IDENTIFYING THE WAYS DARK WEB HAS EFFECTED SOCIETY AND BLACK MARKET

Siddharth Dayal 21BCY10019
Harshitaa Ashish 21BCY10123
Indrakshi Mandal 21BCY10008
Ayshath Afla 21BCY10133
TEAM NUMBER 14

October 2022

1 Abstract

The web consists of many websites which can be explored through search engines such as Google, Firefox, etc. This is known as the "surface web." The Internet is segmented further into the Deep Web, where there is content that is not indexed and cannot be accessed by a traditional search engine. The Dark Web is a huge segment of the Deep Web. It is accessible through TOR. Dark Web websites are anonymous and hidden from the user. Anonymity, privacy, and the possibility of non-detection are three factors that are provided by this special browser. In this paper, we are going to discuss and provide results about the influence of the Dark Web on different aspects of online and offline society.

2 Introduction

In terms of conceptualization, the web is a collection of accessible web sites through search engines . This content is known as "Surface Web." Another part of the Internet is the Deep Web , which refers to a class of content where, for different technical reasons, it is not indexed by search engines and we cannot access it via traditional search engines. It includes information on private networks and intranets, and sites with Query Content or Search Forms. The Deep Web also includes the Dark Web . Its content is intentionally hidden and cannot be accessed by standard web browsers . The site's publishers on the Dark Web are anonymous. Users are accessed on the Dark Web to share data with little risk and to be undetected . Anonymous user access is critical for the Dark Web, which has recently been supported by encryption tunnelling. The Dark Web content is supported by Onion Routing (TOR). It is an anonymous network, and access is by the TOR browser.

3 Related Works

Anonymity, privacy, and the possibility of non-detection are three factors that are provided by special browsers such as TOR and I2P. Beshiri et al.[1] are going to discuss and provide results on the influence of the Dark Web in different spheres of society. The social network analysis (SNA) is a topic of interest, and it is being carried out with the goal of obtaining graph-based methods that make the analysis of the network group easier by depicting the group or population strength. Therefore, cyberspace is becoming an increasingly active place for crime, terrorism, and other unlawful acts. One of the most important issues facing governments around the world is crime on the dark web. Due to the anonymity it offers thanks to specialised technologies like TOR, the dark web makes it challenging to identify offenders and follow activity. It has developed into a platform for a variety of criminal operations, including trafficking in weapons, drugs, counterfeit documents, and, most notably, terrorism. Dark Web analyses are essential for creating effective counter-terrorism policies. Sonmez et al.[9] objectives are to conduct a critical review of the literature and to show the research efforts in terrorism-related dark web studies. This part of the Internet has not yet been sufficiently investigated. Moore et al. [4] investigate how useful and informative this section of the Internet may be for crisis management. A pilot study on Puerto Rico in the months after Hurricane Maria reveals potential signs of the growth of underground markets for food, water, and prescription medications, which can have an effect on long-term recovery and reconstruction efforts when these supplies are snatched up from legitimate supply chains. Researchers and management need to pay more attention to activity in this area as more individuals use this hidden portion of the Internet. Subsequently , Mazi et al.[3] show us how the Dark Web has affected the Black Market and how it has provided an unrestricted platform for many people to trade with one another. It is much like the surface web except it's not regulated by law and it also provides anonymity and secrecy to its users. It hosts a cyber underground market like any other regular market , which is controlled by supply and demand. The use of the Dark Web and bit coins to carry out transactions makes it even harder to trace transactions. Mazi et al.[3] suggest that the government take action against the crimes conducted in the black market and that the hacking and stealing industry be destroyed. A machine with artificial intelligence (AI) can respond to, interact with, and learn from its surroundings. Rigano et al.[8] focus on how AI is being researched to help law enforcement agencies reduce the rate of criminal activity by providing it with exciting data from which it can learn from and find patterns . Rigano et al.[8] suggest how AI can be used for video analysis , DNA analysis , gunshot detection, and crime forecasting. Due to anonymity on the dark web, there has always been an interest by criminals in generating illicit revenues across borders. Rawat et al.[7] predict crime using ML (Machine Learning), CV(Computer Vision), and DL(Deep/Data Learning). Crime statistics are presented to track criminal chains and compare the comparative study with the implemented features of the given approach. Based on digital traces and evidence, security agencies can track the network. Our future research will begin with the creation of a machine that can predict and recognise patterns with geo-location coordinates and the dates of similar crimes. The goal of Rawat et al.[7] is to present the dark web crime statistics and forecasting model for generating alerts of illicit activities like drug supply, human trafficking, terrorist radicalization, and fraudulent activities that are associated with gangs or organisations showing online presence using ML and CV to assist law enforcement organisations to analyse, identify, and generate strategic techniques for solving cybercrime cases more accurately and quickly. There are large sections of the internet that are un-indexed and hidden from normal web pages . This concealed part is called the "deep web . Within the Deep Web, a subset that is mostly used for illicit purposes is the Dark Web, or Dark Net. Criminal activities and illegal content are used The associate editor coordinating the review of this manuscript and approving it for publication was Nazh et al.[5] with a percentage of 57. Steel et al.[10] state that the market for stolen identities has evolved over three generations . The first generation primarily consists of individuals. They also monitor the thefts. The second generation consisted of large-scale data breaches. It led to the creation of a free market for stolen identities. The third generation has consisted of data theft on the scale of billions of identities, which has caused the price of identities to come to an all-time low . Lacey et al.[2] talk about the growth of the dark web and how there is very little research on how the vendors and customers interact . It is observed that trust is built on the actions taken by the user instead of their identity. It ultimately develops trustworthiness to a point where engagement of new users within such forums is accepted by hosts and existing participants. To achieve this aim of analysing the dark web, the research team required access to a dark web marketplace . The marketplace and enrolment process were broken down into 3 tasks. The reviewer determines the precise nature of the trust-building requirements. Dark Web structural mining is measured as an essential portion of data analysis associated with cyber security. It is a problem that was initially proposed by Rajawat et al.[6] in the context of market basket analysis with the instruction to discover frequent cyber crime activity collections that are accepted. As a pruning approach, novel approaches are designed to explore dark web patterns created on antimonotone things. These approaches are able to solve two significant problems: classifying data accurately and reducing search space. Dark Web Structural Patterns Mining using Neural Network S3 VM for Criminal Networks has a significant role in different circumstances. It has been used in different domains, and it represents an increasing range of knowledge. Though the types of data are assorted, these data sets are contingent on the application's nature.

4 Survey

Author	**Key contribution**	**P1 - Cyber Physical Systems**	**P2 - Network Security**	**P3 - User Education and Awareness**	**P4 - Identify threats**
Beshiri et al [1]	Concluded that anonymity is not completely verifiable on the Dark Web .	NO	YES	YES	YES
Eda Sonmez et al [9]	Using and one's goal, dataset, and method for locating offenders and committing crimes there.	NO	YES	YES	YES
Kathleen et al [4]	This study looks into how useful and insightful dark web might be managing all kinds of illegal activites	YES	YES	NO	YES
Mazi et al [3]	Discusses about how the black market is now on a global platform without any restrictions	NO	YES	NO	YES
Christopher et al [8]	The paper suggest this tech will pave the way for future crime and fraud investigation.	YES	YES	YES	NO
Rawat et al [7]	Pushes for the need to create software or an authority that can act as a universal security official.	YES	YES	YES	YES
Nazah et al [5]	The paper concludes by stating technical and forensic challenges	YES	YES	YES	YES
Steel et al [10]	The paper covers all points regarding identity theft .	NO	NO	NO	YES
Lacey et al [2]	The researcher used a social experiment on large scale	YES	NO	YES	YES
Rajawat et al [6]	The paper concludes that we can try to implement a real-time scenario for criminal activity tracking using an artificial neural network .	YES	NO	NO	YES

Author	**Key contribution**	**P5 - Data leakage**	**P6 - Vulnerabilities**	**P7 - Private databases**	**P8 - Artificial intelligence /Machine Learning**
Beshiri et al [1]	Concluded that anonymity is not completely verifiable on the Dark Web .	NO	NO	YES	NO
Eda Sonmez et al [9]	Using and one's goal, dataset, and method for locating offenders and committing crimes there.	YES	YES	YES	YES
Kathleen et al [4]	This study looks into how useful and insightful dark web might be managing all kinds of illegal activites	YES	YES	NO	YES
Mazi et al [3]	Discusses about how the black market is now on a global platform without any restrictions	YES	YES	NO	NO
Christopher et al [8]	The paper suggest this tech will pave the way for future crime and fraud investigation.	YES	YES	NO	YES
Rawat et al [7]	Pushes for the need to create software or an authority that can act as a universal security official.	YES	YES	NO	YES
Nazah et al [5]	The paper concludes by stating technical and forensic challenges	NO	YES	NO	YES
Steel et al [10]	The paper covers all points regarding identity theft .	YES	YES	NO	NO
Lacey et al [2]	The researcher used a social experiment on large scale	NO	NO	YES	NO
Rajawat et al [6]	The paper concludes that we can try to implement a real-time scenario for criminal activity tracking using an artificial neural network .	YES	NO	NO	YES

5 Methodology

5.1 Background

The internet can be broadly divided into three parts: surface, deep, and dark. This review investigates and discusses the impact of the dark web and how people's privacy is affected. It has provided an unrestricted platform for many people to trade with one another. It also provides anonymity and secrecy to its users, and it hosts a cyber underground market like any other regular market, which is controlled by supply and demand. The use of the Dark Web and bit coins to carry out transactions makes it even harder to trace transactions. This study's objectives are to conduct a critical review of the literature and to show the research efforts in terrorism-related dark web studies. The study's findings suggest that further research is needed in this area and that there should be a variety of scientific techniques utilised to find and stop terrorist activity on the dark web. We also looked at the crisis study. The dark web is a crucially understudied portion of the Internet. It also investigates this section of the Internet for information and functionality useful to crisis managers. We also integrated Artificial Intelligence to help solve and reduce criminal activities, presenting the dark web crime statistics and forecasting model for generating alerts of illicit activities and identifying the types of dark web threats. Identify the methods, technologies, and applications used by law enforcement to track and detect crimes and criminals on the Dark Web. Also, we analysed how trust is created among the dark web users while maintaining their anonymity and secrecy. The goal was to try to implement a real-time scenario for criminal activity tracking using an artificial neural network in the future.

5.2 Problem statement

The black market is now on a global platform without any restrictions, which allows it to get bigger and promote more criminal activities and trade. The methods for predicting crime in detail before it occurs, or creating an "automated machine" to help police officers, remove the stress on cops while also aiding in crime prevention. The crimes committed were examined retrospectively using an ensemble model to synthesise the findings of logistic regression (LR) and neural network (NN) frameworks using the predictive analytic approach to produce weekly and monthly forecasts (based on the previous three years of cybercrime datasets) for the year [1]. Rawat et al [6] came to the conclusion that comparing weekly forecasts of monthly analysis predictions significantly enhanced the outcomes. Machine learning was used to examine crime predictions. The gathering of data, data categorization, pattern recognition, prediction, and visualisation are all part of ML-based criminal investigation. The crime data set was further analysed using boosted decision tree (BDT) and K-nearest neighbour (KNN) methods. In separate but similar research, the studies predicted crime with an accuracy of 44 percent to 39 percent, respectively. Security agencies can track the network using digital trails and proof. Our future research will begin with the development of a machine that can anticipate and identify trends in geo-located coordinated crimes and their dates. To create software that can act as a universal security official, with eyes and ears everywhere. EAST is a comprehensive method that provides researchers of the dark web an opportunity to view a system from multiple perspectives . The limitations of the task analysed in this paper should not dissuade researchers from applying EAST to a broader dark web market system. The EAST analysis presented did not incorporate the full analysis approaches utilised in other EAST assessments.

References

[1] A. S. Beshiri, A. Susuri, et al. Dark web and its impact in online anonymity and privacy: A critical analysis and review. *Journal of Computer and Communications*, 7(03):30, 2019.

[2] D. Lacey and P. M. Salmon. It's dark in there: Using systems analysis to investigate trust and engagement in dark web forums. In *International conference on engineering psychology and cognitive ergonomics*, pages 117–128. Springer, 2015.

[3] H. Mazi, F. N. Arsene, and A. M. Dissanayaka. The influence of black market activities through dark web on the economy: a survey. In *The Midwest Instruction and Computing Symposium.(MICS), Milwaukee School of Engineering and Northwestern Mutual, Milwaukee, Wisconsin*, 2020.

[4] K. Moore. Dark web, black markets: Crisis as opportunity. In *ISCRAM 2019. Proceedings*. 2019.

[5] S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan. Evolution of dark web threat analysis and detection: A systematic approach. *IEEE Access*, 8:171796–171819, 2020.

[6] A. S. Rajawat, P. Bedi, S. Goyal, S. Kautish, Z. Xihua, H. Aljuaid, and A. W. Mohamed. Dark web data classification using neural network. *Computational Intelligence and Neuroscience*, 2022, 2022.

[7] R. Rawat, S. A. AJAGBE, and A. O. Olukayode. Techniques for predicting dark web events focused on the delivery of illicit products and ordered crime. 2022.

[8] C. Rigano. Using artificial intelligence to address criminal justice needs. *National Institute of Justice Journal*, 280:1–10, 2019.

[9] E. Sönmez and K. Seçkin Codal. Terrorism in cyberspace: A critical review of dark web studies under the terrorism landscape. *Sakarya University Journal of Computer and Information Sciences*, (5), 2022.

[10] C. M. Steel. Stolen identity valuation and market evolution on the dark web. *International Journal of Cyber Criminology*, 13(1):70–83, 2019.