acquiring Intrusion Detection Systems (IDS). The inherent benefits of ML, including automatic learning and feature extraction, make computing highly complex detection models feasible. Moreover, the accuracy and precision capabilities of ML-driven AD systems suggest much-improved surveillance techniques that are required to monitor the increasing size of modern communication networks. Nonetheless, due to the intrinsic complexity of these security capabilities, as well as the varying resource properties, environments, and dynamics that characterize these communication networks, a range of significant challenges and potential solutions exist explicitly for using ML techniques in AD systems. To conclude, this chapter provides a brief overview of the forthcoming study.

16. Conclusion and Key Takeaways

In some ways, the other critical infrastructures are more scattered, diverse, and disparate than the energy markets. Those differences may protect other critical sectors from the widespread attack, especially those who do not employ the interconnectedness in the same way as the electric grid does. Please keep in mind this is my opinion. The forthcoming sections are divided into the development of Machine Learning (ML), the development of Anomaly Detection for the energy sector, and a description of how the new technology can protect the energy grid. This research analyzes changes in the electric power market that have occurred as a result of information technology in the last 30 years. That analysis of the electric power market, coupled with information obtained from previous cyberattacks, led to the conclusion that the electric power market is presently the most vulnerable of all critical infrastructures to cyber-related attacks. The analysis advances proposals that the power market can reconfigure its electronic security position to address the current level of vulnerability.

The specter of cyber-related attacks on critical infrastructure causes consternation across both public and private sectors. Both bear the responsibility to prevent and mitigate the effect of cyberattacks on critical infrastructure. This research examines five cybersecurity incidents related to attacks on critical infrastructure focusing on the energy sector. Whether it's loss of power or money, the damage from cyberattacks affects everything in our modernized world. This world is connected in ways unthought-of twenty years ago. All potential players in the energy markets need to have a good understanding of their vulnerabilities and should be reacting to potential threats.

17. References

1. M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 19-31, Jan. 2016.
2. C. Yin, Y. Zhu, S. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954-21961, 2017.
3. T. Zhang, J. Song, and G. Chen, "A deep learning approach for network intrusion detection based on NSL-KDD dataset," IEEE Access, vol. 7, pp. 182458-182472, 2019.
4. S. Mohammadi, S. S. Asadi, and S. Shamsuddin, "An intrusion detection system based on deep learning algorithms and a multiscale convolutional neural network," IEEE Access, vol. 8, pp. 166876-166890, 2020.

5. X. Luo, E. W. W. Chan, and R. W. S. Ko, "A deep reinforcement learning-based anomaly detection framework for cyber-physical systems," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 4937-4946, Jun. 2020.
6. R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying deep learning approaches for network traffic analysis and intrusion detection," Advances in Intelligent Systems and Computing, vol. 728, pp. 113-126, 2018.
7. A. Shone, D. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. 2018.
8. S. Wang, Y. Zhang, and Y. Wang, "A novel unsupervised anomaly detection approach for internet of things networks," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8734-8743, Oct. 2019.
9. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303-336, 1st Quart. 2014.
10. X. Du, and F. Lin, "A novel anomaly detection method based on principle component analysis in cloud computing," IEEE Access, vol. 7, pp. 27473-27481, 2019.
11. Z. Xiao, S. Guo, W. Liang, and H. L. Wang, "Malware detection and traffic classification using CNN," IEEE Access, vol. 8, pp. 84001-84011, 2020.
12. N. Moustafa, and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," 2015 Military Communications and Information Systems Conference (MilCIS), pp. 1-6, 2015.
13. S. M. H. Bamakan, H. Wang, Y. Shi, and Y. Xia, "An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization," Neurocomputing, vol. 199, pp. 90-102, Jul. 2016.
14. Pulimamidi, Rahul. "To enhance customer (or patient) experience based on IoT analytical study through technology (IT) transformation for E-healthcare." *Measurement: Sensors* (2024): 101087.
15. Pargaonkar, Shravan. "The Crucial Role of Inspection in Software Quality Assurance." *Journal of Science & Technology* 2.1 (2021): 70-77.
16. Menaga, D., Loknath Sai Ambati, and Giridhar Reddy Bojja. "Optimal trained long short-term memory for opinion mining: a hybrid semantic knowledgebase approach." *International Journal of Intelligent Robotics and Applications* 7.1 (2023): 119-133.
17. Singh, Amarjeet, and Alok Aggarwal. "Securing Microservices using OKTA in Cloud Environment: Implementation Strategies and Best Practices." *Journal of Science & Technology* 4.1 (2023): 11-39.

18. Singh, Vinay, et al. "Improving Business Deliveries for Micro-services-based Systems using CI/CD and Jenkins." *Journal of Mines, Metals & Fuels* 71.4 (2023).
19. Reddy, Surendranadha Reddy Byrapu. "Big Data Analytics-Unleashing Insights through Advanced AI Techniques." *Journal of Artificial Intelligence Research and Applications* 1.1 (2021): 1-10.
20. Raparthi, Mohan, et al. "Data Science in Healthcare Leveraging AI for Predictive Analytics and Personalized Patient Care." *Journal of AI in Healthcare and Medicine* 2.2 (2022): 1-11.