VOLUME-3, ISSUE: 1, MAY 2026
ISSN: 3049-0006 (ONLINE)

# A Survey on AI and Machine Learning Techniques for Crime Detection in the Dark Web

***Charmi A. Chauhan[1]|Dr. Shripal Shah[2]***
*[1] Sascma English Medium College, Surat*
*[2] Shree Ramkrishna Institute of Computer Education and Applied Sciences, Surat*

## Abstract

The Dark web enables many illegal activities including drug and weapon trafficking, human exploitation and sale of stolen digital information that are difficult to monitoring so due to anonymity and changing nature. Its hidden structure, supported by strong anonymity tools like Tor, makes tracking these activities extremely difficult. Traditional methods are ineffective so AI and ML are now used to automate analysis and improve detection. This anonymity makes investigation difficult and methods often fail.AI and ML now play the important role by automated data collection, improving detection accuracy and generating useful cyber threat intelligence. This paper surveys recent advances in AI based dark web crime detection. It also discusses challenges, future possibilities and ethical issues.

**Keywords:** Dark web, Artificial Intelligence, Machine learning, Cyber Threat Intelligence, Dark web Monitoring, Crime Detection

## Introduction

Generally, the Internet has three layers: surface, deep and dark. The dark web is a secret part of the Internet. You cannot open it with regular browsers like Google Chrome. To access the dark web, you need special software like the Tor browser. The Tor browser keeps your identity and online actions private. This helps protect privacy, but some people misuse it. Many illegal activities occur on the dark web, such as weapons, cybercrime, online fraud, selling drugs, and human trafficking (Raman et al.,2023) [1].

In recent years, dark web markets have grown rapidly, creating many problems for police and cybersecurity teams. Traditional investigation methods use a lot of manual work like collecting data and checking data by hand. These methods take a lot of time and do not work well because the dark web is hidden part and keeps changing (Mishra et al., 2024) [2].As cybercriminals also update their methods often, so improved and faster solutions are needed.

AI can help solve many issues related to dark web security. They helps in handling many security problems of the dark web. Methods like Machine Learning, Deep Learning and Natural Language Processing help security systems work better and faster. This paper reviews several studies that describe how AI is applied in dark web monitoring. some tools are built to automatically gather and track dark web data continuously (Ruiz Ródenas et al., 2023) [3]. In addition, advanced AI models like large language models can study this data and prepare threat reports. This helps reduce human effort and saves time (Shah & Parast, 2024) [4].Third, AI-based crawlers analyze text and images on the dark web to find illegal activities, such as cybercrime and illegal trading (Medipelly & Abosata, 2024) [5].

Overall, this research shows that AI helps move security from a reactive approach to a proactive one. By continuously checking dark web data, AI can detect threats early and help prevent security incidents (Ovabor et al., 2024) [6].

## Literature Review

Studies have shown that Artificial Intelligence (AI) and Machine Learning (ML) are widely used to monitor the dark web and collect cyber threat information (Raman et al., 2023) [1]. Researchers have developed different approaches, such as modular frameworks, AI-driven

analysis, automated crawlers, and image-based detection techniques, to identify illegal activities on the dark web (Ruiz Ródenas et al., 2023) [3]; (Jegan et al., 2024) [6]; (Medipelly & Abosata, 2024) [5]. These methods support scalability, automation, and improved detection accuracy (Ovabor et al., 2024) [6].

However, several challenges remain, including limited real-time monitoring, a lack of labeled datasets, the anonymous nature of the dark web, and limited practical implementations (Mishra et al., 2024) [2]; (Dhirshal, 2024) [7]. This highlights the need for strong, quick, and ethical AI systems to monitor the dark web and gather cyber threat information (Shah & Parast, 2024). [4].

| Author(s) | Year | Paper Title | Methodology | Key Finding | Research Gap |
|---|---|---|---|---|---|
| Ruiz Ródenas, J. M., Pastor-Galindo, J., & Mármol, F. G. | 2023 | A General and Modular Framework for Dark Web Analysis | Modular microservice-based framework for onion domain analysis | Scalable and flexible dark web analysis system | Existing tools lack modular design |
| Mishra, D. A., Rath, P. S., & Sahu, M. R. | 2024 | A Study on AI Driven Analysis of Dark Web Marketplaces | Analytical study of AI-based monitoring techniques | Improves detection in dark web markets | Real-time monitoring remains difficult |
| Shah, S., & Parast, F. K. | 2024 | AI-Driven Cyber Threat Intelligence Automation | LLM-based automation using GPT models | Reduces manual effort in CTI reporting | Traditional CTI methods are slow and inefficient |
| Ovabor, K., et al. | 2024 | AI-Driven Threat Intelligence for Real-Time Cybersecurity | Review and survey of AI/ML-based CTI tools | Improves accuracy and scalability | Threat complexity is increasing faster than traditional methods |
| Jegan, R., Rajavarman, V., & Geetha, S. | 2024 | AI-Enhanced Dark Web Crawler for Cybersecurity Monitoring | NLP and ML-based dark web crawler | Automates threat detection | Dark web anonymity limits detection accuracy |
| Dhirshal, S. J. | 2024 | Artificial Intelligence in Dark Web Monitoring | Conceptual analysis of AI-based monitoring | Enables real-time monitoring | Limited practical implementation details |
| Raman, R., et al. | 2023 | Darkweb Research: Past, Present, and Future Trends | Bibliometric and trend analysis | Identifies research trends | Does not focus on implementation techniques |

| | | | | | |
|---|---|---|---|---|---|
| Medipelly, S., & Abosata, N. | 2024 | Detection of Dark Web Threats Using ML and Image Processing | ML classifiers with image processing | Detects human trafficking content | Limited dataset and scope |

**Objective**

The main purpose of this study is to understand how Artificial Intelligence (AI) and Machine Learning (ML) are used to detect illegal activities on the dark web. This study had the following objectives:

- To understand the role of AI and ML methods help in detecting, tracking and predicting illegal activities on the dark web, such as cybercrime, drug sales, weapon sales and human trafficking as stated by Mishra et al. (2024) [2].
- To compare different AI-based systems and tools used in dark web monitoring and cyber threat Intelligence focusing on how they system design and their use of automation according to Ruiz Ródenas et al. (2023) [3].
- Jegan et al. (2024) [6] studied how methods like Natural Language Processing (NLP), deep learning, topic modelling, sentiment analysis, and image analysis help find useful information in large, unstructured dark web data.
- To identify existing research gaps, technical difficulties and performance issues in current dark web crime detection methods. Special attention is given to problems related to real-time detection, accuracy, change to new types of threats, and the lack of reliable and high-quality datasets, as highlighted by Ovabor et al. (2024) [5].
- To discuss the ethical, legal, and privacy concerns related to the use of AI for dark web monitoring and to highlight the need for the responsible use of AI in cybersecurity and law enforcement, as emphasized by Alevizos and Dekker (2021) [7].

**Research Methodology**

This study shows how AI and ML help find crimes on the dark web. It reviews past research to compare and combine earlier findings on dark web monitoring and cyber threat intelligence (Ovabor et al., 2024) [1].

Researchers used keyword searches with terms like AI-driven cybersecurity and Dark web marketplaces. They chose studies based on quality, relevance, and goals (Ruiz Rodenas et al., 2023) [3].

Each selected papers were analyzed by their methods, datasets. AI Techniques and results particular focus was given to NLP, Deep Learning , image processing and automated crawling techniques (Jegan et al., 2024) [4]; (Medipelly & Abosata, 2024) [5].

Finally, the studies categorized by application area to clearly identify strengths, limitations and future research needs (Ovabor et al., 2024) [1].

**Research Problem**

Cybercrime on the dark web is increasing worldwide. Criminals use Tor, encryption, and cryptocurrency to hide their identities (Mishra et al., 2024) [1]; (Raman et al., 2023) [2]. Traditional monitoring methods are manual and rule-based, so they do not work well.

Unstructured data, changing markets, and coded language make detection difficult (Ruiz Ródenas et al., 2023) [4]. Therefore, AI-based automated systems are needed to monitor the dark web continuously and detect threats quickly while following ethical and legal guidelines (Shah & Parast, 2024) [5]; (Alevizos & Dekker, 2021) [6].

## Analysis and Findings

Earlier research shows that AI-based techniques are more effective than traditional methods for identifying crimes on the dark web. Machine learning and NLP help analyze dark web content automatically and support early crime detection (Jegan et al., 2024) [6].

AI-based tools can quickly collect data from onion websites, making the process faster and reducing the need for manual work (Ruiz Ródenas et al., 2023) [3].Large language models help improve the speed and quality of cyber threat intelligence faster and with better results (Ruiz Rodenas et al., 2023) [3].Deep Learning and image analysis techniques are used to detect illegal images related to human trafficking (Medipelly & Abosata, 2024) [8].

Still, several problems such as lack of labeled data, incorrect results, criminals avoiding detecting and privacy concerns (Ovabor et al., 2024)[5].

## Conclusion

This review shows that work Dark web Monitoring and detecting important role in Artificial Intelligence (AI) and Machine Learning (ML).So Traditional methods that depend on rules and manual checking do not work well because the dark web is hidden and changes quickly (Mishra et al., 2024) [2].AI methods like Machine Learning, Deep Learning, Natural language processing and large language Models help find crimes on the dark web faster and more accurately (Ruiz Rodenas et al., 2023) [3]; (Shah & Parast,2024) [4].

These results indicate that Artificial Intelligence helps in faster data collection and Early Threat Detection. Machine learning combined with image processing makes it easier to detect crimes such as Human trafficking and illegal markets (Medipelly & Abosata, 2024) [5]. Still Problems like limited labeled Datasets, criminals trying to hide their activities, false positives and privacy issues to affect AI-Based systems (Ovabor et al. 2024) [6].

In the future, Focus on building strong, flexible and Ethical AI-Based systems that can work in real-time and can adjust to changing threat patterns. This study concludes that AI-Based framework are necessary to improve dark web Monitoring and for helping cybersecurity Experts and How enforcement agencies (Raman et al., 2023) [1].

## References

1. Ruiz Ródenas, J. M., Pastor-Galindo, J., & Mármol, F. G. A general and modular framework for dark web analysis. *Cluster Computing*, 27, 4687–4703. DOI: 10.1007/s10586-023-04189-2
2. Mishra, D. A., Rath, P. S., & Sahu, M. R. A Study On AI Driven Analysis Of Dark Web Marketplaces. *International Journal of Research Publication and Reviews*, 5(6), 4658–4660.
3. Shah, S., & Parast, F. K. AI-Driven Cyber Threat Intelligence Automation. *arXiv preprint*, arXiv:2410.20287.
4. Ovabor, K., Sule-Odu, I. O., Atkison, T., Fabusoro, A. T., & Benedict, J. O. AI-driven threat intelligence for real-time cybersecurity: Frameworks, tools, and future directions. *Open Access Research Journal of Science and Technology*, 12(02), 040–048. DOI: 10.53022/oarjst.2024.12.2.0135

5. Jegan R., Rajavarman, V., & Geetha, S. AI-Enhanced Dark Web Crawler for Cybersecurity Monitoring. *Tuijin Jishu/Journal of Propulsion Technology*, 45(2).
6. Dhirshal, S. J. Artificial Intelligence in Dark Web Monitoring (Chapter 14). Publication details not fully specified. DOI: 10.5281/zenodo.13329074
7. Raman, R., Nair, V. K., Nedungadi, P., Ray, I., & Achutha, K. (2023). Darkweb research: Past, present, and future trends and mapping to sustainable development goals. *Heliyon*, 9(e22269).
8. Medipelly, S., & Abosata, N.. Detection of Dark Web Threats Using Machine Learning and Image Processing.
9. Akhtar, Z. B., & Rawol, A. T. Enhancing Cybersecurity through Artificial Intelligence (AI) - Powered Security Mechanisms. *IT Journal Research and Development (ITJRD)*, 9(1). DOI: 10.25299/itjrd.2022.16852
10. Alevizos, L., & Dekker, M. Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline. *Electronics*, 13(11), 2021. DOI: 10.3390/electronics13112021