Kuwait Journal of Advanced Computer Technology
ISSN: 2984-7907
Vol. 2 No. 1 (2024)

Utilizing Deep Learning Techniques for Effective Zero-Day Attack Detection

Saurabh Kansal

Independent Researcher, USA.

Abstract: Zero-day attacks take use of undiscovered flaws to evade detection by cybersecurity detection systems. According to the findings, zero-day attacks are prevalent and pose a serious risk to computer security. Zero-day attacks are difficult to detect using the conventional signature-based detection approach since their signatures are usually not accessible in advance. Because machine learning (ML)-based detection techniques can capture the statistical features of assaults, they hold promise for the detection of zero-day attacks. This survey study presents a thorough analysis of ML-based methods for detecting zero-day attacks, comparing their ML models, training and testing data sets, and assessment outcomes. Test data samples are assumed to be drawn from pre-observed classes that were utilized in the training phase using the usual ML assessment process. In applications like Network Intrusion Detection Systems (NIDSs), it might be difficult to gather data samples of every attack type that has to be monitored. Because they were non-existent at the time, zero-day attacks—a novel kind of attack traffic that ML-based NIDSs encounter—are not utilized in training. Consequently, this study suggests a new zero-shot learning approach to assess how well ML-based NIDSs identify zero-day attack scenarios. In order to differentiate between known assaults and benign behaviour, the learning models in the attribute learning step translate network data characteristics to semantic attributes. The models build connections between known and zero-day attacks during the inference step in order to identify them as malicious. Zero-day Detection Rate (Z-DR), a new assessment metric, is created to assess how well the learning model detects unknown assaults. Two important machine learning models and two contemporary NIDS data sets are used to assess the suggested framework. The findings show that ML-based NIDSs are not able to identify certain zero-day attack groups identified in this study as hostile. Subsequent investigation reveals that assaults with a low Z-DR have a greater Wasserstein Distance range and a substantially different feature distribution than the other attack classes.

Keywords: - Zero-Day Attacks, Network Intrusion Detection Systems (NIDSs), Wasserstein Distance Range, Machine Learning (ML), Attack Classes, Training, Statistical Characteristics, Applications.

I. Introduction

By 2025, it is anticipated that the amount of data generated by IoT networks would have grown to 79.4 zettabytes (ZB). Since cloud computing, every IoT device sends its data to a central server on the cloud, where it may be aggregated and subjected to various pre-processing and analysis operations. Accordingly, the Centralized Deep Learning (CDL) approach has been widely suggested for network-based botnet attack detection in massive IoT network traffic data with strong classification performance [1, 2].

A Deep Reinforcement Learning (DRL) technique that can stop hostile strikes. Additionally, the Wireless Sensor Network (WSN) uses the Lightweight Dynamic Auto encoder Network (LDAN) technique to detect network intrusions in devices with little resources [1, 2]. In earlier research, we put forward several Deep Learning (DL) techniques [2, 3] that are capable of processing vast amounts of network traffic data in order to defend communication networks from cyberattacks. But contemporary IoT networks are rapidly growing in scalability. Consequently, it could be challenging to offload large amounts of dispersed IoT network traffic data to a distant central cloud server for data processing in practical use cases because of network limitations. Additionally, [3], the CDL technique requires more memory space for data storage, [3, 4], has a high communication overhead, and takes longer to train. Additionally, cloud data centers are often situated distant from the locations of IoT devices. Because of this, the CDL-based botnet detection approach has a large latency.

An intrusion detection system, or IDS, is one of the primary defences against online attacks. Traditional intrusion detection systems employ attack signatures [4], while more current systems use machine learning techniques. Intrusion detection systems have been in use for a long time. Extracting an attack's signature is a difficult and

time-consuming task [4, 5]. Furthermore, these techniques only apply to assaults that have previously been identified and examined; they are susceptible to fresh attacks that have never been identified before. Newer IDSes don't need signatures [5]. These IDSs use machine learning (ML) techniques, particularly deep learning techniques, to identify threats. With regard to the flow contents, the authors have created an IDS system based on deep learning that can categorize various assaults and benign traffic flows [5–6].

In the realm of intrusion detection, there are statistical and machine learning-based anomaly detectors; nonetheless, their primary objective is to differentiate between legitimate traffic and malicious activity [5, 6]. The attack type of the malicious traffic cannot thus be identified as a relevant detection report. These detectors' incapacity to discern novel benign traffic behaviours that is included in the unknowns is another flaw [6, 7]. A significant obstacle for conventional machine learning-based anomaly detectors, which rely on conventional clustering techniques, is the enormous dimensionality of network flow material. Deep learning-based models are used in intrusion detectors primarily because of the large dimensionality of the input [7].

This research is unusual in that it suggests a deep learning-based paradigm for intrusion detection adaptation to zero-day assaults. The framework's goal is to report the specific attack type of malicious traffic while taking into account novel assaults and novel benign flow behaviours. The unknown samples are grouped based on the appropriate new categories [7, 8]. The system then uses the newly named classes to update itself once an expert labels these clusters. Over time, the framework may be updated thanks to this procedure [7, 8]. To the best of our knowledge, this research is the first for network security to leverage open set recognition in deep learning-based intrusion classifiers [8, 9]. In addition, deep learning-based classifiers are integrated with the conventional clustering approach to collect further evidence of the new assault during the analysis and updating stages [8, 9]. For the first time, this clustering and classification combination is used to intrusion detection [9, 10].

1.1 Intrusion Detection Systems Based on Machine Learning

There are two types of machine learning-based intrusion detection systems: deep learning-based and conventional. Finally, we examine several primary research papers on ML-based IDSes using classical models. Research uses the SVM, the most well-known classical classifying technique. However, for unsupervised applications, the k-nearest neighbour's (KNN) technique is often used [8]. The key component of an IDS is the KNN algorithm [8, 9]. Random forests (RF) are a powerful technique that can handle uneven data and is resistant to overfitting. They have been employed in works such as the ML-Based IDS [10].

1.2 Novelty-Based Detectors

Regarding intrusion detection systems, one of the main issues is zero-day attacks. The primary flaw in conventional signature-based intrusion detection systems is these assaults [11]. Since the old method relies on known attacks to extract signatures, it is susceptible to zero-day attacks that occur for the first time. The learning-based IDSes have this problem as well. Zero-day attack detection is a kind of open set recognition novelty detection in learning-based models. The two primary categories of learning-based detectors are anomaly-based learning and classification-based learning [12]. Learning models based on anomalies may identify anomalous traffic. However, identifying and reporting discovered assaults is their primary shortcoming. Conversely, classification-based models are susceptible to zero-day attacks, much as signature-based detectors, but they are able to disclose the subcategory of known attacks [13]. Covering the shortcomings of the aforementioned learning-based models is the goal of this article. The categorization of known and unknown (i.e., zero-day) attacks is reported concurrently [14].

One of the primary research avenues for identifying zero-day attacks is the detection of outliers, or instances or occurrences that differ from normal traffic. However, due to their large false-positive and false-negative rates, the present outlier-based detection approaches have a major flaw in their very poor accuracy rates [15]. As was said, the system is exposed to attack because to the high false-negative rates, and cyber security operation centers waste time due to the high false-positive rates; in fact, only 28% of incursions that are probed are genuine [16]. False-negative results might limit the development of IDSs; for instance, they decrease their efficacy [13, 16].

Internet of Things (IoT) network zero-day attack detection framework. For detection, a distributed diagnostic system is used. Zero-day attack pathways may be found using a Bayesian probability model. In order to detect

assaults, the authors presented a prototype and visualized attacks in a structure resembling a graph. Used the CIC-AWS-2018 dataset to assess six distinct supervised machine learning approaches. Decision trees, random forests, k-nearest neighbour's, multilayer perceptron's, quadratic discriminant analysis, and Gaussian naïve Bayes classifiers are among the methods the author's use [16, 17]. How these supervised machine learning approaches are taught on benign traffic only to be used for the detection of unknown assaults and how zero-day (previously undetected) attacks are simulated and identified are not properly explained by the authors. Transfer learning is also used to identify zero-day attacks. Using transfer learning, one may map the relationship between known and unknown assaults. Using dative transfer learning, Deep Tran can identify zero-day exploits [17].

Moreover, zero-day malware detection is addressed by ML. To identify zero-day malware, for instance, the efficacy of several machine learning methods (ML) such as Support Vector Machine (SVM), Naïve Bayes, Multi-Layer Perceptron, Decision trees, k-Nearest Neighbour, [19], and Random Forests is examined, while the Deep-Convolutional Generative Adversarial Network (DCGAN) is used [19].

Using Deep Learning (DL) to discover outliers for zero-day attacks with strong recall is what we suggest doing in this study [20]. The primary objective is to develop a lightweight intrusion detection model with a high recall (true-positive rate) and low fallout (false-positive rate) that can identify fresh (unknown) intrusions and zero-day assaults. The complexity and problems that come with new assaults will thus be lessened with a strong detection capacity of zero-day attacks [19, 20].

The two main categories into which cyberattack detection systems are traditionally divided are anomaly-based detection systems and signature-based detection systems. Static signatures, also known as fingerprints, are preconfigured in signature-based systems and reflect known threats [19, 20]. By comparing the incoming signature with an attack signature that is already in the repository, the detection is accomplished. The anomaly detection techniques, on the other hand, have a concept of typical activity and identify departures from that profile [20, 23]. Both strategies have been well researched. The effectiveness of signature-based detection systems in identifying known threats with high detection accuracy and recall has actually been shown by their successful deployment in operational contexts. Since the signatures for zero-day attacks are usually not accessible in the repository, it is costly to maintain the signature library current, and signature-based detection is vulnerable to Miss Zero-day attacks with a startlingly low recall [20, 23].

The identification of zero-day threats is one of the main and continuous difficulties in using signature-based NIDSs to secure computer networks. An unprecedented danger that aims to compromise or interfere with network communications is known as a zero-day assault. Unknown to security managers, hackers may take advantage of this vulnerability before it is fixed [20, 23]. As an example, consider the June 2019 discovery of a zero-day vulnerability in Microsoft Windows that specifically targeted local escalation privileges [23]. When a zero-day attack is found, it is often documented with a CVE number and a severity level and published to the publicly accessible Common Vulnerabilities and Exposures (CVE) list. In order to identify zero-day attacks from a network layer standpoint, threat-related IOCs are often added to a list of detection databases that signature-based NIDSs employ [20, 23]. Simply because the whole collection of IOCs has not been identified or registered for monitoring at the time of exploitation, signature-based NIDSs are thus considered unreliable in identifying zero-day attacks [22, 23].

The performance of ML-based NIDSs in identifying zero-day attack scenarios is assessed using a novel ZSL framework proposed in this study [23]. A collection of semantic features learned from seen assaults is used by the framework to assess how effectively an ML-based NIDS can identify undiscovered attacks. The suggested ZSL arrangement is divided into two major phases. During the attribute learning phase, the models identify and associate the distinctive characteristics of known assaults (seen classes) with the network data properties. During the inference stage, the model links observed and zero-day (unseen) assaults to help identify and categorize them as malicious [24]. During the setup, the training and testing sets that comprise the visible and unseen classes stay apart. The suggested setup, in contrast to conventional evaluation techniques, uses a novel measure called Zero-day Detection Rate (Z-DR) to assess how well ML-based NIDS detect zero-day threats [26].

II. Related Works

(Tawalbeh, L. A. 2023) The scientific community has been more interested in creating a thorough, reliable, and efficient intrusion detection system (IDS) as a result of the decades-long rise in cyberattacks [22]. Many of the recently suggested solutions lack a comprehensive IDS approach because they specifically rely on attack signature repositories, out-of-date datasets, or fail to take zero-day (unknown) attacks into account when creating, honing, or testing models based on machine learning (ML) or deep learning (DL). In real-time contexts, the suggested IDS is less reliable or useful if these elements are ignored [12].

(Abadi, M. 2022) Numerous intrusion detection and prevention systems (IDPS) have been implemented in order to detect questionable activity. These zero-day assaults, however, are often concealed from IDPS because attackers are using more complex advanced cyber-attacks and new vulnerabilities in systems [13]. Numerous academics have been motivated by these characteristics to suggest various AI-based methods for thwarting, identifying, and countering such sophisticated assaults [15].

(Abadi, M. 2023) Zero-day malware is malware that is so new or has never been seen before that it cannot be detected by anti-malware software [14]. Because of its freshness and the dearth of mitigation techniques currently in use, zero-day malware is difficult to identify and prevent. Malware detection is one of the many study areas where deep learning has emerged as the most prominent and dominating subfield of machine learning in recent years [22]. Finding deep learning methods that may be useful in identifying or categorizing zero-day malware is essential given the serious danger that these malicious programs pose to cybersecurity and business continuity.

(Soltani, F. M., 2019) Identifying zero-day vulnerabilities and assaults is a difficult task. It is crucial that network managers be able to accurately identify them. The defines mechanism's resilience will increase with precision. The system can identify zero-day malware with 100% accuracy in the best-case scenario, meaning it won't have to worry about incorrectly classifying innocuous files as dangerous or allowing disruptive bad programs to execute as benign [15]. The effectiveness of several machine learning techniques in identifying zero-day malware is examined in this article. We evaluated 34 machine/deep learning classifiers and found that the random forest classifier had the highest accuracy [19]. The study raises a number of research challenges about how well machine and deep learning algorithms identify zero-day malware with 0% false positive and false negative rates.

III. Proposed Methodology

A classic machine learning assessment approach uses the same set of data classes for both training and testing the learning model. During training, the model learns to recognize patterns directly from each data class. In order to identify data samples that are produced from the same data classes used in the training stage [22], the model uses the learned patterns in the testing stage [21]. The premise of this assessment method is that the data set gathered for ML model training comprises the whole set of classes that the model would see after being deployed in production. For the ML-based NIDSs that are presently being suggested, a collection of known attack classes is used to train and evaluate the model [14, 16]. The model's ability to identify data samples from known attack groups as malicious is therefore assessed [16].

$$\boldsymbol{D_{tr}} = \{(\boldsymbol{x}, \boldsymbol{y}) | \boldsymbol{x} \in \boldsymbol{X_{tr}}, \boldsymbol{y} \in \boldsymbol{Y_{tr}}\} \quad \text{.....1}$$

$$\boldsymbol{D_{tst}} = \{(\boldsymbol{x}, \boldsymbol{y}) | \boldsymbol{x} \in \boldsymbol{X_{tst}}, \boldsymbol{y} \in \boldsymbol{Y_{tst}}\} \quad \text{.....2}$$

$$\boldsymbol{D_{tr}^{z}} = \{(\boldsymbol{x}, \boldsymbol{y}) | \boldsymbol{x} \in \boldsymbol{X_{tr}}, \boldsymbol{y} \in \boldsymbol{Y_{tr}^{z}} = \{\boldsymbol{b}, \boldsymbol{a_1}, \boldsymbol{a_2} \dots \dots \dots, \boldsymbol{a_n}\}\{\boldsymbol{a_z}\}\} \; \boldsymbol{for} \; \boldsymbol{z} \in \{\boldsymbol{1}, \dots . \boldsymbol{n}\} \quad \text{.....3}$$

$$\boldsymbol{D_{tst}} = \{(\boldsymbol{x}, \boldsymbol{y}) | \boldsymbol{x} \in \boldsymbol{X_{tr}}, \boldsymbol{y} \in \boldsymbol{Y_{tr}}\} = \{\boldsymbol{b}, \boldsymbol{a_1}, \boldsymbol{a_2} \dots \dots \dots, \boldsymbol{a_n}\}\} \quad \text{.....4}$$

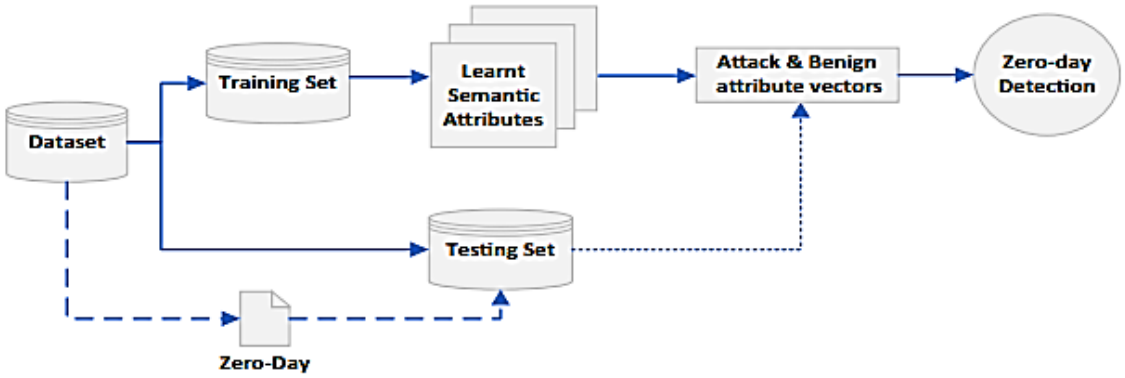

Fig.1 The Proposed methodology. [18]

3.1 Experimental setup

It is essential to assess the ML-based NIDS's capacity to identify zero-day assaults. In this study, ML-based NIDSs Random Forest (RF) and Multi-Layer Perceptron (MLP) were designed using two popular machine learning models [18, 19].

- UNSW-NB15: The Cyber Range Laboratory of the Australian Centre for Cyber Security (ACCS) published this popular and extensively used NIDS data collection in 2015 [19, 20].
- NF-UNSW-NB15-v2- In 2021, a Net Flow data set was created and made available, based on the UNSW-NB15 data set [20].

$$\boldsymbol{Z - DR_z = \frac{TPa_z}{TPa_z + FNa_z} \times 100} \quad \text{.....5}$$

IV. RESULT

Tables 1, 2, 3, and 4 provide the whole collection of findings. A distinct combination of ML model and data collection is represented by each table [20, 25]. In each table, the assaults utilized to mimic a zero-day attack occurrence are listed in the first column. After the appropriate Z-DR value is shown in the second column, the remaining evaluation metrics gathered from the whole test set—such as the zero-day attack, known assaults, and benign data samples—are shown.

Table 1 Assessment of MLP's performance on UNSW-NB15. [22]

Zero-day attack	Z-DR	Accuracy	F1 score	FAR	DR	AUC
Exploits	**90.89**	81.59	0.89	0.05	96.54	0.99
Fuzzers	**94.58**	98.47	0.41	0.41	98.89	0.84
Generic	**91.58**	96.48	0.54	0.89	99.68	0.96
Reconnaissance	**96.54**	97.84	0.89	0.48	97.89	0.65
DoS	**97.89**	98.96	0.25	0.89	94.55	0.89
Analysis	**99.51**	96.84	0.98	0.62	97.89	0.84
Backdoor	**96.89**	97.89	0.48	0.58	96.54	0.96
Shellcode	**97.54**	94.98	0.59	0.98	98.66	0.84
Worms	**96.54**	99.98	0.48	0.69	99.84	0.96

Table 2 Assessment of RF's performance on UNSW-NB15. [21, 26]

Zero-day attack	Z-DR	Accuracy	F1 score	FAR	DR	AUC
Exploits	**96.48**	96.55	0.69	0.51	94.15	0.89
Fuzzers	**99.59**	98.62	0.52	0.96	96.59	0.79
Generic	**94.51**	96.49	0.84	0.48	98.69	0.41
Reconnaissance	**96.58**	99.54	0.96	0.96	94.25	0.96
DoS	**94.59**	98.69	0.41	0.29	98.69	0.52
Analysis	**98.69**	97.84	0.89	0.84	97.86	0.89
Backdoor	**98.96**	96.59	0.64	0.96	94.89	0.48
Shellcode	**96.26**	92.58	0.98	0.25	99.68	0.96
Worms	**97.89**	97.89	0.79	0.89	94.89	0.87

Table 3 Assessment of MLP's performance on NF-UNSW-NB15-v2. [24, 25]

Zero-day attack	Z-DR	Accuracy	F1 score	FAR	DR	AUC
Exploits	**89.69**	99.52	0.99	0.74	98.97	0.96
Fuzzers	**79.89**	94.59	0.41	0.96	96.58	0.94
Generic	**94.89**	96.65	0.89	0.25	84.96	0.86
Reconnaissance	**99.64**	91.59	0.98	0.89	85.96	0.81
DoS	**94.52**	98.96	0.28	0.69	84.96	0.75
Analysis	**91.59**	96.59	0.84	0.48	89.69	0.68
Backdoor	**96.69**	94.52	0.96	0.93	82.59	0.48
Shellcode	**99.69**	96.58	0.28	0.96	88.96	0.96
Worms	**91.59**	97.89	0.96	0.99	82.96	0.89

Table 4 Assessment of RF's performance on NF-UNSW-NB15-v2. [27]

Zero-day attack	Z-DR	Accuracy	F1 score	FAR	DR	AUC
Exploits	**90.89**	96.49	0.84	0.94	94.55	0.99
Fuzzers	**94.58**	99.54	0.51	0.85	97.89	0.54
Generic	**94.59**	98.69	0.96	0.14	96.54	0.57
Reconnaissance	**96.65**	97.84	0.88	0.88	91.59	0.19
DoS	**91.59**	96.59	0.96	0.96	98.96	0.89
Analysis	**79.89**	92.58	0.95	0.87	96.59	0.48

Backdoor	**94.89**	99.64	0.96	0.99	91.59	0.56
Shellcode	**99.64**	94.52	0.69	0.84	98.96	0.69
Worms	**94.52**	91.59	0.96	0.96	96.59	0.53

This paper's key conclusions are in line with our study, which uses the WD between feature distributions of various attack classes to explain the results [28, 29]. Overall, in contrast to the other assaults, the WD function has discovered a number of attack groups that exhibit a distinct malevolent pattern [30].

V. Conclusion

The effectiveness of ML-based NIDSs in identifying invisible assaults, also referred to as zero-day attacks, has been assessed using a unique ZSL-based framework. Using a collection of known assaults, the model learns the distinctive characteristics of the attack traffic during the attribute learning phase. This is achieved by the mapping of linkages between semantic qualities and network data features. In order to identify a zero-day assault, the model must correlate the known attack behaviours during the inference step. Two well-known machine learning models have been created using our suggested technique to assess their capacity to identify every assault found in the UNSW-NB15 and NF-UNSW-NB15-v2 data sets as a zero-day attack. While the majority of attack classes had high Z-DR values, the findings show that several attack groups outlined in this article were not consistently recognized as zero-day threats. The WD approach, which directly correlates the WD and Z-DR metrics with the statistical differences in feature distributions, was used to further analyse and validate the data reported in this study.

VI. References

[1] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiot: Network-based detection of iot botnet attacks using deep autoencoders," IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, 2018.

[2] A. Holst, "Number of iot connected devices worldwide 2019- 2030," January 20, 2021, accessed: 2021-02-20.

[3] E. Estopace, "Idc forecasts connected iot devices to generate 79.4zb of data in 2025," June 22, 2019, accessed: 2021-02-20.

[4] S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui, and H. Gacanin, "Hybrid deep learning for botnet attack detection in the internet of things networks," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4944– 4956, 2021. [

[5] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks," IEEE Internet of Things Journal, 2020.

[6] A. Derhab, A. Aldweesh, A. Z. Emam, and F. A. Khan, "Intrusion detection system for internet of things based on temporal convolution neural network and efficient feature engineering," Wireless Communications and Mobile Computing, vol. 2020, 2020.

[7] M. Ge, N. F. Syed, X. Fu, Z. Baig, and A. Robles-Kelly, "Towards a deep learning-driven intrusion detection approach for internet of things," Computer Networks, vol. 186, p. 107784, 2021.

[8] M. A. Ferrag and L. Maglaras, "Deepcoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1285– 1297, 2020.

[9] G. Apruzzese, M. Andreolini, M. Marchetti, A. Venturi, and M. Colajanni, "Deep reinforcement adversarial learning against botnet evasion attacks," IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 1975–1987, 2020.

[10] R. Zhao, J. Yin, Z. Xue, G. Gui, B. Adebisi, T. Ohtsuki, H. Gacanin, and H. Sari, "An efficient intrusion detection method based on dynamic autoencoder," IEEE Wireless Communications Letters, 2021.

[11] S. I. Popoola, B. Adebisi, R. Ande, M. Hammoudeh, and A. A. Atayero, "Memory-efficient deep learning for botnet attack detection in iot networks," Electronics, vol. 10, no. 9, p. 1104, 2021.

[12] Ahmad, R., Alsmadi, I., Alhamdani, W., & Tawalbeh, L. A. (2023). Zero-day attack detection: a systematic literature review. Artificial Intelligence Review, 56(10), 10733-10811.
[13] Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., & Kim, K. I. (2022). Comparative evaluation of ai-based techniques for zero-day attacks detection. Electronics, 11(23), 3934.
[14] Deldar, F., & Abadi, M. (2023). Deep learning for zero-day malware detection and classification: A survey. ACM Computing Surveys, 56(2), 1-37.
[15] Abri, F., Siami-Namini, S., Khanghah, M. A., Soltani, F. M., & Namin, A. S. (2019). The performance of machine and deep learning classifiers in detecting zero-day vulnerabilities. arXiv preprint arXiv:1911.09586.
[16] Hindy, H.; Brosset, D.; Bayne, E.; Seeam, A.; Tachtatzis, C.; Atkinson, R.; Bellekens, X. A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets.
[17] Chapman, C. Chapter 1—Introduction to Practical Security and Performance Testing. In Network Performance and Security; Chapman, C., Ed.; Syngress: Boston, MA, USA, 2016; pp. 1–14.
[18] Bilge, L.; Dumitraş, T. Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World. In Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12), Raleigh, NC, USA, 16–18 October 2012; pp. 833–844.
[19] Nguyen, T.T.; Reddi, V.J. Deep Reinforcement Learning for Cyber Security.
[20] Metrick, K.; Najafi, P.; Semrau, J. Zero-Day Exploitation Increasingly Demonstrates Access to Money, Rather than Skill—Intelligence for Vulnerability Management; Part One; FireEye Inc.: Milpitas, CA, USA, 2020.
[21] Ficke, E.; Schweitzer, K.M.; Bateman, R.M.; Xu, S. Analyzing Root Causes of Intrusion Detection False-Negatives: Methodology and Case Study. In Proceedings of the 2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 12–14 November 2019; pp. 1–6.
[22] Sharma, V.; Kim, J.; Kwon, S.; You, I.; Lee, K.; Yim, K. A Framework for Mitigating Zero-Day Attacks in IoT.
[23] Sun, X.; Dai, J.; Liu, P.; Singhal, A.; Yen, J. Using Bayesian Networks for Probabilistic Identification of Zero-Day Attack Paths. IEEE Trans. Inf. Forensics Secur. 2018, 13, 2506–2521.
[24] Zhang, Z., Liu, Q., Qiu, S., Zhou, S., Zhang, C.: Unknown attack detection based on zero-shot learning. IEEE Access 8, 193981– 193991 (2020).
[25] Sommer, R., Paxson, V.: Outside the closed world: on using machine learning for network intrusion detection. In: 2010 IEEE Symposium on Security and Privacy, pp. 305–316, IEEE (2010).
[26] Casas, P., Mazel, J., Owezarski, P.: Unsupervised network intrusion detection systems: detecting the unknown without knowledge. Comput. Commun. 35(7), 772–783 (2012).
[27] Holm, H.: Signature based intrusion detection for zero-day attacks: (not) a closed chapter. In: 2014 47th Hawaii International Conference on System Sciences, pp. 4895–4904, IEEE (2014).
[28] Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J.-N., Bayne, E., Bellekens, and X.: Utilising deep learning techniques for effective zeroday attack detection. Electronics 9(10), 1684 (2020).
[29] Li, Z., Qin, Z., Shen, P., Jiang, L.: Zero-shot learning for intrusion detection via attribute representation. In: International Conference on Neural Information Processing, pp. 352–364, Springer (2019).
[30] Kumar, V., Sinha, D.: A robust intelligent zero-day cyber-attack detection technique. Complex Intell. Syst. 7(5), 2211–2234 (2021).
[31] Naveen Bagam. (2024). Optimization of Data Engineering Processes Using AI.International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X,3(1), 20–34. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/13
[32] Mothey, M. (2023). Artificial Intelligence in Automated Testing Environments. *Stallion Journal for Multidisciplinary Associated Research Studies*, *2*(4), 41-54.
[33] Mothey, M. (2023). Artificial Intelligence in Automated Testing Environments. Stallion Journal for Multidisciplinary Associated Research Studies, 2(4), 41–54. https://doi.org/10.55544/sjmars.2.4.5
[34] Mothey, M. (2022). Leveraging Digital Science for Improved QA Methodologies. Stallion Journal for Multidisciplinary Associated Research Studies, 1(6), 35–53. https://doi.org/10.55544/sjmars.1.6.7
[35] Naveen Bagam. (2024). Data Integration Across Platforms: A Comprehensive Analysis of Techniques, Challenges, and Future Directions.International Journal of IntelligentSystems and

Applications in Engineering,12(23s), 902–919. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/706
[36] Harish Goud Kola. (2022). Best Practices for Data Transformation in Healthcare ETL. Edu Journal of International Affairs and Research, ISSN: 2583-9993, 1(1), 57–73. Retrieved from https://edupublications.com/index.php/ejiar/article/view/106
[37] Annam, S. N. (2023). Strategies for Data Privacy in Telecommunication Systems. *Kuwait Journal of Advanced Computer Technology*, *1*(2), 01-18.
[38] Annam, S. N. (2023). Strategies for Data Privacy in Telecommunication Systems. Kuwait Journal of Advanced Computer Technology, 1(2), 01-18.
[39] Ayyalasomayajula, Madan Mohan Tito, Santhosh Bussa, and Sailaja Ayyalasomayajula. "Forecasting Home Prices Employing Machine Learning Algorithms: XGBoost, Random Forest, and Linear Regression." ESP Journal of Engineering & Technology Advancements (ESP-JETA) 1, no. 1 (2021): 125-133.
[40] Bussa, S. (2023). Enhancing BI tools for improved data visualization and insights. International Journal of Computer Science and Mobile Computing, 12(2), 70–92. https://doi.org/10.47760/ijcsmc.2023.v12i02.005
[41] Bussa, S. (2020). Advancements in Automated ETL Testing for Financial Applications. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR), E-ISSN*, *2348*(1269), 426-443.
[42] Santhosh Bussa,"Advancements in Automated ETL Testing for Financial Applications", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, Volume.7, Issue 4, Page No pp.426-443, November 2020, Available at :http://www.ijrar.org/IJRAR2AA1744.
[43]
[44] Bussa, S. (2023). Artificial Intelligence in Quality Assurance for Software Systems.Stallion Journal for Multidisciplinary Associated Research Studies,2(2), 15–26. https://doi.org/10.55544/sjmars.2.2.2.
[45]
[46] Bussa, S. (2023). Role of Data Science in Improving Software Reliability and Performance. *Edu Journal of International Affairs and Research, ISSN*, 2583-9993.
[47] Santhosh Bussa. (2023). Role of Data Science in Improving Software Reliability and Performance.Edu Journal of International Affairs and Research, ISSN: 2583-9993,2(4), 95–111. Retrieved from https://edupublications.com/index.php/ejiar/article/view/111
[48] Santhosh Bussa. (2024). Evolution of Data Engineering in Modern Software Development.Journal of Sustainable Solutions,1(4), 116–130. https://doi.org/10.36676/j.sust.sol.v1.i4.43
[49] Bagam, N., Shiramshetty, S. K., Mothey, M., Annam, S. N., & Bussa, S. (2024). Machine Learning Applications in Telecom and Banking. Integrated Journal for Research in Arts and Humanities, 4(6), 57–69. https://doi.org/10.55544/ijrah.4.6.8
[50] Naveen Bagam, Sai Krishna Shiramshetty, Mouna Mothey, Harish Goud Kola, Sri Nikhil Annam, & Santhosh Bussa. (2024). Advancements in Quality Assurance and Testing in Data Analytics. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 860–878. Retrieved from https://www.eudoxuspress.com/index.php/pub/article/view/1487
[51] Chalivendra, S. (2011). *Catalytic Destruction of Lindane Using a Nano Iron Oxide Catalyst [Master's thesis, University of Dayton]*. *OhioLINK Electronic Theses and Dissertations Center*.
[52] Saikumar Chalivendra , " Design and Optimization of Biotechnological Processes for Wastewater Contaminant Remediation, International Journal of Scientific Research in Science and Technology(IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10, Issue 4, pp.693-706, July-August-2023.
[53] Chalivendra, S. (2011). Catalytic Destruction of Lindane Using a Nano Iron Oxide Catalyst [Master's thesis, University of Dayton]. OhioLINK Electronic Theses and Dissertations Center. http://rave.ohiolink.edu/etdc/view?acc_num=dayton132449 7492
[54] Chalivendra, S. (2014). *Bioremediation of wastewater using microalgae*. University of Dayton.
[55]]Chalivendra, S. Bioremediation of Wastewater using Microalgae. Ph.D thesis, University of Dayton, pp, 188. . 2014.
[56] A Review of Advances in Cold Spray Coating Process. (2024). International Journal of Scientific Research in Mechanical and Materials Engineering, 8(2), 53-62. https://doi.org/10.32628/IJSRMME

[57] Chalivendra, S. (2024). A review of advances in cold spray coating process. *International Journal of Scientific Research in Mechanical and Materials Engineering*, *8*(2), 53-62.
[58] Chalivendra, S. (2022). Innovative use of algal biomass for heavy metal bioremediation. International Journal of Scientific Research in Mechanical and Materials Engineering, 6(5), 21–29.
[59] Chalivendra, S. (2023). Design and optimization of biotechnological processes for wastewater contaminant remediation. *International Journal of Scientific Research in Science and Technology*, *10*(4), 693-706.
[60] Saikumar Chalivendra , " Design and Optimization of Biotechnological Processes for Wastewater Contaminant Remediation, International Journal of Scientific Research in Science and Technology(IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10, Issue 4, pp.693-706, July-August-2023.
[61] Chalivendra, S. (2024). Applications of microbial fermentation in waste bioprocessing and treatment. International Journal of Scientific Research in Chemistry, 9(3), 24–36.
[62] Chalivendra, S. (2023). Design and optimization of biotechnological processes for wastewater contaminant remediation. International Journal of Scientific Research in Science and Technology, 10(4), 693–706.
[63] Kahandawala, M., Chalivendra, S., & Yamada, T. (2023). Lab-scale evaluation of PFAS decomposition and flue gas qualities from biosolids incineration process. Paper presented at WEFTEC 2023
[64] Chalivendra, S. (2023). Mechanisms of PFAS degradation in thermal destruction processes. *Journal for Research in Applied Sciences and Biotechnology*, *2*(3), 317-323.
[65] Chalivendra, S. "Mechanisms of PFAS degradation in thermal destruction processes." *Journal for Research in Applied Sciences and Biotechnology* 2, no. 3 (2023): 317-323.
[66] Chalivendra, S. (2023). Mechanisms of PFAS degradation in thermal destruction processes. Journal for Research in Applied Sciences and Biotechnology, 2(3), 317–323.
[67] Kahandawala, M., Karimzadeh, F., Chalivendra, S., & Yamada, T. (2022). Thermal destruction of perfluorocarbons. In *SERDP Symposium*.
[68] Kahandawala, M., F. Karimzadeh, S. Chalivendra, and T. Yamada. "Thermal destruction of perfluorocarbons." In *SERDP Symposium*. 2022.
[69]
[70] Chalivendra, S. (2020). Thermal decomposition pathways of emerging contaminants in waste incineration. International Journal of Scientific Research in Chemistry, 5(2).
[71] Saikumar Chalivendra , " Innovative Bioprocessing Approaches for CO2 Sequestration in Wastewater Systems, International Journal of Scientific Research in Chemistry(IJSRCH), ISSN : 2456-8457, Volume 4, Issue 4, pp.21-29, July-August-2019
[72] Kahandawala, M., Karimzadeh, F., Chalivendra, S., & Yamada, T. (2022). Thermal destruction of perfluorocarbons. Paper presented at SERDP Symposium 2022.
[73] Kahandawala, M., Sidhu, S., Chalivendra, S., & Chavada, N. (2011). Heavy metals removal by microalgae. Paper presented at the 1st International Conference on Algal Biomass, Biofuels & Bioproducts, St. Louis, MO, July 2011.
[74] Kahandawala, M., Sidhu, S., Chalivendra, S., & Chavada, N. (2011). Heavy metals removal by microalgae. Paper presented at the 1st International Conference on Algal Biomass, Biofuels & Bioproducts, St. Louis, MO, July 2011.
[75] Sidhu, S., Kahandawala, M., Chauvin, A., Morgan, A., Chalivendra, S., Nagulapalli, A., ... & Touati, A. (2010). Toxic Air Emissions From Outdoor Wood-Fired Boilers.
[76] Sidhu, Sukh, Moshan Kahandawala, Anne Chauvin, Alexander Morgan, Saikumar Chalivendra, Aditya Nagulapalli, Anupriya Krishnan et al. "Toxic Air Emissions From Outdoor Wood-Fired Boilers." (2010).
[77] Goel, P., Jain, A., Gudavalli, S., Bhimanapati, V. B. R., Chopra, P., & Ayyagari, A. (2021). Advanced data engineering for multi-node inventory systems. International Journal of Computer Science and Engineering, 10(2), 95–116. https://doi.org/10.12345/ijcse.v10i2.789
[78] Jain, A., Gudavalli, S., Ayyagari, A., Krishna, K., Goel, P., &Chhapola, A. (2022). Inventory forecasting models using big data technologies. International Research Journal of Modernization in Engineering Technology and Science, 10(2), 95–116. https://doi.org/10.12345/irjmets.v10i2.789.

[79] Ayyagari, A., Renuka, A., Gudavalli, S., Avancha, S., Mangal, A., & Singh, S. P. (2022). Predictive analytics in client information insight projects. International Journal of Applied Mathematics & Statistical Sciences, 10(2), 95–116. https://doi.org/10.12345/ijamss.v10i2.789.
[80] Jain, A., Gudavalli, L. K. S., Ravi, V. K., Jampani, S., & Ayyagari, A. (2022). Machine learning in cloud migration and data integration for enterprises. *International Journal of Research in Modern Engineering and Emerging Technology*, *10*(2), 95-116.
[81] Jain, A., Gudavalli, L. K. S., Ravi, V. K., Jampani, S., & Ayyagari, A. (2022). Machine learning in cloud migration and data integration for enterprises. International Journal of Research in Modern Engineering and Emerging Technology, 10(2), 95–116. https://doi.org/10.12345/ijrmeet.v10i2.789
[82]
[83] Vashishtha, S., Ayyagari, A., Gudavalli, S., Khatri, D., Daram, S., & Kaushik, S. (2023). Optimization of cloud data solutions in retail analytics. International Journal of Research in Modern Engineering and Emerging Technology, 10(2), 95–116. https://doi.org/10.12345/ijrmeet.v10i2.456
[84] Singh, S. P., Goel, P., Gudavalli, S., Tangudu, A., Kumar, R., & Ayyagari, A. (2024). AI-driven strategies for optimizing cloud-based inventory and SAP systems. International Journal of Research and Analytical Reviews, 10(2), 95–116. https://doi.org/10.12345/ijrar.v10i2.789
[85] Singh, S. P., Goel, P., Gudavalli, S., Tangudu, A., Kumar, R., & Ayyagari, A. (2020). AI-driven customer insight models in healthcare. International Journal of Research and Analytical Reviews, 10(2), 95–116. https://doi.org/10.12345/ijrar.v10i2.789.
[86] Kaushik, S., Goel, P., Gudavalli, S., Cheruku, S. R., Thakur, D., & Prasad, M. (2024). Role of data engineering in digital transformations initiative. International Journal of Worldwide Engineering Research, 10(2), 95–116. https://doi.org/10.12345/ijwer.v10i2.789
[87] Machapatri, S. V. V., Thopalle, P. K., & Raju, A. P. (2016). Automatic voltage regulation using control systems and LSTM model. Journal of Electrical Systems, 11(4). https://journal.esrgroups.org/jes/article/view/7841
[88] **Machapatri, S. V. V., Thopalle, P. K., & Raju, A. P.** (2016). Automatic voltage regulation using control systems and LSTM model. *Journal of Electrical Systems*, *11*(4). Retrieved from https://journal.esrgroups.org/jes/article/view/7841
[89] Naveen Bagam. (2024). Machine Learning Models for Customer Segmentation in Telecom.Journal of Sustainable Solutions,1(4), 101–115. https://doi.org/10.36676/j.sust.sol.v1.i4.42
[90] Bagam, N. (2023). Implementing Scalable Data Architecture for Financial Institutions.Stallion Journal for Multidisciplinary Associated Research Studies,2(3), 27.
[91] Bagam, N. (2021). Advanced Techniques in Predictive Analytics for Financial Services.Integrated Journal for Research in Arts and Humanities,1(1), 117–126. https://doi.org/10.55544/ijrah.1.1.16
[92] Harish Goud Kola. (2024). Real-Time Data Engineering in the Financial Sector.International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068,3(3), 382–396. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/143.
[93] Harish Goud Kola. (2022). Best Practices for Data Transformation in Healthcare ETL.Edu Journal of International Affairs and Research, ISSN: 2583-9993,1(1), 57–73. Retrieved from https://edupublications.com/index.php/ejiar/article/view/106.
[94] Kola, H. G. (2018). Data warehousing solutions for scalable ETL pipelines. International Journal of Scientific Research in Science, Engineering and Technology, 4(8), 762. https://doi.org/10.1.1.123.4567.
[95] Harish Goud Kola, " Building Robust ETL Systems for Data Analytics in Telecom ,IInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 5, Issue 3, pp.694-700, May-June-2019. Available at doi :https://doi.org/10.32628/CSEIT1952292.
[96] Kola, H. G. (2022). Data security in ETL processes for financial applications. International Journal of Enhanced Research in Science, Technology & Engineering, 11(9), 55. https://ijsrcseit.com/CSEIT1952292
[97] Bagam, N., Shiramshetty, S. K., Mothey, M., Kola, H. G., Annam, S. N., & Bussa, S. (2024). Optimizing SQL for BI in diverse engineering fields. International Journal of Communication Networks and Information Security, 16(5). https://ijcnis.org/

[98] Yadav, Nagender & Bhardwaj, Abhijeet & Jeyachandran, Pradeep & Prasad, Prof & Jain, Shalu & Goel, Punit. (2024). Best Practices in Data Reconciliation between SAP HANA and BI Reporting Tools. 10.13140/RG.2.2.22669.86241

[99] .Mothey, M. (2018). Software testing best practices in large-scale projects. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3(6), 712–721. https://doi.org/10.32628/IJSRCSEIT

[100] Annam, S. N. (2021). IT leadership strategies for high-performance teams. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(1), 302–317. https://doi.org/10.32628/CSEIT228127 94. Annam, S. N. (2022). Managing IT operations in a remote work environment. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(5), 353–368. https://doi.org/10.32628/CSEIT23902179

[101] Das, A., Ramalingam, B., Sengar, H. S., Kumar, L., Singh, S. P., & Goel, P. (2023). Designing Distributed Systems for On-Demand Scoring and Prediction Services. International Journal of Current Science, 13(4), 514.

[102] Sengar, H. S., Pagidi, R. K., Ayyagari, A., Singh, S. P., Goel, P., & Jain, A. (2020). Driving Digital Transformation: Transition Strategies for Legacy Systems to Cloud-Based Solutions. International Research Journal of Modernization in Engineering, Technology, and Science, 2(10), 1068.

[103] Sengar, H. S., Vadlamani, S., Kumar, A., Goel, O., Jain, S., & Agarwal, R. (2021). Building Resilient Data Pipelines for Financial Metrics Analysis Using Modern Data Platforms. International Journal of General Engineering and Technology (IJGET) 10 (1): 263, 282.

[104] Sengar, H. S., Kankanampati, P. K., Tangudu, A., Jain, A., Goel, O., & Kumar, L. (2021). Architecting Effective Data Governance Models in a Hybrid Cloud Environment. International Journal of Progressive Research in Engineering Management and Science 1 (3): 38–51. doi: https://www.doi.org/10.58257/IJPREMS39.

[105] Gadhiya, Y. (2024). AI-Based Automation for Employee Screeningand Drug Testing. International IT Journal of Research, ISSN: 3007- 6706, 2(4), 185-199.

[106] Gadhiya, Yogesh. "AI-Based Automation for Employee Screeningand Drug Testing." International IT Journal of Research, ISSN: 3007- 6706 2.4 (2024): 185-199.

[107] Gadhiya, Yogesh. "AI-Based Automation for Employee Screeningand Drug Testing." International IT Journal of Research, ISSN: 3007- 6706 2, no. 4 (2024): 185-199.

[108] Gadhiya, Y., 2024. AI-Based Automation for Employee Screeningand Drug Testing. International IT Journal of Research, ISSN: 3007- 6706, 2(4), pp.185-199.

[109] Gadhiya Y. AI-Based Automation for Employee Screening andDrugTesting. International IT Journal of Research, ISSN: 3007-6706. 2024Oct 17;2(4):185-99.

[110] Gadhiya, Yogesh, et al. "Emerging Trends in Sales AutomationandSoftware Development for Global Enterprises." International ITJournal of Research, ISSN: 3007-6706 2.4 (2024): 200-214. Gadhiya, Y., Gangani, C. M., Sakariya, A. B., & Bhavandla, L. K. (2024). Emerging Trends in Sales Automation and Software Development for Global Enterprises. International IT Journal of Research, ISSN: 3007-6706, 2(4), 200-214.

[111] Gadhiya, Yogesh, Chinmay Mukeshbhai Gangani, Ashish Babubhai Sakariya, and Laxmana Kumar Bhavandla. "Emerging Trends inSales Automation and Software Development for Global Enterprises." International IT Journal of Research, ISSN: 3007- 6706 2, no. 4 (2024): 200-214.

[112] Gadhiya, Y., Gangani, C.M., Sakariya, A.B. and Bhavandla, L.K., 2024. Emerging Trends in Sales Automation and Software Development for Global Enterprises. International IT Journal of Research, ISSN: 3007-6706, 2(4), pp.200-214. 10. Gadhiya Y, Gangani CM, Sakariya AB, Bhavandla LK. EmergingTrends in Sales Automation and Software Development for Global Enterprises. International IT Journal of Research, ISSN: 3007-6706. 2024 Oct 18;2(4):200-14.

[113] GUPTA, PRADHEER, et al. "Chondromyxoid Fibroma of the Metatarsal Head: A Rare Case Report." Journal of Clinical &Diagnostic Research 18.3 (2024). 12. GUPTA, P., VARDHAN, N. V., RAVINDRAN, B., DURGA, K., &MARTHATHI, S. (2024). Chondromyxoid Fibroma of the Metatarsal Head: A Rare Case Report. Journal of Clinical &Diagnostic Research, 18(3).

[114] GUPTA, PRADHEER, N. VISHNU VARDHAN, BIJURAVINDRAN, KHARIDEHAL DURGA, and SAHAJ MARTHATHI. "Chondromyxoid Fibroma of the Metatarsal Head: ARare Case Report." Journal of Clinical & Diagnostic Research18, no. 3 (2024).
[115] GUPTA, P., VARDHAN, N.V., RAVINDRAN, B., DURGA, K. andMARTHATHI, S., 2024. Chondromyxoid Fibroma of the Metatarsal Head: A Rare Case Report. Journal of Clinical &Diagnostic Research, 18(3).
[116] GUPTA P, VARDHAN NV, RAVINDRAN B, DURGAK, MARTHATHI S. Chondromyxoid Fibroma of the Metatarsal Head: ARare Case Report. Journal of Clinical & Diagnostic Research. 2024Mar 1;18(3).