A Survey on Dark Web Monitoring and Corresponding Threat Detection

Imtiaaze Mahmood
ID: 012202039
Master of Science in CSE
United International University
Dhaka, Bangladesh

Md. Anisur Rahman
ID: 012202047
Master of Science in CSE
United International University
Dhaka, Bangladesh

Md. Anas Kabir
ID: 012211070
Master of Science in CSE
United International University
Dhaka, Bangladesh

Mohammad Shahriar Rahman, Phd
Associate Professor
United International University
Dhaka, Bangladesh

***Abstract*— The Web is only a segment or portion of the internet. And surface web is the most upfront segment of the web which is easily accessible through conventional search engines like Google, Yahoo or Bing. After the surface web. The Deep web starts its journey and it is unclear how much bigger is the Deep web than the surface web. Almost 96 percent is the Deep Web of WWW (World Wide Web) and a portion of the Deep Web is called the Dark Web which holds around 57 percent of illegal activities. Unlawful discussions, terrorist activities, weapons and drugs dealing, child pornography are some of the criminal activities from the Dark Web. Techniques used for locating criminals and their arranged crimes are somewhere more difficult than real-world tracing as most of them occur anonymously. The dark web was designed mainly to provide users with more privacy. But nowadays, most dark webs are built for crimes, illegal data extraction, hacking, creaking, breaking security and facing trouble to the danger of human life. So we need to monitor the dark websites, threats analysis and detection for cyber security.**

Keywords*— *Dark Web, Cyber Security, Detection, Techniques, Deep web, Privacy, TOR, Monitoring, cybercrime, Cyber Terrorism.

I. INTRODUCTION

Many people mistakenly believe that the WWW (World Wide Web) and the internet are the same things, however, they are not. The web is merely a piece of the internet. And the surface web is the most accessible part of the internet, which can be found using traditional search engines such as google, Yahoo, or Bing. Following the web's surface. The Deep Web is getting underway, and it's uncertain how much larger it is than the surface web. According to some studies, the Deep Web is 4000-5000 times greater than the surface web and is developing at an exponential rate. The Deep Web is normally inaccessible since the material is not indexed. This deep web stores information from intranets (internal networks of organizations, government agencies, and commercial reasons) as well as information that may be accessed through specific search queries or forms. [1] If we go further, we can locate a section of the dark web that is not accessible through standard search engines and instead relies on special technology or software such as TOR (The Onion Router). [2] We are going to work and research in this place on the internet.

Dark Web monitoring is an approach to detect crimes and criminal activities with finding out illegal extraction. It provides secured privacy of the web but nowadays the Dark Web is hampered by many hackers, crackers and intruders. So, Dark Web Monitoring is an important step.

A. Background

Army researchers in the United States invented the dark webs in the middle of the 1990s. Intelligence personnel used the technology that sealed the mechanism for what is now known as the deep webs to transfer files anonymously. 'Tor,' also known as 'The Onion Router,' was the name of the first platform. Tor enlists our participation in a cyber-security network that conceals our identity when we surf the web, share material, and engage in other online activities. Tor is integrated in hidden word clients that are accessible through The Onion Router, and it encrypts all information transferred from our laptop so that nobody can see UN agencies or wherever we are, even while we are signed into a website. It was developed by the US military research laboratory in the 1990s.

Illicit darknet markets have grown more accessible as a result of the increased usage of anonymization technologies. Bitcoin was widely embraced as a payment option in black marketplaces after its introduction in 2009. The Silk Road market, an onion website that provides a platform for buying and selling illegal goods (mainly narcotics), began operating via the Tor network in 2011, using Bitcoin as its principal payment mechanism (although today the use of privacy coins, such as Monero and Ethereum is increasing). Silk Road was the first time these technologies were coupled to allow a major increase in the size of an online market for illicit goods. These marketplaces haven't created new technology; instead, they've blended a variety of advancements to provide new benefits to both vendors and consumers.

We should adopt certain measures that are absolutely applicable to the identification and prevention of cybercrime since this is a basic topic about cybercrime. Some tools and approaches based on networks, hardware, and memory can be used for this goal, allowing for a better output of the data and a clearer comprehension.

In Fig:1, The levels of the surface web, deep web, and black web are clearly delineated for better comprehension and to eliminate any potential for misunderstanding while researching. Clear notions of multiple layers can open up new avenues for the development of new technologies. In Fig:1, The levels of the surface web, deep web, and black web are clearly delineated for better comprehension and to eliminate

any potential for misunderstanding while researching. Clear notions of multiple layers can open up new avenues for the development of new technologies.

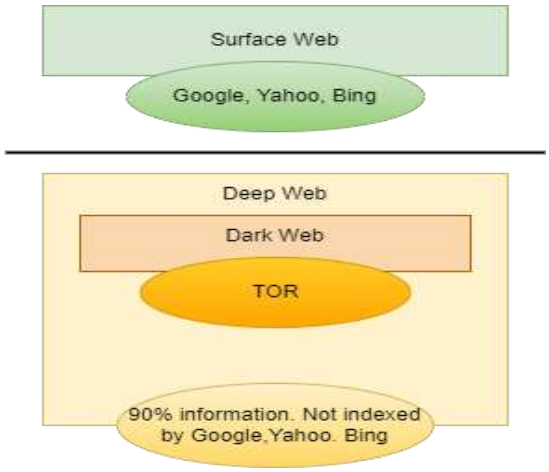

Fig-1: Overview of Surface Web, Deep Web and Dark Web

B. Problem

The dark web was designed mainly to provide users with more privacy. Nowadays, most dark webs are built for crimes, illegal data extraction, hacking, breaking security and facing trouble and danger to human life. So we need to monitor the dark website threat analysis and criminals detection for cyber security. Dark Web is a specific platform that can be accessed by specific tools and procedures. It provides security and protects our web privacy with safeguards.

We will discuss Dark Web monitoring and criminal detection techniques in a way that when other researchers or reviewers want to work on this aspect, they can get a comprehensive idea.

The likelihood of dark web-related crimes is increasing by the day. On the dark web, massive marketplaces are emerging. Some are for noble causes and legitimate enterprises, while others are for illegal activity. The major goal of this study is to show several methods and apps for detecting distinct dark web dangers in order to conduct additional forensic investigations. A summary of all strategies can be extremely useful to investigators who are already conducting or planning procedures.

C. Our Contribution

1. Comprehensive discussion on Dark Web and Dark Web Monitoring
2. Discussion on available threats and target places.
3. Categorizing techniques
4. Possibly a taxonomy on detection techniques

II. RELATED WORKS

Cybercrime is similar to real-life crime in certain ways and may cause chaos in people's lives, S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan gave a thorough examination of detecting approaches, as well as their extracted studies from implementations. We discovered several huge illicit operations that are still going on. [5]

On the dark web, we discovered several ongoing large criminal activities. Human trafficking, pornography, assassination-based marketing, drug-related transactions, child pornography, terrorism-related crimes, stolen data marketplaces, as well as venues for cybercrime tools and currency exchange concerns.[3,4]

This key reference comes up with remedies in two separate approaches after describing the primary challenges and problems. The first is locating offenders on the dark web, and the second is detecting crimes. [5]

Proxying, information leakage, onion routing, torture, bitcoin fraud, and cyber assaults such as correlation attack, congestion attack, session hijacking, and man in the middle attack, Cross-Site Scripting, Phishing, SQL Injection, and so on were mentioned by Kaur, Shubhdeep, and Randhawa. We've left out the assaults that were frequent in earlier research. Only preventative strategies for various sorts of cyber assaults were provided by the writers. [6]

Some strategies with suitable tool implementation are required to detect dark web dangers and crimes. A collection of tools and their targeted aims with their target systems are briefly described to have a better knowledge of the existing tools and their application to identify dark web threats. [7]

Table-1: Some more Literature Reviews

SL	Ref. No.	Authors/ Year	Work
A	6	Surya Kusuma, Ridho, 2021	Network forensics Dark Web networking Trigger, Acquire, Analysis
B	7	Basheer, Randa & Alkhatib, Bassel.	TOR Establishment, Networks Forensics using Wireshark, Anomaly Detection using Wireshark tools.
C	2	Tavabi, Nazgol & Bartley, Nathan & Abeliuk (2019)	Discovered several ongoing large criminal activity as well as venues for cybercrime tools and currency exchange concerns

In this paper, the authors proposed a novel crawling system for collecting Dark Web forum content. To gain access to Dark Web forums, the system employs a human-assisted accessibility approach. Several URL ordering features and techniques enable efficient forum posting extraction. The system also includes an incremental crawler and a recall-improvement mechanism to aid in the retrieval and updating of collected content. Experiments to assess the efficacy of the human-assisted accessibility approach and the recall-improvement-based, incremental-update procedure produced positive results. The human-assisted approach improved access to Dark Web forums significantly, while the incremental crawler with recall improvement outperformed standard periodic- and incremental-update approaches. Using

the system, we were able to collect over 100 Dark Web forums from three different regions.[15]

III. METHODOLOGY

This section discusses the steps taken to arrange and display the works on a given topic. This will also include, if necessary, selection criteria, approach categories, technique kinds, and research questions.

A. Selection Criteria

First, we determine the search terms that will be utilized to find material for our review article. When searching, the 'AND' and 'OR' syntax are utilized. 'AND' denotes the word that was most likely used in the search, while 'OR' denotes any of the words that can be picked from the list of terms.

Table-2: Searching by Keywords

Serial	Search Keywords
1	"Dark Web" OR "Dark Net" OR "Deep Web"
2	"Dark Web" AND "Cyber" OR "Threats" OR "Crimes"
3	"Dark Web" AND "Monitoring"
4	"Dark Web" AND "Cyber Crime Detection" AND "Techniques"
5	"Challenges" AND "Dark Web"

Several criteria for inclusion and exclusion were chosen. We choose the criteria based on availability, best techniques, better output, and overall, which make working on this issue simpler for us. The exclusion criteria helped us save time and increase our focus on the task at hand.

Table-3: Inclusion and Exclusion Criteria

Inclusion	Exclusion
Focused on Dark Web based explanations	Duplicate articles
Based on Dark Web Threat Detection techniques	Exclude the articles which are not Dark Web Cyber Crimes
Studies must be in English language	Excludes the studies on only cyber crimes
Articles or data must be from after 2000 and till present	Excludes the studies which only discusses web forums but not Dark Web forums

We'll start by looking into dark web-related difficulties. These problems may be seen from two distinct angles. One is predicated on criminal activity, whereas the other is not. From the standpoint of a criminal, there are several concerns. The anonymity of the corresponding offenders is the most crucial factor. When criminals commit crimes through the dark net, they have the option of remaining invisible in some way. As a result, it's a big deal when it comes to enforcing laws or working with field investigators. Then there's the classification of offenses. These include things like human trafficking, pornography, assassination-based marketing, various sorts of cyber-attacks, bitcoin money exchange, and so on.

As long as there are issues, there will be solutions. The solution can be portrayed in three different dimensions. One option is to use pre-existing solutions. Proper law enforcement is one current answer. There are also various more options, such as employing social media, DARPA and MEMEX, bitcoin flow, MLAT, and so on. The technologies that can be employed for crime and criminal detection are another sort of solution. These technologies are being studied and might be used in conjunction with existing solutions to provide more precise results. The final type of approach is to employ tools. In the dark web, several tools may be used to identify criminality and illicit information. Capturing RAM, relative database identification, and network analysis are all things that these technologies may aid with.

B. Approaching Process

As this is a review paper, the emphasis will be on theory, but some techniques will be illustrated with diagrams and flowcharts. For a better understanding, a detailed overview of various recent and continuing methods will be shown. This review will be divided into two categories:

1. Dark web criminal detection methods and approaches.
2. Dark web crime detection methods and procedures.

B. Research Techniques

We will follow some techniques in our way of research. Those are:

1. Propagating based on law enforcement and social network awareness
2. Recently researched methods for detecting criminals and crimes in dark web
3. Organized summary of some available tools and their usages

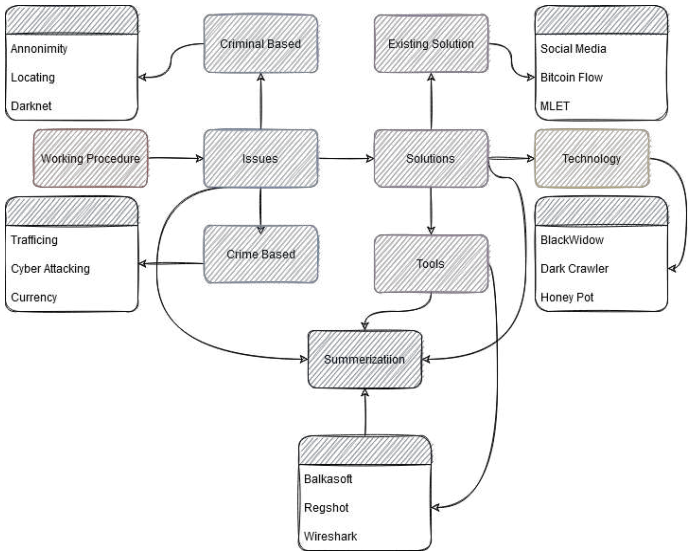

Fig 2: Working Procedure

C. Research Questions

We will answer some research questions at the end of our work.

1. What are the procedures to detect criminals on the dark web?

2. What are the regular places for dark web crime arrangements?
3. Is there any way to find and locate criminals and crimes from the surface web?

IV.Dark Web Monitoring

Dark Web monitoring is an approach to detect crimes and criminal activities by finding out about illegal extraction. It provides secured privacy of the web but nowadays the Dark Web is hampered by many hackers, crackers and intruders. Dark Web monitoring is a very important step in cyber security.

A.Hidden Service Analysis

It is useful to identify content hosted by hidden services in order to determine the nature of the dark Web. This classification includes analyzing the content of each hidden service and categorizing the information accordingly. chose to classify hidden services rather than utilize automated techniques. Manual classification, on the other hand, was tedious because there were over 6,000 HTML files to filter through. We expected, however, that manual classification would be more effective than any computer classifier's results.
Additionally, the deep Web offered a varied number of topics, including journals and supporter forums, which demanded a thorough assessment in order to appropriately classify them.

During the classification process, we discovered hidden services that did not fit into any of the categories and had to be eliminated. The following were among the reasons for dismissal:

A) Three or fewer words are used in the text.
B) hidden service may return an error, such as a server configuration error.
C) Errors in the database, client-side scripts, and so on.
D) There was only an image with no supporting information.
E) Web pages that are empty or blank. Sites with redirection links, and so on.

We discovered a total of 2,125 hidden services. After removal, the dataset contained 4,102 hidden services for classification out of a total of 6,227. 3,480 of the 4,102 covert services were in English, whereas 622 were not.

The contents of websites are hashed and saved in databases using popular hashing methods. Authorities and law enforcement agencies review this information for future investigations, and then geodata is retrieved from WhoIS and utilized to hunt down specific crimes among the recorded data. [8]

Table 4: Tor Hidden Services Categories with English content.[12]

Adult Content	Electronics	Cryptocurrency
Bitcoin doubling	Ethical hacking	Personal Websites
Bitcoin mixer	Forged documents	Political
Bitcoin trading	Forums & others	Religious
Bitcoin wallets	Gambling-betting	Services
Books	Hosting	Software
CC dumps & others	Login	Tor
Counterfeits	Marketplace	Uncensored journalism
Directory	Music-entertainment	Violence
Drugs	News	Whistleblowers
Study	Illegal	Legal

B. Bitcoin in Dark Web

Bitcoin is referred to as a cryptocurrency since it's a decentralized payment system that uses cryptography for authentication, transfer, and creation (usually elliptic curve cryptography, such as SHA-256). As a result, it's commonly used on the dark web as a method of anonymous (at least in theory) payment for unlawful items.
Many of the most prominent dark websites are referred to as "darknet markets" because they offer things that are frequently illegal and virtually always use bitcoin or other cryptocurrencies (like Monero). Dream Market, Wall Street Market, CGMC, and Point/Tochka Market are just a handful of the markets that are hosted on Tor. Bitcoin was also used by AlphaBay Market and Hansa Market, which were recently caught by law authorities. Although it varies per market, most consumers create a bitcoin wallet, either on the site itself or separately, on a site such as Electrum. When purchasing items, users will choose what they want on the website and then transfer bitcoin to the vendor via the website's payment mechanism. This varies a lot from site to site, since many have different verification processes in place to prevent scammers - but the bitcoin should always wind up in the hands of the vendor. Most darknet markets, for example, are either escrow or multisig markets. The bitcoins are held in escrow until the transaction is completed on an escrow market to ensure that everyone keeps their end of the bargain. The term "multisig" refers to a transaction that requires more than one cryptographic key to complete. A third option is to "finalize early," or "FE," which means that bitcoins are given to the vendor without being verified first Peer-to-peer (P2P) transactions are also supported on some sites, but without all of the precautions in place, such as two-factor authentication. This usually entails a direct bitcoin transfer from the buyer to the vendor, which is much riskier due to the lack of an

authentication system. Markets may also reward vendors for suggesting new customers and/or sellers, in which case their rewards will be increased. The key distinction is the types of items being offered, which is similar to referral networks used by legal firms. Regardless, bitcoin is utilized on sites other than the major exchanges, although it is mostly used on them. Some of the smaller websites that purport to sell goods and services have turned out to be cunning con artists. I can think of another way it's been used in a scam context - I've come across a number of sites claiming to "double your bitcoin." These are, without a doubt, scams as well. They sound too good to be true, and they're similar to hanging bait in front of a fish (thus the word "phishing"). P.S. To my understanding, the stories concerning human skin and "hitmen" are either urban legends or frauds. Furthermore, human skin is available for purchase on the Clearnet.

C. *Use of Onion Router in Dark web*

Because of Tor browser's access is naturally limited to websites served as Tor hidden services, it can't access much of the black web. Accessing dark web pages hosted on alternate darknets necessitates special network configuration and software. The bulk of black websites are protected by virtual private networks, to which only authorized users have access. Because most dark websites are not promoted to the general public, passing background checks and taking work where you have a "need to know" is the quickest approach to gain trust. To acquire verified access, you'll need to show proof of identity and be informed how to visit numerous dark websites controlled by others. To see site contents whose hostname is unresolvable with canonical network configuration, you may only need to use an alternative DNS root or add an entry to your hosts' file.

D. Monitoring Challenges

1. Acquisition of Target Forum

The first challenge is determining which target forums are relevant to our operation, i.e. those with users and information related to cyber counterintelligence. When combined with the previously noted fact that 87% of dark internet sites do not link to other dark internet sites, we can conclude that the dark internet is more of a collection of isolated short-lived silos than the traditional internet, which has a clear and stable graph structure. On the dark internet, there are more than just loose and sometimes out-of-date collections of URLs (both from the surface internet and Tor Hidden Services). To combat this problem, a totally automated technique is impracticable, hence a semi-manual approach must be utilized at first.[8]

2. Resources of Scalability

A Scalability Resource component that made our resources more challenging was the habit of sampling a large number of the most important online forums that were accessible without this notice, allowing us to collect and analyze data without having to manually evade such security measures. However, because we've come across a few of these forums (or sections of forums), our approach may naturally be applied to them, though this would necessitate significant manual resource effort.[10]

3. Real-Time Data Extraction

The focus of Real-Time Data Extraction is on the challenges posed by the nature of a time period data extraction approach. Previous research has gathered information from the ark web for analytical purposes, but it has been done in a static environment. Time period capability may be a critical requirement for the system's long-term utility, given the target forum typically has short lifespans. From data collection to live data analysis, a high level of automation is required to support these functionalities.[8][10]

4.TOR Browser Forensics

Tor Browser routes all of your internet traffic via the Tor network. Tor is a three-layer proxy, similar to layers of an onion (Tor Browser connects haphazardly to the public listed entry nodes, bounces that traffic through an at the randomly chosen middle relay, and eventually spits out your traffic through the third and final exit node). As a result, don't be surprised if Google or another service greets you in a language you don't understand but when we use Tor, around the world. The Tor network routes all types of TCP traffic but is optimized for web browsing.[12]

V. Dark Web Criminal Detection

Cyber attackers abound on the surface and on dark webs. Criminals on the dark web are more vulnerable because they are less focused and tracked on the internet in general. As a result, some steps can be taken to make the dark web safer and more reliable in some ways, such as detecting dark web criminals and, if possible, their locations.

A. Law Enforcement

The problem of law enforcement for dark web offenders is critical. To make criminals less active in the dark web sector, civil and regular laws must be appropriately applied. Because minor investigative organizations are unable to prosecute these offenders, they must be seen in a larger context. Agencies within a jurisdiction have the authority to enforce laws against criminals in a controlled manner. They can entail penalties and punishments ranging from minor to death, depending on the severity of the offense. Criminals can be identified and deterred from committing more crimes if laws are properly implemented.

B. Social Media

Criminals can be tracked down through social media. Criminals successfully use both social media and the dark web for their crimes. Facebook. Criminals frequently utilize social media platforms such as Twitter, SnapChat, Instagram, and WhatsApp to carry out their nefarious acts. On the dark web, crimes such as stealing logical items and using them on surface online platforms for real-world gain are occasionally committed. Many offenders have lately been apprehended as a result of their actions on social media.

C. DARPA and MEMEX

DARPA is Defense Advanced Projects Research Agency. DARPA has selected several tools on the market which are available to help finding individuals who are responsible for criminal activities in dark web. One of them is Metasploit Decloaking Engine which was used by FBI for enhancing their investigation on dark web. This Metasploit Decloaking

Engine and MEMEX are combinedly used for indexing deep websites for identifying criminals or the human traffickers in dark web.

D. Bitcoin Flow

Bitcoin is a virtual currency used by criminals on the dark web to conduct illegal activities. So the dark web, where the bit currency movement is unregulated, is an excellent place to look for criminals and track them down. The law enforcement authorities exploit this bitcoin flow to track down persons. The Silk Road Server is one example that may be shown here.

E. MLAT

MLAT is Mutual Legal Assistance Team. This MLAT helps law agencies to apply law over the borders with set of rules and laws. If one country needs information which are on other borders then MLAT helps with the seeking problem to get to access to digital evidence. MLAT is protecting the legal rights of people throughout the borders.

VI. Dark Web Crime Detection

A. Black Widow

Blackwidow is an automated process for detecting illegal activity on the dark web, particularly on dark web forums. Manual work will only be done in Blackwidow while integrating and initializing the targeted forums. Other processes, on the other hand, are heavily automated.

B. Dark Crawler

A 'Dark Crawler' was developed based on CENE (Child Exploitation Network Extractor) which was mainly developed on exploitation materials based on children. CENE was successful in finding child exploitation materials like images, videos, and other activities.

Dark Crawler was enhanced and had access to TOR but it was also accessed in the public internet at the same time. The websites in TOR were automatically searched by dark crawler according to the keyword. After finding the keyword matched data it was able to store data in database with TOR network based pre-defined keywords.

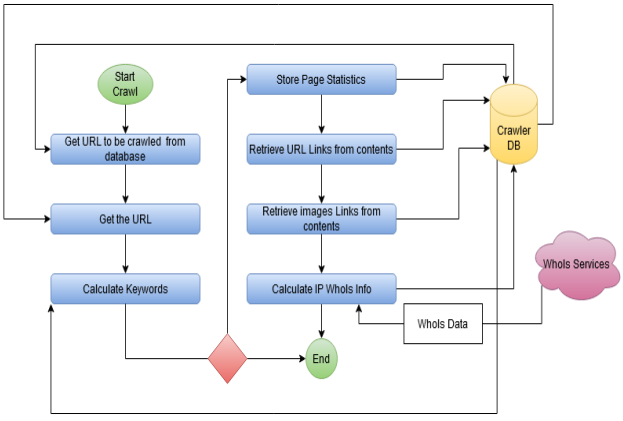

Fig 3: A thread of Dark Crawler

The contents found in websites are hashed using common hashing algorithms and stored in database. This information are checked by authorities and law agencies for future investigations and then geodata is retrieved from WhoIS and used for tracking down the selective crimes among the stored information.

Network analysis is a step used for detecting crimes as it can come up with entry and exit nodes for crimes. Continued monitoring Dark Web is beneficial to maintain Dark Web criminal activities controlled.

Honeypot Deployment and Tripware implementations can be very effective measure to keep balance in Dark Web crimes and their traceability [8]. Anomaly Detection Techniques are used for preventing security breaches and as well as attacks. Intrusion detection methods plays a great role for in case of prevention.

Other ways for detecting crimes on the dark web are included below.

MD5, SHA-1, SHA-256, SHA-512, and other hash algorithms are widely employed. The originality of investigations is preserved by the values created by hash functions. Sock Puppet detection is another important and crucial method for recovering identities. Network analysis is a method for detecting crimes since it can identify crime entry and exit nodes.

Table 5: Survey paper Comparison

RF	Year	RQ	Monitoring Technique	Detection Technique
[13]	2016	N	N	Y
[12]	2019	N	Y	Y
[3]	2019	N	N	Y
[8]	2021	N	Y	Y
[27]	2012	N	Y	Y
[16]	2010	N	Y	N
[7]	2021	N	Y	Y
[18]	2010	N	Y	Y
[10]	2010	N	Y	N
[9]	2016	N	Y	Y
[21]	2006	N	Y	Y
[22]	2017	N	N	Y
[29]	2018	N	Y	Y
[24]	2017	Y	N	N
[15]	2006	N	N	N
[30]	2019	N	Y	Y
Our Paper		Y	Y	Y

VII. TAXONOMY

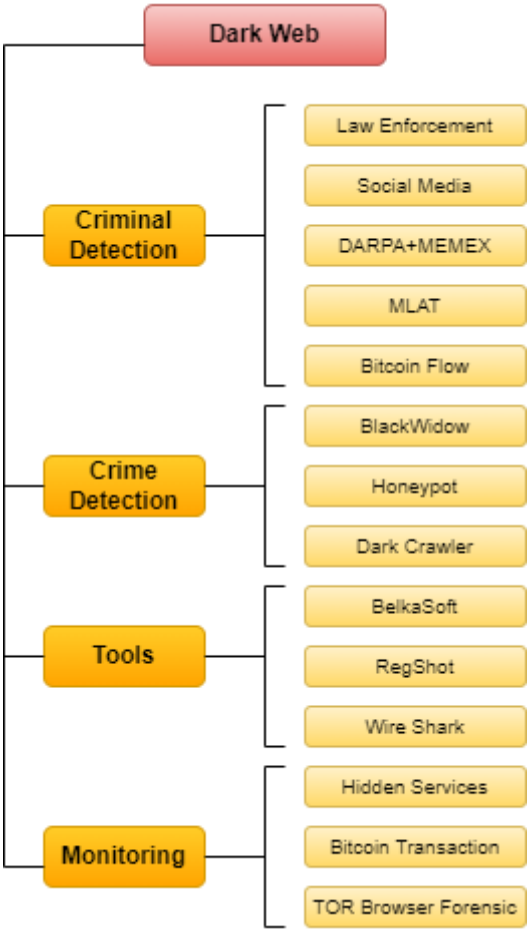

Fig 4: Taxonomy

VIII FUTURE PLAN

Analysis More personal data on the dark web, full-filled dark net market study challenges, bitcoin/crypto-currency's widespread adoption are some of the future working scopes. As WHOIS revoke the availability of information's, We would like to improve dark crawler replacing WHOIS with several databases to detect and prevent crimes.

. IX CONCLUSION

The dark web is a section of the internet that can only be accessed with specialized browser software like Tor. It's a web of anonymity in which users' names and locations are shielded by encryption technology that passes data through several servers around the world, making tracking individuals extremely difficult.

The dark web's obscurity makes it an appealing technology for criminal activities. Unfortunately, acquiring awareness of illicit locations is challenging: it necessitates specialized knowledge, access to closed sources, and equipment capable of monitoring these sources for data misuse.

With the purpose of offering guidance and aspects of rising criminal threats in the Dark Web to researchers and specialists in the cyber security industry, we used the Systematic Literature Review (SLR) technique. For this SLR with TOR Browser Forensics, we selected the most relevant papers from top dark web resources for data extraction and synthesis to answer our defined research questions.

Our paper reviewed dark web detection, Tor browser forensics, dark web monitoring and has also discussed Dark Web challenges, dark web taxonomy which includes necessary constraints dark web monitoring, criminal detection, crime detection and criminal detection techniques in a way that when other research papers or review papers want to work on this aspect, they can get a comprehensive idea.

REFERENCES

1. [url=https://digital.library.unt.edu/ark:/67531/metadc700882/]Dark Web[/url] hosted by [url=https://texashistory.unt.edu/] The Portal to Texas History[/url]
2. Tavabi, Nazgol & Bartley, Nathan & Abeliuk, Andres & Soni, Sandeep & Ferrara, Emilio & Lerman, Kristina. (2019). Characterizing Activity on the Deep and Dark Web
3. Hsinchun Chen & Wingyan Chung & Jialun Qin & Edna Reid & Marc Sageman & Gabriel Weimann, 2008. "Uncovering the dark Web: A case study of Jihad on the Web," Journal of the American Society for Information Science and Technology,Association for Information Science & Technology, vol. 59(8), pages 1347-1359, June.K. Elissa, "Title of paper if known," unpublished.
4. S. NAZAH, S. HUDA, J. ABAWAJY AND M. M.HASSAN, "EVOLUTION OF DARK WEB THREAT ANALYSIS AND DETECTION: A SYSTEMATIC APPROACH," IN IEEE ACCESS, VOL. 8, PP. 171796-171819,2020, DOI:10.1109/ACCESS.2020.3024198.
5. Kaur, Shubhdeep & Randhawa, Sukhchandan.(2020). Dark Web: A Web of Crimes. Wireless Personal Communications. 112. 10.1007/s11277-020-07143-2
6. Surya Kusuma, Ridho et al. "Network Forensics Against Ryuk Ransomware Using Trigger, Acquire, Analysis, Report, and Action (TAARA) Method." (2021).
7. Basheer, Randa & Alkhatib, Bassel. (2021). Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. Journal of Computer Networks and Communications. 2021. 1-21. 10.1155/2021/1302999.
8. https://www.unodc.org/roseap//en/2021/02/darknet-cybercrime-southeast-asia/story.html
9. https://firstmonday.org/ojs/index.php/fm/article/download/9473/7794#author
10. M. Schäfer, M. Fuchs, M. Strohmeier, M. Engel, M. Liechti and V. Lenders, "BlackWidow: Monitoring the Dark Web for Cyber Security Information," 2019 11th International Conference on Cyber Conflict (CyCon), 2019, pp. 1-21, doi: 10.23919/CYCON.2019.8756845.
11. A. Nursetyo, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto and C. A. Sari, "Website and Network Security Techniques against Brute Force Attacks using Honeypot," 2019 Fourth International Conference on Informatics and Computing (ICIC), 2019, pp. 1-6, doi: 10.1109/ICIC47613.2019.8985686
12. A. T. Zulkarnine, R. Frank, B. Monk, J. Mitchell and G. Davies, "Surfacing collaborated networks in dark web to find illicit and criminal content," 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 2016, pp. 109-114, doi: 10.1109/ISI.2016.7745452
13. [url=https://digital.library.unt.edu/ark:/67531/metadc700882/]Dark Web[/url] hosted by [url=//texashistory.unt.edu/]The Portal to Texas History[/url]

14. Fu, Tianjun & Abbasi, Ahmed & Chen, Hsiu-chin. (2010). A Focused Crawler for Dark Web Forums. JASIST. 61. 1213-1231. 10.1002/asi.21323.

15. Yang, Christopher & Tang, Xuning & Thuraisingham, Bhavani. (2010). An analysis of user influence ranking algorithms on Dark Web forums. 10. 10.1145/1938606.1938616

16. Park, Andrew & Beck, Brian & Fletche, Darrick & Lam, Patrick & Tsang, Herbert. (2016). Temporal Analysis of Radical Dark Web Forum Users. 10.1109/ASONAM.2016.7752341.

17. Rawat, Romil and Kumar, Anil and TELANG, SHRIKANT and Pachlasiya, Kiran and Garg, Bhagwati and Mahor, Vinod and Chouhan, Mukesh, Systematic literature Review (SLR) on Social Media and the Digital Transformation of Drug Trafficking on Darkweb (August 12, 2021). AIBM - 2nd International Conference on "Methods and Applications of Artificial Intelligence and Machine Learning In Heterogeneous Brains" 2021 [September 4-6, 2021], Available at SSRN: https://ssrn.com/abstract=3903797 or http://dx.doi.org/10.2139/ssrn.3903797

18. Al Nabki, Wesam & Fidalgo, Eduardo & Alegre, Enrique & Paz, Ivan. (2017). Classifying Illegal Activities on Tor Network Based on Web Textual Contents. 35-43. 10.18653/v1/E17-1004

19. Arnold, Nolan & Ebrahimi, Mohammadreza & Zhang, Ning & Lazarine, Ben & Patton, Mark & Samtani, Sagar. (2019). Dark-Net Ecosystem Cyber-Threat Intelligence (CTI) Tool. 92-97. 10.1109/ISI.2019.8823501

20. M. Bailey, E. Cooke, F. Jahanian, A. Myrick, and S. Sinha, ``Practical darknet measurement," presented at the 40th Annu. Conf. Inf. Sci. Syst.,Mar. 2006.

21. Lightfoot, Summer. (2017). Surveillance and privacy on the deep web. 10.13140/RG.2.2.21692.74889

22. Hayes, Darren & Cappa, Francesco & Cardon, James. (2018). A Framework for More Effective Dark Web Marketplace Investigations. Information (Switzerland). 9. 186. 10.3390/info9080186

23. Eimer, Thomas & Luimers, Jorrit. (2019). Onion governance: Securing drug transactions in dark net market platforms.

24. Alkhatib, Bassel & Basheer, Randa. (2019). Mining the Dark Web: A Novel Approach for Placing a Dark Website under Investigation. International Journal of Modern Education and Computer Science. 11. 10.5815/ijmecs.2019.10.01.

25. Coffey, Mollie. (2020). Library application of Deep Web and Dark Web technologies. SLIS Student Research Journal. 10. 10.31979/2575-2499.100108.

26. C. Fachkha, E. Bou-Harb, A. Boukhtouta, S. Dinh, F. Iqbal and M. Debbabi, "Investigating the dark cyberspace: Profiling, threat-based analysis and correlation," 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), 2012, pp. 1-8, doi: 10.1109/CRISIS.2012.6378947.

27. Michael L. Brodie. 2003. Illuminating the dark side of web services. In Proceedings of the 29th international conference on Very large data bases - Volume 29 (VLDB '03). VLDB Endowment, 1046–1049.

28. L. Liu, O. De Vel, Q. -L. Han, J. Zhang and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," in IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1397-1417, Secondquarter 2018, doi: 10.1109/COMST.2018.2800740.

29. N. Arnold et al., "Dark-Net Ecosystem Cyber-Threat Intelligence (CTI) Tool," 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), 2019, pp. 92-97, doi: 10.1109/ISI.2019.8823501.

30. Iliou, Christos, 2017, Adaptive detection evasion techniques for terrorism-related information gathering on the surface and dark web, Available at: http://hdl.handle.net/11544/15220, [Accessed June 1, 2022].