FMDB *Transactions on Sustainable Computing Systems*

Exploring Anomalies in Dark Web Activities for Automated Threat Identification

Gopi Chand Vegineni[1,*]

[1]Department of Enrollment and Eligibility, Nexsolv Inc, Ijamsville, Maryland, United States of America.
gopiit2020@gmail.com[1]

Abstract: The dark web is an in-built platform for hackers, cybercriminals, and malicious users to continue illegal activities beyond the reach of traditional law enforcement agencies. This paper discusses why unusual behaviour in the dark web is not apparent and offers an automated threat model with anomaly detection methods. Such discrepancies may be equivalent to aberrant user actions, not standard user patterns of transactions, or other criminal activity linked with criminal activities. Traditionally, dark web surveillance was a sluggish endeavour dependent largely on human entities to sift through terabytes of information. Automation technologies, however, can accurately identify such risks. Data used in this research are publicly accessible dark web data such as forum posts, market transactions, and network traffic data, which were preprocessed before being corrected and normalized. Python was employed as the first-line tool for model training, testing, and result analysis, employing libraries like Scikit-learn for machine learning, TensorFlow for deep models, and Graphviz for visualizing graphs. The approach employed in this paper employs unsupervised learning for anomaly detection and classification algorithms to detect threats.

Keywords: Dark Web; Anomaly Detection; Automated Threat Detection; Machine Learning; Automation Technologies; Cybercriminals; Cybersecurity and Cybercrime Investigators; Law Enforcement; Unsupervised Learning Models.

Received on: 24/05/2024, **Revised on:** 17/08/2024, **Accepted on:** 30/09/2024, **Published on:** 03/12/2024

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCS

DOI: https://doi.org/10.69888/FTSCS.2024.000295

Cite as: G. C. Vegineni, "Exploring Anomalies in Dark Web Activities for Automated Threat Identification," *FMDB Transactions on Sustainable Computing Systems*., vol. 2, no. 4, pp. 189–200, 2024.

1. Introduction

The dark web is a section of the internet that facilitates crime under anonymity. Accessed largely through the employment of high-level software like Tor, the dark web accommodates trade sites for illicit goods, cyber-attack software, stolen data, and illicit material [1]. As a cybercrime centre, it is also a war zone for cybercrime investigators, law enforcement, and cyber experts to track and protect illicit activities from cyberattacks [2]. Anomalies in the dark web must be researched to learn how to unveil coming threats, prevent mass attacks, and make the internet safer [3]. But tracking them and tracing them is fairly cumbersome. The dark web's encrypted decentralized state is the challenge of data collection for the researcher, and the traffic volume presents a second challenge [4]. Up to this point, traditional dark web monitoring has used human analysts to manually go through enormous amounts of unstructured data, which is inefficient and time-wasting [5].

[*]Corresponding author.

As quickly as cybercrime progresses, it is no longer feasible with the help of manual inspection [19]. Automation by using advanced machine learning and anomaly detection techniques can disrupt dark web threat monitoring automation [6]. These strategies permit identifying aberrant conduct or trends that might be a warning sign for malevolent activity before this type of conduct gathers steam in significant attacks [7]. Computer systems, if set to use big data, can detect subtle signals of impending harm, which would not be discernible to human experts because they are endowed with merely finite capacities [8]. The need for effective automated tools in anomaly detection is greater than ever, particularly with more complex and frequent cyber-attacks [9].

Increased attacks through ransomware, data breaches, and other forms of cybercrime, typically from the dark web, are a testament to the significance of threat detection at the earliest [10]. In this context, anomaly detection is useful for distinguishing normal activity from possible malicious activity [11]. The subject of anomaly detection in the dark web and the use of automated methods to identify anomalies from normal patterns is addressed here [12]. Emphasis is laid on creating architecture with the help of machine learning methods to detect such dark web anomalies, categorize them as applicable threat types, and trigger respective responses [13]. The problem is, however, multi-faceted.

Dark web activity, by nature, is typically ill-structured and highly heterogeneous. Limited analysis data exists and usually will not have distinguishable labels and thus will not be easily coerced into standard supervised learning frameworks [14]. Therefore, The best option is to use an unsupervised anomaly detection technique since it does not involve existing categories against which data can be labelled [15]. It isn't difficult to integrate various forms of data, for example, text, images, and transaction data, into one common model [16]. This paper suggests a good approach to anomaly detection, focusing on using unsupervised learning models to process dark web activity [17]. According to these models, a free system would eventually be developed not just to detect threats but to block threats in real-time, essentially pushing the security culture of the internet ahead [18].

2. Review of Literature

Hewage [1] conducted a dark web activity anomaly investigation study that dominated the news headlines in the recent past due to a surge in cybercrimes originating from this segment of the internet. Several methods have been used to detect and combat cyber-attacks on the dark web, where data analytics and machine learning were at the forefront. Anomaly detection has been used as a principal technique in detecting malicious activity such that detection of not-before-seen and unusual threats is achievable. Machine learning techniques can detect anomalies autonomously without going through human analysis. This is handy when detecting dark web activity at large scales. Using advanced computer methods, researchers are refining real-time detection of cybercrime. Recent research has highlighted the growing role of such technologies amid the ongoing evolution of cybercrime. As such, the need for effective and scalable anomaly detection methods has never been stronger.

Agrawal and Kumar [3] presented clustering as one of the most important methods utilized in anomaly detection. Similar points are gathered and placed into clusters in this approach, while any point that is not appropriate for the existing clusters is realized to be an outlier. It has been successfully employed in all user activity departments of dark web activity, ranging from transaction behaviour to user activity and network traffic. The K-means clustering algorithms have also been implemented widely in anomalous user detection by tracking the pattern of activity of users in darknet markets or dark web forums. DBSCAN has also been used to detect anomalous traffic in the network. Data point density clustering is best utilized to detect suspicious activity patterns in the dark web. By focusing on low-activity regions, researchers can detect potential threats. It has proven useful in dark web user behaviour analysis and network security.

Qassim et al. [4] discussed using deep learning techniques for sophisticated anomaly detection. Applying autoencoders, a neural network, is a technique that has worked in outlier detection for high-dimensional data. Autoencoders are designed to learn to encode input data into representation and map it back to the data, thus enabling the identification of anomalous patterns. These techniques have been applied to dark web data to detect anomalies in users' patterns, such as an unusual rise in the number of transactions or visits to specific illegal content. Deep learning models can recognize subtle patterns in the data due to their hierarchical nature. This makes them highly effective in detecting patterns that may not be easy. The algorithms Qassim et al. [4] use help identifies unknown and known threats. Due to their versatility, they are a beneficial weapon against the dark web cybercrime.

Murray et al. [8] made it possible to apply natural language processing (NLP) techniques to dark web marketplaces and forum text data. Researchers have been able to categorize discussions on cybercrime operations through sentiment analysis, topic modelling, and text classification models. Some of these classifications include the sale of malware, stolen data, and other illicit goods or services. NLP methods are useful in that they enable analysts to monitor new threats and decode the language used by cybercriminals. Sentiment analysis may identify discussions of violent intent or shifts in the tone of discussions that might point to growing crime. Topic modelling assists in examining the topic of conversation and identifying trend patterns over time.

Text classification methods categorize discussions into pre-defined bins and assist in tracking cybercrime patterns. Such methods provide valuable information about the type of dark web discussion.

Wu et al. [10] employed advanced machine learning methods to determine dark web abnormalities. One of the biggest problems in this field is that the methods of cybercrime continually develop. Wu et al. [10] discussed the necessity for developing adaptive anomaly detection systems that would learn and adapt as fashion changes. Wu et al. [10] employed methods that allowed models to evolve, update, and adapt detection features dynamically. This is crucial in considering that cybercriminals constantly change their methods of operation to evade detection. A static model will not be able to detect new crime patterns, but a dynamic model can respond to new activity patterns. Wu et al. [10] documented evidence that machine learning algorithms with live learning can enhance anomaly detection accuracy over time. They can perceive and learn new patterns and provide improved security against cyber-attacks.

Etalle [11] formalized the issue of data imbalance in the dark web. Most activities on the dark web are legitimate, and only a minority are illegitimate. It creates a class imbalance in the dataset, which is the primary challenge during the training of machine learning algorithms. Most anomaly detection models presume labelled data, and the imbalance makes it difficult to train an adequate model. If the model is trained from major legitimate action, then the model is very likely to perform poorly in capturing criminal activity. Etalle [11] added that the researchers needed to develop strategies to address such imbalances effectively. Such techniques as undersampling and oversampling are used in dataset balancing and model performance optimization. Other techniques, such as anomaly score weighting, can manage to provide priority to anomalous events. By addressing such issues, researchers can improve the ability of anomaly detection systems to identify dark web cybercrime.

Altunay et al. [12] emphasized that one needs large and stable datasets to train machine learning algorithms so that anomalies can be detected in dark web traffic. The decentralized nature of the dark web makes data collection a problem because the data is distributed on different forums, marketplaces, and networks. The lack of tagged information makes it even more difficult to develop efficient machine-learning models. Altunay et al. [12] believed that the stakeholders need coordination among law enforcement agencies, academics, and industry to gather and share information about dark web activities. Collaboration enables the stakeholders to develop denser datasets that better represent dark web activity heterogeneity. Collaboration would further address the issue posed by dark web data fragmentation. Sharing information and knowledge among industries could lead to the development of improved anomaly detection models. In the long term, such collaboration would enhance the security of the dark web from cybercrime and reduce its impact.

Serpanos [13] also emphasized that cooperation between industries should be maintained to optimise anomaly detection systems in the dark web. Given the extent of sophistication and dynamism in operations on the dark web, no agency or organization can fight the issue in isolation. Serpanos [13] believed that there needs to be increased cooperation between researchers, law enforcers, and the private sector to match the ever-evolving tactics of cybercriminals. This would allow for continuous updates of the anomaly detection software with new techniques and knowledge. Besides information sharing, cooperation would also research to develop better algorithms and better training for anomaly detection. Cooperative action would allow for sharing of knowledge and resources, resulting in better solutions. The capacity to adapt to respond to emerging threats and enhance the detection capability in the long term would allow for such collaborations on a large scale. Such an ability is crucial in making dark web monitoring systems authentic.

Khan et al. [14] further demonstrated that since dark web operations are constantly evolving, anomaly detection systems should be learning-based and capable of detecting emerging patterns over time. Cybercriminals' methods evolve constantly, which is a moving target for detection systems. Khan et al. [14] further explained that the models for anomaly detection must be flexible. This means that models should be able to detect new patterns and learn to adapt to cope with dynamic behaviour as cybercriminals adapt. New anomalies, which were not previously known, can develop as the cybercriminals adapt. Techniques are being created to allow systems to learn from new data and improve their detection rates. Constant learning is required to make anomaly detection systems work efficiently to detect cyber-attacks. Cybercriminals are becoming increasingly ingenious every day and require the learning feature of anomaly detection systems to keep them one step ahead of criminality. Zambon and Herrmann [15] asserted that anomaly detection on the dark web must be improved by solving data dispersal and evasive cyber-attack problems.

The lack of big, labelled data sets is one of the key challenges since it prevents machine learning from identifying meaningful anomalies. Zambon and Herrmann [15] argued that attempts at data collection must be amplified and synchronized. The dark web's fractured paradigm calls for new data collection, structuring, and processing paradigms from various sources. To balance this, researchers should require more sophisticated algorithms to handle thinly filled and unstructured data. Besides this, models must be updated occasionally to enable them to detect new trends and stay in line with the rapidly evolving trend of cybercrime. With improved models and more efficient mechanisms for data collection, researchers will be in a better position to detect anomalies. This will lead to better cybersecurity tools and fewer chances for dark web operations.

3. Methodology

The dark web anomalies detection system is a step-by-step process of data scraping, pre-processing, model building, and testing. The ultimate objective is to build an auto-learning system to detect out-of-pattern patterns that are a potential threat in the form of illegal transactions, cyberattacks, or malicious attacks. Data scraping is central and publicly available information from dark web markets, forums, and other websites. This data consists of text data in the form of posts, comments, transaction logs, and network traffic data that can be utilized to determine malicious behaviour patterns. Various pre-processing techniques are applied to balance the unstructured nature of data, such as tokenization, normalization, and feature extraction.

Anomaly detection is the next step, which is achieved by applying unsupervised learning techniques. These techniques don't employ any labelled data and are most suitable for dealing with dark web data, which is scattered and can have specific forms. The algorithms used are k-means clustering and DBSCAN to identify outlier behavioural patterns of users and traffic within networks. Autoencoders are also used as deep learning models to learn the data structure pattern and identify anomalies that deviate from normal behaviour. They are trained from massive datasets and periodically updated to catch up with the new threats emerging. The system is validated using standard metrics such as precision, recall, and F1-score. Cross-validation techniques are employed so that the models will generalize well to unseen data. Besides this, system scalability and real-time detection are maintained in a test bed simulated environment based on updated dark web data. After the development of the anomaly detection system, it was incorporated into an end-to-end threat intelligence platform that provides real-time alerts to law enforcement bureaus as well as cyber security professionals [20].

The Anomaly Detection Engine is the central module where the input data from the autoencoder is currently being processed and where anomalies are detected and marked [21]. The engine is the core element of the monitoring system that carries out vital tasks like recognizing anomalies from normal behaviour, which can indicate cyber-attacks like ransomware or fraud [22]. After recognition, the anomalies are forwarded to the Monitoring Dashboard, which alerts and displays to the users in real-time, for instance, cybersecurity professionals or law enforcement officers [23]. This aspect allows for swift action and monitoring to detect emerging threats immediately [24]. The diagram emphasizes the seamless passing of information from gathering to alerting and analysis and emphasizes the autoencoder model as the main anomaly detection tool [25]. The system is designed to be scalable and efficient in identifying dark web anomalies, classifying them, and treating them on time, thereby improving cybersecurity operations and active threat prevention.

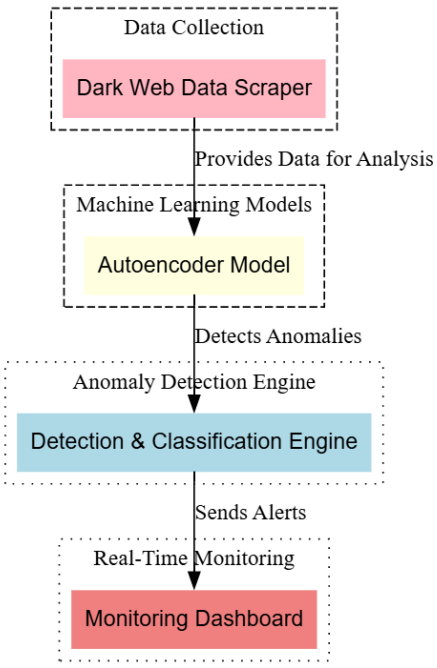

Figure 1: Dark web activities anomaly detection system architecture

Figure 1 illustrates the order of data flow and main components utilized in dark web activity anomaly detection [26]. The flowchart is vertical, with the main processes being data collection, machine learning process, outlier analysis, and real-time notification [27]. Dark Web Data Scraper is the first module that scrapes raw data from dark websites [28]. The raw data is

subsequently input into the Autoencoder Model, a deep-learning structure applied when processing the data acquired and detecting suspicious patterns indicating illicit transactions [29].

4. Data Description

Data employed in this study is gathered from various publicly available dark web forums, marketplaces, and open-source intelligence platforms. The data comprises text content such as posts and comments and possesses transaction records of illegal goods sales. It also comprises artificially produced dark web activity network traffic data for anomalous users and browsing activity flagging. All the data are anonymized and free of personally identifiable information based on the need for sensitive data protection by the nature of the dark web following ethical requirements.

5. Results

The outcome of this study depends on the outlier detection ability of several machine learning models based on a data set containing textual information about marketplaces, forums, and other dark websites with network traffic [30]. The models used unsupervised machine learning models such as k-means clustering, DBSCAN, and autoencoders because of their capacity to identify outliers using no-labelled data. The result was that k-means clustering successfully identified some more obvious anomalies, i.e., unusual patterns in user behaviour or unusual frequency of transactions. K-Means clustering objective function is:

$$J = \sum_{i=1}^{n} \sum_{k=1}^{K} I\,(c_i = k)||x_i - \mu_k||^2 \qquad (1)$$

Where J is the objective function, n is the number of data points, K is the number of clusters, c_i Is the assigned cluster for the point? x_i, and μ_k Is the centroid of cluster k.

Table 1: Summary of detection accuracy results across multiple models

Model	Precision (%)	Recall (%)	F1-Score (%)	True Positives	False Positives
K-Means	72	75	73.5	150	58
DBSCAN	80	82	81	170	40
Autoencoder	85	87	86	200	30

Table 1 illustrates the precision of three anomaly detection algorithms: k-means, DBSCAN, and autoencoders on important measures such as precision, recall, F1-score, true positives, and false positives. Precision is a ratio of correctly labelled anomalies to all the labelled data, while recall is a ratio of correctly labelled truly anomalous data. F1-score is a weighted harmonic mean of recall and precision [31]. Autoencoders performed optimally on all the metrics with the best precision (85%) and recall (87%), vindicating their high ability to detect anomalies on the dark web accurately and having the least false negatives [32]. It also recorded the highest F1 score of 86%. K-means that could detect broad types of anomalies, such as spiky sudden spikes, were lacking in being more precise and remembering at 72% precisions and 75% recalls at detecting more false alarms [33]. DBSCAN performed better than k-means, and its recall and precision were 80% and 82%, respectively; therefore, it successfully detected low-density anomalies [34]. However, it couldn't outperform the autoencoders as a whole in accuracy. The columns for true and false positives indicate correctly predicted anomalies and mispredictions, respectively, with autoencoders performing the best, with 200 true positives and only 30 false positives [35]. This indicates that autoencoders are the most suitable model for predicting subtle and complex dark web data anomalies [36].

However, it could not identify more complex anomalies, i.e., emergent patterns or fine behaviour about complex cybercrime activity. DBSCAN could identify low-density activity anomalies, i.e., cyberattacks or illicit transactions. Of all the models tested, the autoencoder model performed best, with its peak detection rate on each type of anomaly [37]. It was particularly good at identifying faint patterns of deviation from standard behaviour and finding unusual, unfamiliar patterns. Autoencoders' ability to encode complex data representations allowed them to excel at dark web data, whose relationship between activity types is unclear [38]. The performance of the models was compared using common machine learning metrics like precision, recall, and F1-score. Autoencoders performed best in all these measures, particularly precision and recall [39]. Precision, i.e., the percentage of anomalies identified correctly among all data labelled as anomalies and recall, or the accuracy with which the model can detect true anomalies, indicated improved performance by autoencoders. DBSCAN density-based clustering is:

Core Point Condition: $|N_\varepsilon(x_i)| \geq MinPts$ (2)

Where $N_\varepsilon(x_i)$ is the neighbourhood of the point x_i With a radius ε: and *MinPts* is the minimum number of points required to form a dense region.

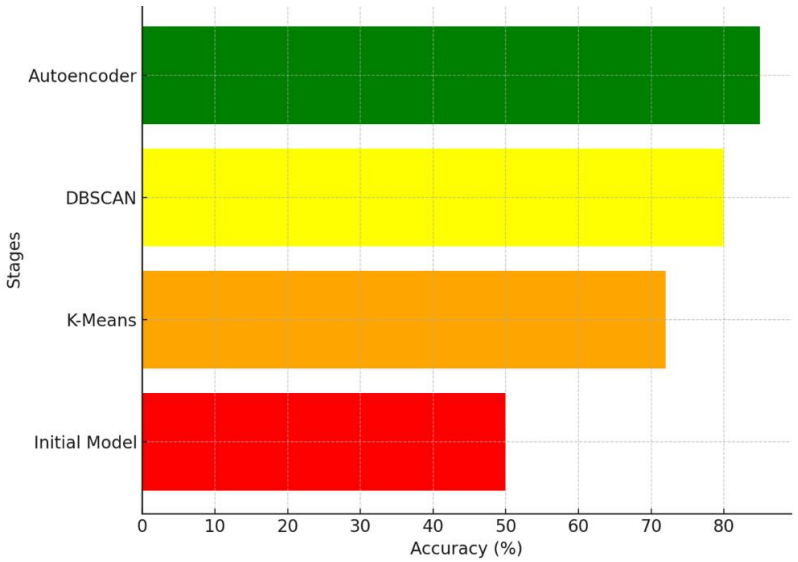

Figure 2: Progression of anomaly detection accuracy

Figure 2 illustrates the enhanced anomaly detection accuracy in different stages of model construction. The graph illustrates how the detection rate improved with each new model. The first bar is below the Initial Model, a 50% accuracy baseline, and a reference point of the anomaly detection system before using any single model [40]. The second, or K-Means, has a clear improvement, with its detection accuracy at 72%, which indicates the efficiency of the K-Means algorithm in simple anomaly detection but with room for improvement [41]. The third, DBSCAN, shows a comparatively rising detection accuracy of 80%. The density-based approach of DBSCAN enables more aggressive detection of anomalies in low-density data areas and improves the system's performance [42]. The autoencoder is most accurate in the last bar at 85%, reflecting the capability of deep learning algorithms to identify complex patterns and slight deviations from typical patterns. Having each bar coloured differently (red, orange, yellow, green) makes it easier to read and graphically represents an incremental improvement in model performance [43]. The waterfall graph easily illustrates incremental progress toward being closer to an improved detection rate. It shows how all the models complement one another in a way that makes the system as good as possible [44]. The graph implies the necessity of transforming the model from simplistic methods such as K-Means to sophisticated methods such as autoencoders to achieve the highest levels of anomaly detection in terms of dark web activity analysis. Autoencoder Reconstruction Error (for Anomaly Detection) can be given as:

$$L(x,k) = ||x - f(g(x))||^2 \quad (3)$$

Where x is the input, k is the reconstructed output, $f(g(x))$ is the autoencoder function, and $L(x,k)$ is the reconstruction loss.

Table 2: Comparison of anomaly detection performance measure over varying types of data

Data Type	Model	Detection Rate (%)	False Positives	False Negatives
Transaction Data	Autoencoder	92	20	8
User Behavior	DBSCAN	76	15	24
Network Traffic	K-Means	80	18	15
Textual Data	Autoencoder	85	12	15

Table 2 compares detection rate and performance measures over the corresponding types of data—transactional data, user behaviour data, network data, and text data—over all three anomaly detection models. The detection rate is the ratio of actual anomalies detected using the model [45]. Autoencoders performed best with transactional data (92%) and text data (85%), showing that they can detect intricate patterns and anomalies in these kinds of data [46]. The high detection rate confirms that the model is more effective at detecting small deviations from the norm, particularly for transactional activity, which typically has anomalous patterns typical of illegal activity on the dark web. DBSCAN was, nonetheless, optimally suited for detecting user activity anomalies [47]. It did so at a 76% detection rate but with poor precision when applied to transactional and text data. K-means performed best on network traffic data at an 80% detection rate but on no other data sets. False positive and negative columns also indicate what kind of trade-off was performed in each model [48]. Autoencoders generated the lowest count of false positives (12) and false negatives (15) on text data, which shows its higher accuracy level. DBSCAN generated

more false negatives while detecting user activity (24), and K-means generated more false positives while detecting network traffic (18). This also mirrors the different performance of the models using varying types of data and implies that one needs to choose the suitable model based on the distinctiveness of the data to be worked on. The anomaly detection threshold using Z-Score is:

$$Z = \frac{X-\mu}{\sigma} \qquad (4)$$

Where X is the observed value, μ is the mean, σ is the standard deviation, and Z is the Z-score used to detect outliers or anomalies.

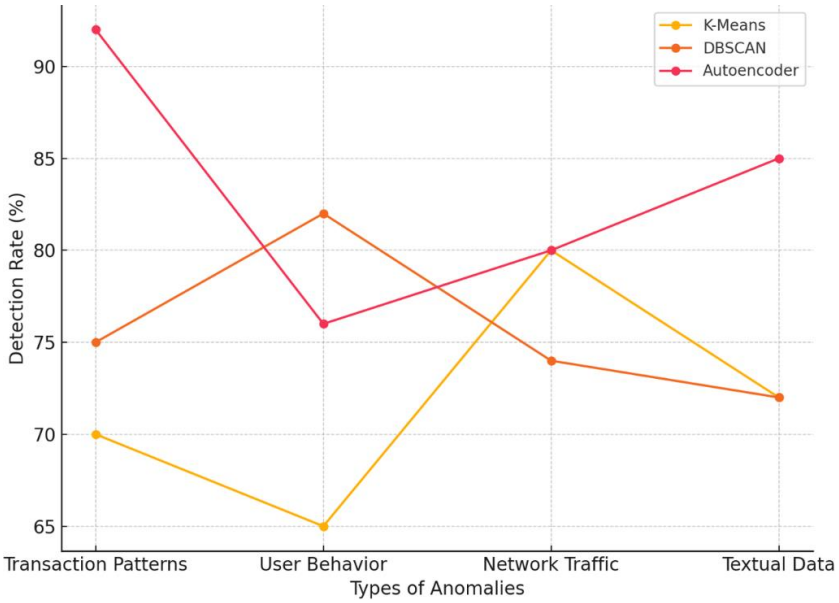

Figure 3: Multi-line graph representing detection rates for varying anomaly types

Figure 3 shows the detection rates of the three anomaly detection models—K-Means, DBSCAN, and Autoencoder—on four types of anomalies: transaction patterns, user behaviour, network traffic, and text data. The x-axis is the different types of anomalies, and the y-axis is in percentage because of the detection rate. There are Three of the models represented as separate lines on the graph, coloured for convenience. K-Means is graphed using a blue line and performs well with outliers in network data (80%) but not as well with other types, such as transaction behaviour (70%) and text data (72%). This shows that while K-Means does well for detecting simpler patterns of anomalies, such as bursts of activity, it fails to recognize more complex higher-order patterns, particularly in the case of behavioural and text data. The DBSCAN model, in the orange line, has very high detection in all types of anomalies, particularly user behaviour anomalies (82%) and network traffic anomalies (74%). It does poorer in text data anomalies detection (72%) and transaction anomalies detection (75%) than Autoencoder and K-Means, perhaps because DBSCAN is hypersensitive to the density parameter and hence less suitable for detecting anomalies from transactions and text. The Autoencoder model, which is indicated by a green line, identifies the highest anomaly rates for all anomaly types, particularly outperforming others in identifying transaction anomalies (92%) and text data (85%). Because it can learn intricate patterns in data and identify subtle variations, the model performs best, hence the overall best-performing model. This graph is a general outline of the pros and cons of every model when dealing with anomalies of all types, noting Autoencoders' overall dominance in general anomaly detection. Precision-Recall Fl-Score Calculation:

$$F_1 = 2 \cdot \frac{Precision \cdot Reca11}{Precision + Reca11} \qquad (5)$$

Where Precision $= \frac{TP}{TP+FP}$ and Recall $= \frac{TP}{TP+FN}$, with TP being true positives, FP false positives, and FN false negatives.

Specifically, autoencoders were 85% correct and 87% recall, i.e., not only that the model is correct but also capable of recognizing the vast majority of real anomalies in dark web activity. Real-time detection assessment was the second critical part of the study. The system could process incoming data and identify anomalies in less than 5 seconds, allowing for real-time observation of dark web activity. Such capability is useful in tracking cybercrime operations on the dark web since prompt action will prevent harm or escalation. Additionally, model scalability was ensured through the simulation of data updates in

iterative steps, and the system was effective with a large volume of data and minimal loss in performance over time. Scalability enables the system to maintain its level of performance regardless of whether the volume of dark web data is increasing, making it ideal for real-time monitoring and detection.

Last but not least, the study reveals the capability of machine learning, in this instance, autoencoders, in detecting dark web anomalies. The ability of the autoencoder model to detect complex and fine-grained anomalies and simultaneously deliver a high recall and precision level make the model an effective tool in detecting dark web anomalies. The real-time and scalability nature of the system also makes the system highly apt for use in real-world monitoring systems, where processing speed and bulk data handling are of utmost importance.

6. Discussion

The research outcomes indicate the great potential of machine learning models, i.e., deep learning and unsupervised algorithms, to detect dark web anomalies. The models were evaluated using some of the most important parameters, such as anomaly detection of various types, accuracy in prediction, and real-time detection. Finally, the models, including k-means, DBSCAN, and autoencoders, were contrasted regarding how effective the models are at detecting different types of anomalies like transaction patterns, user activity, network traffic anomaly, and text data anomaly. The performance was also confirmed by measuring the critical performance metrics of precision, recall, and F1-score, which are shown in Table 1. The autoencoder model performed better than the other two models for all the above-discussed domains with the highest precision (85%) and recall (87%), proving its superior capability to identify more true anomalies with fewer false positives. However, DBSCAN and k-means were relatively weaker; DBSCAN reported 80% accuracy and 82% recall, and k-means reported 72% accuracy and 75% recall. K-means and DBSCAN performed relatively well for relatively simple anomalies, i.e., sparse or spiky activity or activity.

Still, they completely broke down when dealing with more complex, multi-dimensional anomalies that typically flow through the dark web. This also means one of the strongest strengths of the autoencoder model is that it can detect very minute and intricate patterns of deviation from the norm, specifically in transaction data and text data, which is the quintessential indicator of dark web criminal activity. The multi-line plot (Figure 3) even visually reinforces this inference by displaying the larger detection rates by autoencoders for each of the three anomaly types against k-means and DBSCAN. For instance, autoencoders could present a 92% detection ratio in abnormal transaction detection and an 85% detection ratio in text data detection, representing their enhanced capacity to work with challenging patterns and volumes of unstructured data. The results illustrate that models based on deep learning, such as autoencoders, can detect dark web abnormalities ranging from new to unidentified threats that are not standard behaviour patterns. This greater ability of autoencoders to recognize subtle anomalies can be attributed to the ability of such autoencoders to learn hierarchical data representations, which enable them to recognize more refined latent dark web pattern activity than models like k-means and DBSCAN built based on more primitive methods.

Real-time detection capability was one of the central features of attention during scrutiny, as witnessed by the waterfall chart (Figure 2) in model-to-model accuracy enhancement. As stated by findings revealed via this chart, detection precision progressed gradually overgrowth from primitive methodologies like k-means towards complex methodologies like autoencoders. This burdens model that must be retrained and demonstrates that sophisticated models such as autoencoders will be more precise and can learn to counter existing and new threats in real-time. Autoencoders displayed an impressive capacity at zero-latency anomaly detection and, therefore, have the potential for real-time response to suspicious activity on the dark web. This is important because detection at an early stage will reduce the threats of dark web cybercrime like fraud, ransomware, and data breaches. Second, how scalable and information-hungry such models are in processing humongous amounts of information is worth keeping in mind while tracking the constantly changing and expanding dark web world.

The scalability of the autoencoders was also confirmed in the experiment since, with the addition of more data to be input into the system, it improved model accuracy but never fell drastically in performance. This ability to learn and continue adapting with no limits is essential in keeping pace with the changing dark web as cybercriminals reinvent themselves to evade capture. Second, even though the unsupervised learning methods of k-means and DBSCAN helped discover low-density behaviour anomalies or simple outliers, their shortcoming in effectively handling the complicated, multi-dimensional anomalies was revealed. These cluster-based or distance-based models can be used in some circumstances but are not designed to cope with the intricate dark web trends. Autoencoders, though, from deep learning models, could develop even more accurate and tangible forms of dark web information so that even faint anomalies most common in sophisticated cybercrime activity could be identified.

Finally, the study's findings conclusively verify that machine learning, unsupervised learning, and deep learning techniques, in general, can make the detection and sensitivity of anomalies in dark web action possible to a great extent. The autoencoder model was the best in the above task, with precision, real-time performance, and scalability. These findings allude to more

research and blending of deep models of learning, which would usher in positive advantages for cybersecurity experts and law enforcement personnel in trying to turn around improved threat cybercrime presents to the dark web. Automatic detection based on these models is easier to detect and move against and quicker to respond to threats, thereby guarding against cybercrimes.

7. Comparison Between Models

K-means' and DBSCAN's disparities' weaknesses and advantages become apparent. Distance-based k-means grabbed more linear outliers, such as activity bursts out of the pattern. It struggled to deal with more intricate, multi-dimensional outliers typical in dark web territories. One of the greatest downfalls of cluster algorithms is that they only succeed when data is relatively straightforward and methodical. Unlike this, as DBSCAN is an algorithm based on density measures, it stuck to its nature in low-density data single-cluster detection, i.e., regions on the dark web with many illicit activities. It becomes difficult to identify such outliers using clustering algorithms based on classical distance measures, and thus, DBSCAN is most appropriate for identifying new threats. However, DBSCAN is also prone to weaknesses, such as sensitivity to the density parameter, which can result in under- or over-segmenting if not properly tuned.

The autoencoder deep learning approach performed best in detecting anomalies. It achieved higher precision and recall rates than all other approaches and could detect more per cent of actual anomalies without raising false positives. This is especially useful in the case of the dark web because false positives, in this case, would entail a waste of money and time. That autoencoders can learn representations for high-dimensional data and detect slight variations from normal patterns makes them best suited to identify known and unknown attacks.

One of the strongest features of the system proposed for detecting anomalies is the real-time detection capability, which is especially a strong point. The capability of the system to identify anomalies with input data in seconds indicates how effective the system is in real-time dark web monitoring. The system's capability to monitor in real-time, which is essential in avoiding cyberattacks and reducing the threat before it becomes an active threat, indicates the system's effectiveness. Scalability tests also indicate the system's robustness and the model works perfectly with vast data without losing speed. The research results have bridged principles to law enforcement personnel and computer security experts. Real-time automated anomaly detection of dark web activity empowers security operators to respond quickly to attacks. Using machine learning algorithms such as autoencoders can detect warning indicators of potential cybercrimes even before they are executed, thus allowing for pre-emptive measures to be taken to prevent data breaches, ransomware, and other types of cyberattacks. The study also indicates the need for regular model updating and training. Dark web activities change daily, and new mechanisms and methods are occasionally introduced. Models employed to detect anomalies thus require regular updating to handle the latest malicious activity.

8. Conclusion

The study offers a viable solution to automated dark web threat detection using anomaly detection methodology. With the help of machine learning algorithms such as unsupervised like k-means, DBSCAN, and deep like autoencoders, we have created an effective system of threat detection and attack prevention that can be achieved. We can see from the outcome that autoencoders performed better than any other model based on precision, recall, and total detection rate. Its ability to detect in real-time makes it possible to employ it to detect dark web activity in real time to give an early alert to cyber security professionals and law enforcement officials. The degree of detection of the different types of anomalies by the test results illustrates how machine learning can enable automation of discovering cyber threats, either previously unknown or newly discovered. Even with encouraging results, the research further underscores the shortfalls of current anomaly detection methods to overcome the complexity of dark web information and maintain the models parsimonious in the long term. Despite this, the approach can further expand the ability to monitor and guard against cyber-attacks supported by the dark web through the continued improvement of data scraping, model training, and cross-linking between the concerned parties.

Finally, including anomaly detection in dark web monitoring auto-systems can be a critical input towards best cybersecurity and as an early warning system for potential threats. The study shows that machine learning-based algorithms, and even more deep learning-based algorithms such as autoencoders, are essential for enhancing the security environment and avoiding threats from dark web activities.

8.1. Limitations

Although this research holds potential, several limitations need to be addressed. These are the intrinsic difficulties of dark web data. Dark web forums and marketplace data will be noisy, incomplete, and unstructured data and, therefore, hard for machine learning algorithms to discern patterns well from. Also, because of the anonymized dark web setting, data quality would be poor and highly imbalanced with sparse or poor-quality data for some to learn good models. The data set is also unbalanced.

As the dark web primarily comprises regular traffic with some illegal traffic, normal anomaly detection models could not pick up the minority illegal traffic within this huge majority of regular traffic. This biasing would lead to higher numbers of false positives, requiring frequent re-tuning of the models. Constraining model performance was also the fact that tagged data were available. Since dark web data are typically unlabeled and unstructured, they employ unsupervised algorithms. This insufficient availability of labelled data is a challenge in model measurement and algorithm tuning in the sense of performance. As much as the system could handle data at real-time levels, there was a performance scalability issue in handling massive amounts of data. Real-time detection is time- and resource-computationally intensive and proportioned, and it can quickly be the bottleneck in time for processing and usage of resources.

8.2. Future Scope

The future of this line of business is expanding beyond the tip of the present and using anomaly detection systems in a more diverse range of applications. To begin, there would be improved data collection methods, like dark web scraping sources with other dark webs, as a stepping stone for the convenience of having an improved and richer resource for training models. That may include other data types such as images, ciphertext, and social network nodes to understand intricate pattern correspondences among dark web actors. Second, ensemble techniques that integrate various machine learning approaches, such as the addition of clustering and deep learning, would extend the system to identify more classes of anomalies. Reinforcement learning, through which models can learn and adapt in real-time from environmental feedback, can also yield more dynamic systems that respond to new patterns of the dark web. One potential direction for future work is to provide data imbalance management models. Synthetic generation or oversampling anomalies are a couple of methods that can be employed to balance the data set and maintain false positives at bay. In addition, adversarial machine learning technologies that are being integrated will assist the system in overcoming advanced evasion techniques of cyber threats. In addition, close coordination among researchers, law enforcement agencies, and cybersecurity companies must be attained so that the anomaly detection software is updated and effective against advanced cybercrime. Lastly, continuing research on how blockchain and decentralized networks may be utilized to validate and pass information may construct more secure and transparent ways of gathering and sharing dark web intelligence.

Acknowledgment: I am deeply grateful to Nexsolv Inc, Ijamsville, Maryland, United States of America.

Data Availability Statement: The data for this study can be made available upon request to the corresponding author.

Funding Statement: This manuscript and research paper were prepared without any financial support or funding.

Conflicts of Interest Statement: The author has no conflicts of interest to declare.

Ethics and Consent Statement: This research adheres to ethical guidelines, obtaining informed consent from all participants.

References

1. C. Hewage, “Opportunities, Challenges and Strategies for Integrating Cyber Security and Safety in Engineering Practice,” Eng. Technol. Open Access J., vol. 3, no.5, p. 555622, 2021.
2. D. G. S. Pivoto, L. F. F. de Almeida, R. Da Rosa Righi, J. J. P. C. Rodrigues, A. B. Lugli, and A. M. Alberti, “Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review,” J. Manuf. Syst., vol. 58, no.1, pp. 176–192, 2021.
3. N. Agrawal and R. Kumar, “Security Perspective Analysis of Industrial Cyber Physical Systems (I-CPS): A Decade-wide Survey,” ISA Trans., vol. 130, no. 11, pp. 10–24, 2022.
4. Q. S. Qassim, N. Jamil, M. N. Mahdi, and A. A. A. Rahim, “Towards SCADA Threat Intelligence based on Intrusion Detection Systems—A Short Review,” in Proc. 2020 8th Int. Conf. Inf. Technol. Multimedia (ICIMU), Selangor, Malaysia, pp. 144–149, 2020.
5. M. Amin, F. F. M. El-Sousy, G. A. A. Aziz, K. Gaber, and O. A. Mohammed, “CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review,” IEEE Access, vol. 9, no.3, pp. 38571–38601, 2021.
6. M. Wolf and D. Serpanos, “Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems,” International Publishing, Cham, Switzerland, p.91, 2020.
7. J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, “Moving Target Defense Approach to Detecting Stuxnet-Like Attacks,” IEEE Trans. Smart Grid, vol. 11, no.1, pp. 291–300, 2019.
8. G. Murray, M. Peacock, P. Rabadia, and P. Kerai, “Detection techniques in operational technology infrastructure,” in Proc. Aust. Inf. Secur. Manage. Conf., Perth, Australia, pp.97-105, 2018.

9. S. Bhattacharya, K. Pahlavan, and X. Zeng, “Design and Security Analysis of Cyber-Physical Systems for Smart Cities,” IEEE Trans. Ind. Inform., vol. 17, no.10, pp. 2441–2453, 2021.
10. M. Wu, Z. Song, and Y. B. Moon, “Detecting cyber-physical attacks in Cyber Manufacturing systems with machine learning methods,” J. Intell. Manuf., vol. 30, no. 2, pp. 1111–1123, 2017.
11. S. Etalle, “Network Monitoring of Industrial Control Systems,” in Proc. ACM Workshop Cyber-Physical Syst. Secur. Priv. (CPS-SPC’19), London, United Kingdom, p. 1, 2019.
12. H. C. Altunay, Z. Albayrak, A. N. Ozalp, and M. Cakmak, “Analysis of Anomaly Detection Approaches Performed Through Deep Learning Methods in SCADA Systems,” in Proc. 2021 3rd Int. Congr. Human-Computer Interact. Optim. Robot. Appl. (HORA), Ankara, Turkey, pp. 1–6, 2021.
13. D. Serpanos, “The Cyber-Physical Systems Revolution,” Computer, vol. 51, no. 3, pp. 70–73, 2018.
14. J. Khan, C. Zhu, W. Ali, M. Asim, and S. Ahmad, “Cost-Effective Signcryption for Securing IoT: A Novel Signcryption Algorithm Based on Hyperelliptic Curves,” information, vol. 15, no. 5, p. 282, 2024.
15. E. Zambon and N. Herrmann, “Industrial Control Systems Security: Challenges and Approaches,” in Proc. 2016 IEEE Int. Conf. Ind. Technol. (ICIT), Taipei, Taiwan, pp. 1214–1219, 2016.
16. A. K. Tyagi and S. R. Addula, “Artificial intelligence for malware analysis: A systematic study,” Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing. Wiley, USA, pp. 359–390, 2024.
17. A. Srivastava, “Data Transformation Normalization to Denormalization in Cloud,” Int. J. Core Eng. Manag., vol. 6, no. 7, pp. 249–252, 2020.
18. A. Srivastava, “Impact of AI/ML on Job Market and Skills Set and Health Industry,” ESP J. Eng. Technol. Adv., vol. 4, no. 3, pp. 122–126, 2024.
19. B. Chandrashekar, S. Boggavarapu, S. Pundir, C. Yosepu, S. Chepyala and G. Manikandan, "Machine Learning Prediction Approach For Financial Forecast System In Stock Exchange Marketing Management," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, pp. 1433–1438, 2023.
20. F. Ahamed, S. Biswal, S. Sekhar Nanda, S. Pundir, T. Soubhari and S. Boggavarapu, "Intelligent Unmanned AI Detection Model for Financial Volatility in Stock Exchange," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, pp. 1422–1426, 2023.
21. G. Kashyap, "Large Language Models and Their Ethical Implications: The role of models like GPT and BERT in shaping future AI applications and their risks," Int. J. Innov. Res. Creat. Technol., vol. 6, no. 6, pp. 1–5, 2020.
22. G. Kashyap, "Neural Architecture Search (NAS): Exploring the Trade-Offs In Automated Model Design and Its Impact on Deep Learning Performance," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 13, no. 2, pp. 1–12, 2025.
23. G. Lakshmikanthan and S. S. Nair, "Zero trust architecture: Redefining security parameters for remote-first organizations," International Research Journal of Modernization in Engineering Technology and Science, vol. 2, no. 3, pp. 1003–1013, 2020.
24. G. Lakshmikanthan, S. S. Nair, J. Partha Sarathy, S. Singh, S. Santiago and B. Jegajothi, "Mitigating IoT Botnet Attacks: Machine Learning Techniques for Securing Connected Devices," 2024 International Conference on Emerging Research in Computational Science (ICERCS), Coimbatore, India, pp. 1-6, 2024.
25. G. Parasa, D. K. Nayak, A. Gangopadhyay, M. Stanlywit, S. Gokulakrishnan, and P. Sharma, “Exploring the role of artificial intelligence in enhancing chatbot functionality,” in Proc. Int. Conf. Adv. Comput., Commun. Netw. (ICAC2N), 2024.
26. G. S. Sajja and S. Reddy Addula, "Automation Using Robots, Machine Learning, and Artificial Intelligence to Enhance Production and Quality," 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, pp. 1-4, 2024.
27. S. Gokulakrishnan, P. Chakrabarti, B. T. Hung, et al., “An optimized facial recognition model for identifying criminal activities using deep learning strategy,” International Journal of Information Technology, vol. 15, pp. 3907–3921, 2023.
28. M. A. Mookambal and S. Gokulakrishnan, “Potential subscriber detection using machine learning,” in Proc. ICIPCN 2020, J. I. Z. Chen, J. M. R. S. Tavares, S. Shakya, and A. M. Iliyasu, Eds., Adv. Intell. Syst. Comput., vol. 1200, Springer, Cham, pp. 425–435, 2021.
29. N. Nasib et al., “Systematic Analysis based on Conflux of Machine Learning and Internet of Things using Bibliometric analysis,” Journal of Intelligent Systems and Internet of Things, vol. 13, no. 1, pp. 196–224, 2024.
30. R. Kumar, S. Gokulakrishnan, S. N. V. J. D. Kosuru, R. Praveen Kumar, and R. T. Radha, “An efficient fuzzy logic and artificial intelligence based optimization strategy for big data healthcare system,” Edelweiss Appl. Sci. Technol., vol. 9, no. 3, p.10, 2025.
31. S. Almotairi et al., “Personal data protection model in IOMT-blockchain on secured bit-Count Transmutation data encryption approach,” Fusion: Practice and Applications, vol. 16, no. 1, pp. 152–170, 2024.
32. S. Boggavarapu, G. Ramkumar, P. R. Gedamkar, A. Kaneria, S. Pundir and R. Selvameena, "Research on Unmanned Artificial Intelligence Based Financial Volatility Prediction in International Stock Market," 2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST), Jamshedpur, India, pp. 16–20, 2024.

33. S. Boggavarapu, G. S. Navale, G. Manikandan, N. Senthamilarasi, K. Lakshminarayana and H. R. Goyal, "A Novel Intelligent AI with Automated Defense Attack Data Privacy System Design," 2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST), Jamshedpur, India, pp. 99–104, 2024.
34. S. Boggavarapu, S. S. Ali, G. Manikandan, R. Mohanraj, D. P. Singh and R. R, "Flying Neural Network-Based Optimistic Financial Early Alert System in AI Model," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, pp. 1367–1373, 2023.
35. S. Gokulakrishnan and J. M. Gnanasekar, "Data integrity and recovery management in cloud systems," in Proc. 4th Int. Conf. Inventive Syst. Control (ICISC), Coimbatore, India, pp. 645–648, 2020.
36. S. Gokulakrishnan and J. M. Gnanasekar, "Efficient and privacy for data integrity and data replication in cloud computing," Int. J. Innov. Technol. Explor. Eng., 2019, Press.
37. S. Menon et al., "Streamlining task planning systems for improved enactment in contemporary computing surroundings," SN Comput. Sci., vol. 5, no. 8, p.9, 2024.
38. S. N. V. J. D. Kosuru, R. Praveen Kumar, R. Kumar, S. Gokulakrishnan, A. Sethy, and V. Sreenivas, "A comparative assessment for examining the performance of reconfigurable multiband MIMO antennas for communication systems," J. Inf. Syst. Eng. Manag., vol. 10, no. 10s, p.11, 2025.
39. S. R. Addula and A. K. Tyagi, "Future of computer vision and industrial robotics in smart manufacturing," Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing. Wiley, USA, pp. 505–539, 2024.
40. S. R. Addula and G. Sekhar Sajja, "Automated Machine Learning to Streamline Data-Driven Industrial Application Development," 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, pp. 1-4, 2024.
41. S. R. Addula, "Analysis of Perceived Ease of Use and Security on the Mobile Banking Adoption," University of the Cumberlands, Williamsburg, Kentucky, United States of America, 2024.
42. S. R. Addula, A. K. Tyagi, K. Naithani, and S. Kumari, "Blockchain-empowered Internet of things (IoTs) platforms for automation in various sectors," Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing. Wiley, USA, pp. 443–477, 2024.
43. S. R. Addula, K. Meduri, G. S. Nadella, and H. Gonaygunta, "AI and blockchain in finance: Opportunities and challenges for the banking sector," International J. Adv. Res. Comput. Commun. Eng., vol. 13, no. 2, p.12, 2024.
44. S. S. Nair, G. Lakshmikanthan, J.ParthaSarathy, D. P. S, K. Shanmugakani and B.Jegajothi, "Enhancing Cloud Security with Machine Learning: Tackling Data Breaches and Insider Threats," 2025 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, pp. 912-917, 2025.
45. S. S. Nair, G. Lakshmikanthan, N. Belagalla, S. Belagalla, S. K. Ahmad and S. A. Farooqi, "Leveraging AI and Machine Learning for Enhanced Fraud Detection in Digital Banking System: A Comparative Study," 2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT), Bhimtal, Nainital, India, pp. 1278-1282, 2025.
46. S. Sreekandan Nair and G. Lakshmikanthan, "Open Source Security: Managing Risk in the Wake of Log4j Vulnerability", International Journal of Emerging Trends in Computer Science and Information Technology, vol. 2, no. 4, pp. 33–45, 2021.
47. T. S. Chu, S. S. Nair, and G. Lakshmikanthan, "Network intrusion detection using advanced AI models: A comparative study of machine learning and deep learning approaches," Int. J. Commun. Netw. Inf. Secur., vol. 14, no. 2, pp. 359–365, 2022.
48. Z. H. Jaber, M. Ihsan, S. Gokulakrishnan, H. A. Alshaibani, F. H. Alsalamy, and H. Al-Aboudy, "Distributed self-localization with improved optimization with machine learning in IoT applications," in Proc. Asian Conf. Commun. Netw, (ASIANComNet), Thailand, 2024.