Dark Web Markets and Their Role in Facilitating Child Trafficking: A Review

Khatri Renuka[1], John Judy Joana Catherine[2], Panchia Rupli[3], Sivakoti Divya Sai Lakshmi[4], Manishi Shriwas[5], D. Naga Jogayya Kothakota[6]

[1,2,3,4]*Undergraduate student, Department of Forensic Science, Centurion University of Technology and Management, Andhra Pradesh*

[5]*Faculty, Department of Forensic Science, Centurion University of Technology and Management, Vizianagaram.*

[6]*Associate Professor & Head of Department*

[6]*Department of Forensic Science Centurion University of Technology and Management, Andhra Pradesh-*

***Abstract*—Digital technologies have transformed the field of communication in a radical way, but they also allow carrying out new kinds of criminal exploitation. One of the most serious risks is the development of child trafficking with the help of the dark web a localized, encrypted, and anonymized part of the internet that is intended to hide the identity and activity of its users. The study analyses the use of the tools by traffickers to run child sexual abuse content (CSAM), participate in live-streamed abuse, and arrange illicit transactions of children. Some of the operational measures adopted by the perpetrators which are pointed out in the study include the grooming on social media, transfer into encrypted platforms and non-tracible payment in cryptocurrencies. Furthermore, the paper describes the changing environment in terms of the decentralized networks, content created with the use of AI, and the introduction of new, closed by invitation platforms that provide a challenge to traditional methods of investigations. Although the international fight against it--using organizations such as INTERPOL and Europol--has led to significant take-down of sites such as Welcome to Video and Boystown, new sites always arise, usually more advanced. This paper also examines why modern methods of policing are inadequate, what ethical issues are involved in the surveillance program as well as the mental strain that investigators undergo. In future countermeasures, promising developments are discussed by means of AI-based detection tools and blockchain analysis. Nonetheless, the lack of cohesive legal systems and understaffed organizations makes global response unfavourable. Based on the findings of this paper, it can be inferred that a multi-disciplinary, cross-border, and technologically responsive strategy is vital in dealing with the dark web facilitated child trafficking.**

***Index Terms*—Artificial Intelligence (AI), Child Sexual Abuse Material (CSAM), Cryptocurrency, Dark Web, Encrypted Communication.**

I. INTRODUCTION

The modern digital age has changed the world of communication, trade, and the transfer of information through technological breakthroughs. Nevertheless, together with these advantages, the same technologies have resulted in new susceptibilities and criminal vulnerabilities (Yustisia, et.al, 2023). Child trafficking is one of the most worrying and highly intricate crimes conducted with the help of modern digital tools. Child trafficking is considered by the rest of the world as a flagrant abuse of human rights, with millions of children being trafficked annually. Although the given phenomenon is not new, the recent combination of it with the anonymizing technologies and encrypted platforms, especially, the ones active on the dark web, introduced a new degree of complexity to not only commit the given crime, but to prevent it as well. The dark web is a hidden part of the internet that is not indexed by popular search engines and can be accessed with the help of special programs, including Tor (The Onion Router) or I2P (Invisible Internet Project), created in order to enhance the privacy and freedom of speech of the user (Elangovan, et.al,2020). In present times, however, it has become one of the driving forces behind diverse organized crimes such as drug trading, weapons trading, as well as human trafficking and exploitation. Among them, the issue of child

trafficking stands in the spotlight because of the significant impact it has on ethics, law, as well as social aspects of the process. Such dark web sites enable traffickers to gain privacy and a decentralized system to avoid police, as well as allow the exploitative services and materials to be available in every corner of the globe. This has led to the fact that now these dark webs have turned into the major vectors of sale, exploitation, and abuse of children. Dark web child trafficking takes a variety of forms, including the distribution of child sex abuse material (CSAM) to live-streamed abuse, illicit arranged adoption services, and online markets of sexual exploitation or labor. Most victims are usually lured via social media that is popular than channeled into networks that are developed under layers of encryption.

The dark web has forums and marketplaces which traffickers can use to promote children to be abused, share CSAM, and secure trade logistics, easily accessing cryptocurrencies like Bitcoin or Monero to secure the trades in a manner that law enforcement struggles to track (El-Kady, et.al,2025). Such sites can be membership-based based whereby a user has to pay to have access to illegal goods or services, thus forming a dark economic system that enjoys exploitation. These criminal operations have been sophisticated and large, as seen in several notable cases. As an example, the shutting down of sites such as Welcome to Video, which held over 250,000 videos of abuse, and which was viewed by citizens of more than 100 countries, illustrated how well integrated and networked such systems have become. In a similar operation, the major, and extremely well-established, dark web bulletin board (Boystown) based on the exploitation of young males was shut down in a cross-national police sting, with law enforcement agencies in Germany, the Netherlands, and Australia having participated. These examples add to the fact that the threat is international as well as the immense difficulty in recognizing the perpetrators and saving the victims. Their nature is also an indication of the lack of innocence of the dark web with the dark web but a participant in the illicit exchange of ideas, again, an ongoing abuse and trafficking of children. The charm of the dark web with traffickers lies in its structural benefits. Through the dark web, the digital footprint is largely impossible to track, unlike the surface web, where the footprints can be tracked in most cases. Traffickers use these technical controls to evade monitoring, deal in pseudo-identities, and engage in business without any possible evidence to act upon. Accounting of funds is further complicated by the usage of privacy-concerned cryptocurrencies, whose identity of senders/recipients of funds and transaction history are concealed, which makes financial investigations even harder (Raghu Raman, et.al,2023). Additionally, dark web markets commonly introduce user verification procedures, reputation-based models, and two-factor authorization to guarantee that only trusted members can access the market, as they did with the older established organized crime networks, except that this was made to suit digital needs (Wang, et.al,2024). As awareness of the problem increased, the responses to fighting child trafficking through the dark web are mostly sporadic and scattered. Among the main difficulties is the existence of technological disparity between criminals and law enforcement and regulatory bodies. Traffickers are frequently among the first to take advantage of privacy-enhancing technology, and many law enforcement and investigative agencies, especially those located in low-resource countries, have neither the tools nor expertise to deal effectively with cybercriminals nor jurisdiction to act across international boundaries. There are further jurisdictional constraints because the jurisdiction of laws on digital evidence, encryption, and cybercrime is very diverse across countries. This does not harmonize law at the international level and makes international cooperation difficult, enhances delays in the investigation of cases, and may even cause cases to be dismissed on procedural grounds. In addition, the enforcement strategies are complicated by ethical and legal issues. Surveillance instruments, honeypots, and data mining methods based on AI could bring up the issue of the right, entrapment, and due process. Meanwhile, the fact that child exploitation should be prevented instigates more radical measures, but where is the border between effective police business and going overboard when catching criminals? There is also a great psychological danger to the investigators involved in collecting, storing, and analyzing sensitive materials like CSAM, and it requires specific procedures that should be followed to avoid abuse or any secondary victimization that may arise. However, progress has been made towards invalidating these threats. Cybercrime emphasis by international bodies like

INTERPOL, Europol, and the United Nations Office on Drugs and Crime (UNODC) on child trafficking has been so pronounced, with multi-national investigations usually being coordinated by them as well as providing technical support to member countries. Social entrepreneurship in the form of technology companies, bank groups, and child protection NGOs has also formed another useful tool to track and shut down trafficking networks.

PhotoDNA, Project Arachnid, and blockchain analytics tools are more and more frequently applied to identify CSAM, follow cryptocurrency transactions, or recognize abuse patterns. These measures are, however, inconsistently applied and are frequently under-funded, which points to a pressing necessity to make continued investment and to coordinate them. With these issues in mind, it is apparent that previous legal, technological, and institutional counter-reactions to the phenomenon of child trafficking are not always effective against the current change in the ways that child trafficking takes place on the dark web. The combination of anonymizing services, end-to-end encryption, and decentralized Web resources creates special impediments to identification, surveillance, and enforcement (Bello, et.al,2022). This means that it is highly necessary to conduct an in-depth study, which will not only focus on the modes of operation of dark web-based trafficking but will also assess the existing countering mechanisms and pinpoint areas of improved intervention. In this research, the researchers hope to fill this gap, identifying the technological, law enforcement capacity, and international collaboration dynamics in the fight against child trafficking in an encrypted online environment.

II. DEFINITION OF THE DARK WEB

The Dark Web is the network that is restricted to view by anyone and is encrypted and hidden in the search engines by design. Compare to Deep Web, which consists of password-protected or not indexed information, the Dark Web is accessed using special programmes that ensure the concealment of visitors and safe communication. It contains a huge list of different kinds of contents and facilities, ranging to privacy-based websites to illegal marketplaces. Their key distinction to the Dark Web is not in the content but accessibility and deliberate concealment of their infrastructure. Dark Web sites commonly use domain suffixes that are unfamiliar to the normal browsers like ". onion". (Kaur, et.al,2020). Such websites are located on anonymity networks and are configured in a way that the identity neither of the server nor of a user is recognizable. This level of anonymity can be applied in legal purposes like those that the protection of free speech in oppressive dictatorships but it can be used in illegitimate ways as well.

III. STRUCTURE OF THE DARK WEB

The Dark Web has a distinctive technical architecture upon which it is constructed, which differentiates it from the open internet. It is structured around encryption, anonymity, and decentralization technologies, all geared towards concealing the identity and location of users and service providers (Saleem, et.al,2024).

3.1 ENCRYPTED OVERLAY NETWORKS

The Dark Web is centered on what is known as overlay networks, those constructed on top of the internet as we know it that operates using different routing programs. These networks provide a second layer to the exchanged traffic between them and multiple encrypted channels, which hides the user to be viewed and intercepted. The information circulated in these networks is stored in encryptions that are layered in such a way that information transmission is possible. (Castro, et.al,2003).

3.2 HIDDEN SERVICES AND ADDRESSING

Hidden services are called websites and Dark Web services. Unlike the typical web servers that can be reached through the domain name search and location via IP address, the hidden services use the cryptographically created addresses that obscure the physical presence.to give an example, a normal address would appear as a sequence of characters randomly concatenated with “. onion" placed at the end of it that would mean that it will be hosted on the Tor network. (Yadav, et.al,2020). They do not rely on centralized Domain Name System (DNS) infrastructure and they use privately maintained directories in rerouting users to their destination.

3.3 DECENTRALIZED HOSTING AND RESILIENCE

Besides being anonymous about routing, most Dark Web applications do make use of distributed or decentralized hosting arrangements (Chetry, et.al,2023). This entails that content can be backed up in several nodes or replicated in several places, making it less likely to be entirely offline and more likely to defend against a lawsuit takedown or hacking attack. There are also services which are available only in closed used peer-to-peer networks which has more boundary on traceability.

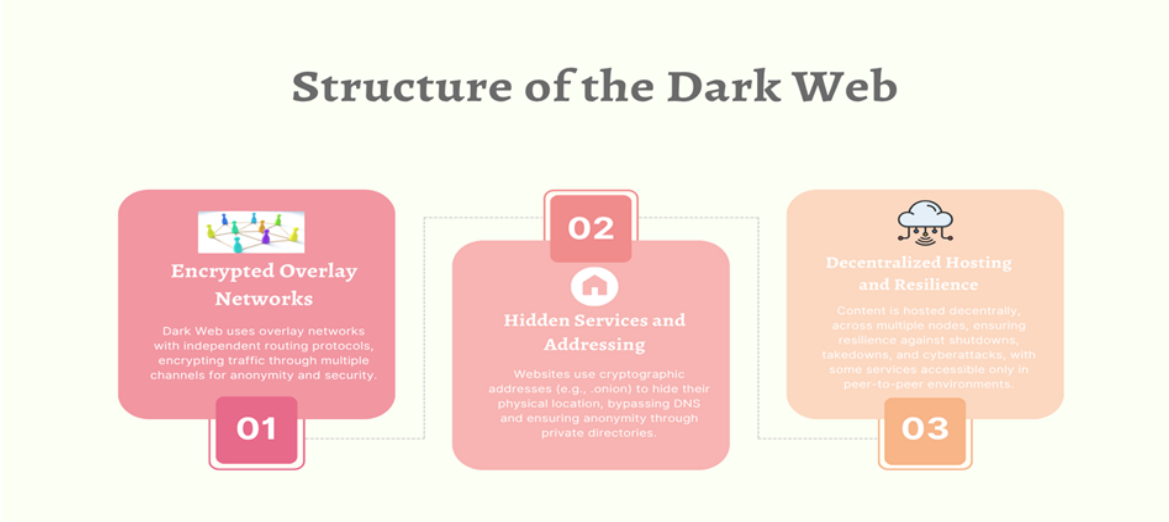

FIG.1- THE DARK WEB OPERATES ON ENCRYPTION, ANONYMITY, AND DECENTRALIZATION TO HIDE IDENTITIES AND LOCATIONS.

IV. TOOLS OF ANONYMITY

Accessing the Dark Web and maintaining privacy within it require specific tools and systems designed to hide user identity, obscure internet traffic, and resist censorship. These tools form the backbone of Dark Web interaction and ensure that both access and activity remain confidential.

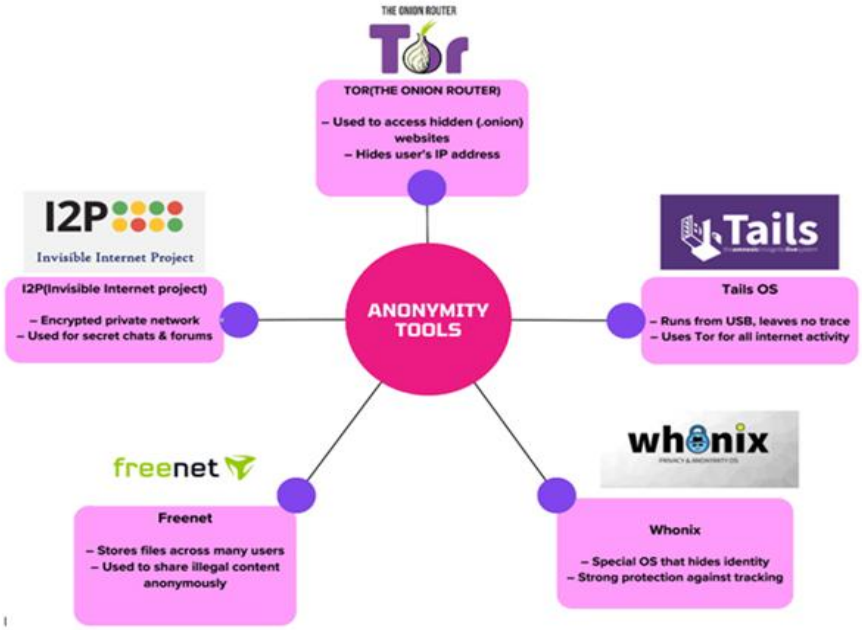

FIG.2- DIFFERENT TYPES OF TOOLS USED IN THE DARK WEB.

4.1 THE ONION ROUTER (TOR)

The most popular and known program to access Dark Web is Tor. It operates by relaying internet traffic across a world-wide scree of servers run by volunteers. Messages transmitted by Tor are encrypted several times, and correspondingly, they are passed by at least three different relay nodes, each performing the removal of one layer of encryption. It is called onion routing because of this property that none of the relays is aware of the complete path of the message (Tran, et.al,2023). Tor does not only allow its users to browse the public internet anonymously, but also allows access to obscure services on the Tor network, which have an onion address, namely, a domain name ending in ". onion".

4.2 I2P (INVISIBLE INTERNET PROJECT)

Another anonymity network that is rather peer to peer communication oriented is I2P. In contrast to the Tor network, which allows reaching hidden services and normal web, I2P is tailored to network-local traffic on a local network. It employs the use of garlic routing, which tends to group together several messages and encrypts them en-masse, thus doing it harder to associate traffic patterns together (Zantout, et.al,2011). I2P is used in anonymous email, writing blogs, file transfer, and has been especially appreciated due to its high level of internal privacy.

4.3 FREENET

Freenet is a decentralized network which is designed to distribute data and publish it anonymously. It is targeted on the principle of data replication and redundancy such that users donate storage capacities of their computers to store encrypted fragments of data. A complete file is not maintained by a single user and the content is obtained on key basis instead of relying on addresses (Clarke, et.al,2001). One of the common uses of Freenet is anonymous discussion forums, websites and document sharing and focus on censorship and surveillance resistance.

4.4 TAILS OS

Tails (The Amnesic Incognito Live System) is an operating system in portable form with the purpose of being privacy and anonymity oriented. It runs off a USB or a DVD and by default passes all web connections through Tor. Tails does not leave any mark in the hardware it is used in; it can be coming in handy in temporary and secure sessions. It is comprising of encrypted messaging, anonymous browser, encrypted files and document storage, all customized to remain confidential.

4.5 WHONIX

Whonix is an operating system security-hardened with an architecture that isolates internet traffic. It consists of 2 virtual machines one of which covers all activity to the network and obliges to pass through Tor, and another is a working environment of the user. This differentiation guarantees that in case the workstation is hacked, chances are that the actual IP address will not be revealed. Whonix is quite common as a tool of people involved in scientific and investigative journalism where a secure and compartmentalized digital workspace is required.

Tools	Function	Utility
Tor (The Onion Router)	*Routes internet traffic through multiple encrypted relays*	*Enables anonymous browsing and access to. onion sites*
I2P (Invisible Internet Project)	*Creates an internal encrypted network of peers*	*Supports anonymous file sharing, messaging, and hidden services*
Freenet	*Peer-to-peer platform with distributed data storage*	*Allows censorship-resistant publishing and content sharing*
Tails OS	*Live operating system running from USB with no traces*	*Offers complete anonymity and leaves no data on host machine*
Whonix	*Linux-based OS that tunnels all traffic through Tor*	*Ensures secure, anonymous computing with strong metadata protection*

TABLE 1- TOOLS USED IN THE DARK WEB ALONG WITH THEIR FUNCTION AND UTILITY.

V. CHILD TRAFFICKING ON THE DARK WEB

5.1 KIND OF EXPLOITATION:

Child exploitation has been in the offline world, and has been making a new scale, Anonymity and sophistication possible. The dark web markets offer a platform to sell and acquire illegal products, usually involving illicit drugs and weapons and services like child exploitation material these days, using a cryptocurrency, such as Bitcoin and monero to obtain anonymity. Encryption tends to TOR (The onion router) to enable anonymous communication by the millions of users on the dark web thus making it hard to track the activity of the users. (He, et.al,2019).

On these networks children are treated as commodities- such as brought, sold and abused to satisfy the anonymous perpetrators around the world. A major form of exploitation is production and distribution of child sexual abuse materials (CSAM) These materials include images and videos of children being sexually abused. Specifically, to be shared and sold online. Another deeply disturbing form is live streamed child sexual abuse – a cruel form of exploitation where viewers pay to watch it as a live. Beyond online content, dark web also facilitates physical tracking of children. Underground markets openly advertise minors of sexual exploitation and forced labour. These markets places provide detailed information including the age, appearance, and sometimes rating from previous buyers. (Rastog, et.al,2020) In addition with dark web hosts forums where offenders share grooming techniques and best practices for luring and controlling children. These discussions often focus on how to build trust with victims online isolate them from support systems and manipulate them from support sources and manipulate them from compliance. These forums not only encourage exploitation but also create a network of offenders who support and reinforce each other abusive behaviour. Finally, the dark web also seen an increase in blackmail children such as threatening, gaining trust or tricking the child and sexual extortion children are coerced in to sharing sexual images or videos, which are used to threaten and control them. Pushing them further in to exploitation or forcing them to meet traffickers in a person.

On these networks children are treated as commodities- such as brought, sold and abused to satisfy the anonymous perpetrators around the world. A major form of exploitation is production and distribution of child sexual abuse materials (CSAM) These materials include images and videos of children being sexually abused. Specifically, to be shared and sold online. Another deeply disturbing form is live streamed child sexual abuse – a cruel form of exploitation where viewers pay to watch it as a live. Beyond online content, dark web also facilitates physical tracking of children. Underground markets openly advertise minors of sexual exploitation and forced labour. These markets places provide detailed information including the age, appearance, and sometimes rating from previous buyers. In addition, with dark web hosts forums where offenders share grooming techniques and best practices for luring and controlling children. These discussions often focus on how to build trust with victims online isolate them from support systems and manipulate them from support sources and manipulate them from compliance. These forums not only encourage exploitation but also create a network of offenders who support and reinforce each other abusive behavior. Finally, the dark web also seen an increase in blackmail children such as threatening, gaining trust or tricking the child and sexual extortion children are coerced in to sharing sexual images or videos, which are used to threaten and control them. Pushing them further in to exploitation or forcing them to meet traffickers in a person.

Like its surface counterpart, the nature of exploitation on the dark web is associated with anonymity, international distribution, engaging in production and trafficking of abuse materials, live-streamed attacks, physical and psychological abuse trafficking, and grooming and psychologically abusive extortion. This merger makes the dark web one of the most disastrous child exploitation areas in modern times.

5.2 MODUS OPERANDI

The modus operandi (MO) by the dark web offenders depicts psychological control, sophisticated technical equipment, and international networks which are challenging to detect.

One of the fundamentals of the process of trafficking is a process known as social engineering which refers to psychological manipulation of the victims (Adel, et.al,2024). Traffickers rely heavily on social media networks and game communities to discover individuals, especially minors. traffickers attempt to

engage in communications and when the base is well-established, they transfer the contact to encrypted messaging programs or to those offered on the dark web. The use of chatbots powered by AI and deepfake technology to victimise people has been on a rise in the past few years. Criminals prefer using end-to-end encrypted services like Signal, Telegram to proprietary encrypted email services Using these services, traffickers establish victim transport routes, payment arrangements, and guard shifts (Sebastian,2023). They also use what is referred to as operational security similar to what is applied by state-sponsored cyber espionage groups. These are: traffic encryption and use of virtual private networks (VPNs) and The Onion Router (Tor) to hide IP addresses. Frequent shifting of pseudonyms and online confidential signature to hide the investigators (Abdelberi, et.al,2010).

VI. TRENDS AND DATA

6.1 THE DARKNET THREAT OF CHILD SEXUAL ABUSE

There are a lot of good things that the internet has done to us. Yet, unfortunately, it also possesses the dark side. Another glaring issue is the increased circulation of child sexual abuse (CSA) material online particularly in the darknet.

There is a dark part of internet which is referred to as the dark net. It is not findable with regular search engines such as Google. It is viewed with the help of the so-called special software, Tor, that protects the identities of people. This highly complicates the ability of the police to understand the identity of the people using the darknet or the activities that they engage in there.

The darkness caused by darknet is used by criminals to post or distribute videos and pictures depicting children being hurt or abused (Valois, et.al,2024). These are clandestine, inhuman and extremely detrimental crimes to children. An example that rose to prominence was a site known as Welcome to Video that contained 250,000 videos on abuse. It was shut down by police across the globe in 2019. More than a thousand people were arrested and several young children were rescued.

Other websites named Boystown dedicated to the abuse of boys counted more than 400,000 visitors, being shut down in 2021. Unfortunately, despite the closure of such sites, new ones emerge soon and sometimes they are even more secure.

6.2 INCREASE IN THE CSA MATERIAL INSTANCES ON DARKNET SITES

The amount of child sexual abuse (CSA) data, identify on the darknet sites, has been growing. Special sites such as Welcome to Video and boystown were closed down revealing thousands of users all over the globe (Gannon, et.al,2023). The activities in these sites are kept secret since they use a sophisticated encryption technique that renders them difficult to trace by authorities. It is clear that it is not easy to completely wipe out such networks since even after takedowns we still continue to see the emergence of new ones.

6.3 MOVEMENT TO DECENTRALIZED NETWORKS AND ANONYMITIES PAYMENTS

The material in CSA is currently being saved and distributed via decentralized networks such as IPFS, which increases the ability to make content hard to remove by the authorities (Desai, et.al,2023). Besides, criminals are using cryptocurrencies such as Monero to transact their business or activities, and it is almost impossible to track the money movement in the acts of CSA. The transition complicates the ability of the authorities to follow the material and as well as follow the payments attached to it.

6.4 THE IMPORTANCE OF THE ARTIFICIAL INTELLIGENCE AND AUTOMATION IN THE DISTRIBUTION OF CSA

Compared to traditional practices, CSA materials are being distributed through artificial intelligence (AI) and automation (Rose, et.al,2025). AI allows generating deepfake content, which is difficult to detect, as it appears to be real, whereas it is not. There are also bots that are automatically posting and sharing the content catching up with the distribution process and providing the offenders with effective hiding.

6.5 UTILIZATION OF ENCRYPTION MESSAGES AND PERSONAL CHATROOMS

CSA material sharing is popular in encrypted messaging, such as Telegram or WhatsApp (Bhuse, et.al,2023). These applications offer a safe dialogue because the communications are encrypted end-to-end, and this makes it difficult to communicate what is being transacted without the law enforcement agency

trespassing. These platforms have the provision of creating or participating in a closed group or channel where the offenders can share the content in secrecy.

6.6 RISE OF DECENTRALIZED FINANCE (DEFI) IN CSA TRANSACTIONS

The newly available anonymous payments can be conducted by using Decentralized finance (DeFi) sites to serve CSA content (Quinteiro dos Santos, et.al,2022). These services enable individuals to send money directly without the involvement of banks which made the offenders be in a position to conceal their finances. It is also quite difficult to trace illegal transactions in DeFi platforms since they are not highly regulated.

6.7 CONTENT SHARING AND CROSS-PLATFORM AS WELL AS MULTI-LAYERED NETWORKS

The distribution of CSA material has increased especially with the use of various platforms and this makes it difficult to trace. In another example, items could be sold on some darknet market and then distributed on private encrypted chat services. With this multi-layer system, authorities find it hard to halt the movement of content as each of these platforms tends to be utilized separately.

6.8 TRANSITION OF THE DARKNET MARKETS OF THE MAINSTREAM TO INVISIBLE WEB COMMUNITIES

CSA content is also being distributed among the more secretive web-based groups that are more difficult to navigate through than a conventional darknet marketplace. Such closed, members-only circles are safer, and use tight encryption and access restrictions. With increased patrolling of the more open locations by the law enforcers, the criminals are shifting to the more hidden areas to carry on with their destructive acts undetected.

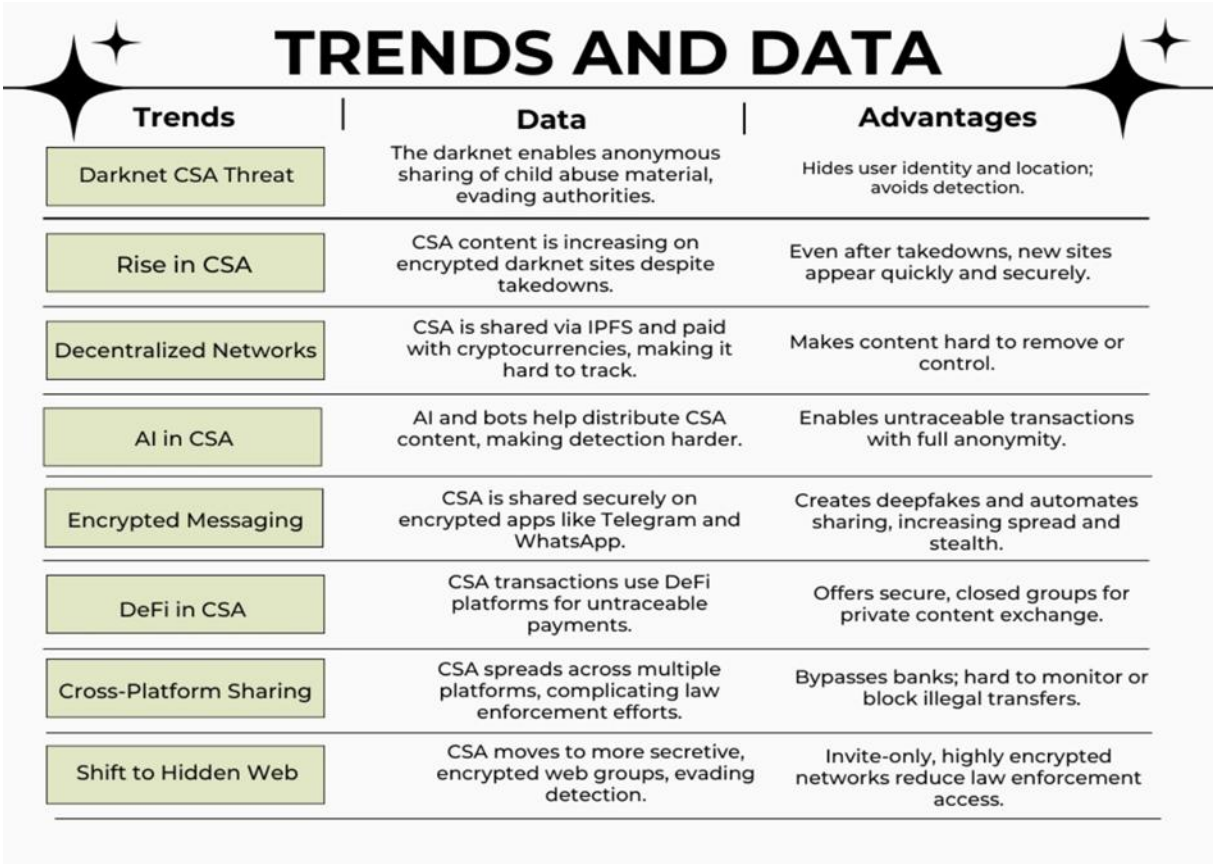

FIG.3- TRENDS AND DATA WITH THEIR ADVANTAGES

VII. CHALLENGES:

7.1 THE ENCRYPTED AND DECENTRALIZED PLATFORMS

Tor, Session, and Briar are encrypted applications used by criminals to transfer message and do not save any data or messages. These applications allow the authorities to nearly impossible to pursue and tap into communication.

7.2 PAYMENT THAT CANNOT BE TRACED

Traffickers no longer use Bitcoin but use so-called privacy coins, such as Monero or Zcash, where the details of the transaction are concealed (Foley, et.al,2019). Money also passes through mixers and this renders it extremely difficult to track down the trail.

7.3 ARTIFICIAL INTELLIGENCE-GENERATED CONTENT

In some instances, traffickers' resort to AI to make counterfeited child abuse photos and videos. They are seen in the form of fake children, though they still contribute to the demand and even baffle investigators. Social Media Grooming Victims are commonly found on profiles on apps such as Instagram or game apps and the conversation is switched to the dark web or coded chat.

7.4 GROOMING WITH THE ASSISTANCE OF SOCIAL MEDIA

Victims are usually identified by traffickers on such platforms as Instagram or games applications and the conversation is taken to the dark web or encrypted chat rooms. (Okocha, et.al,2023).

7.5 JURISDICTION AND LEGAL ISSUES

Numerous criminals are based in nations whose legislations are poor or lack any agreements with police in other nations of the world. This is slowing the process of arresting people and difficult to take down websites (Mark R, et.al,2013).

7.6 CONCEALED, SECRET COMMUNITIES

Traffickers shifted to smaller, invitation-only boards after finding users of big websites closed down by police. These groups are more difficult to locate as well as join (Klabbers RE, et.al,2023).

7.7 INADEQUATE RESOURCES COMPARED WITH THE AMOUNT OF EVIDENCE

The police often find huge volumes of information when they search such sites; photos, videos, chats. To process things and come across the victims is long and demanding in terms of personnel (Rahime Belen Saglam,et. al,2023).

VIII. FUTURE ASPECTS AND THE WAY FORWARD:

8.1 AI-BASED DETECTION AND VICTIM IDENTIFICATION

Advanced AI tools like PhotoDNA, Google Content Safety API, and Griffeye Analyse DI are being used to detect child sexual abuse material (CSAM) and help identify victims faster. Machine learning is also being developed to detect grooming behaviour and trafficking patterns in chats and online forums.

8.2 BLOCKCHAIN AND CRYPTOCURRENCY TRACKING

New tools such as Chain analysis and Cipher Trace now offer deeper tracking of cryptocurrency, including complex laundering patterns and privacy coins like Monero. These tools help trace financial transactions behind trafficking and darknet payments (Liang, et.al,2025).

8.3 INTERNATIONAL COOPERATION AND LEGAL REFORMS

Future efforts focus on strengthening cross-border investigations, speeding up extradition processes, and updating laws to include synthetic CSAM and AI-generated abuse content.

Collaboration through platforms like Europol, Interpol, and INHOPE is essential for timely response and global action. (Yemets, et.al,2024).

FIG.4- FUTURE ASPECTS AND THE WAY FORWARD OF THE DARK WEB.

IX. CONCLUSION

To sum up, the dark web has emerged as a critical enabler of child trafficking and traffickers have taken advantage of the anonymity, encryption and distributed model of the dark web. The patterns are positive towards the increase in different kinds of trafficking such as the spread of Child Sexual Abuse Material (CSAM), live-streamed abuse, and unlawful adoption services. Even financial transactions would be even more difficult to trace with the use of cryptocurrencies such as Monero. Though international organisations such as INTERPOL and Europol put in their best efforts, these difficulties still exist owing to the characters of the traffickers in that they continuously upgraded their technology and the absence of harmonizing regulations in most parts of the world. Law enforcement agencies usually have the problem of shortage of resources and experience when it comes to dealing with such crimes. More vigilance tools, photo DNA and blockchain analytics have been identified to work, but inconsistently so. Trafficking in children on the dark web is so complex that the more coordinated and streamlined response is needed to include more international collaboration implementation, better funding of technological means, and legal framework adaptation. The best way to fight this increasingly becoming massive problem is to keep investing in technological development as well as the cooperation between countries.

CONSENT FOR PUBLICATION

Not applicable

FUNDING

None

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this review paper. The research was conducted independently and received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. All sources of information have been duly acknowledged, and the authors affirm that they have no personal, financial, or professional affiliations that could have influenced the content or interpretation of the findings presented in this paper.

ACKNOWLEDGEMENT

I would like to express my heartfelt thanks to Ms. Manishi Shriwas, whose continuous guidance, encouragement, and insightful feedback provided the foundation for this paper. Their support throughout the research process was invaluable and deeply appreciated.

- Khatri Renuka: Gathered and analyzed important trends, compiled relevant data, and presented appropriate visual materials, enriching the overall presentation and analytical quality of the paper.

- John Judy Joana Catherine: Contributed significantly by preparing a well-structured Introduction and comprehensive abstract, which provided a clear and concise overview and set the tone for the entire project.
- Panchia Rupli: The definition, structure, and tools of anonymity were clearly explained, adding depth to the topic.
- Sivakoti Divya Sai Lakshmi: The topic of child trafficking on the dark web was researched and presented in detail.

REFERENCE

[1] Yustisia, I., Priyanti, D., Mulachelah, N., Azahar, K., Bidin, A., Illahi, A., Tamitiadini, D., Rakhmawati, F., Oktaviani, F., Avicenna, F., Adila, I., Adhrianti, L., Wulandari, M., Ahmad, M., Destrity, N., Wardasari, N., Zaki, N., Kriyantono, P., Safitri, R., & Laturrakhmi, Y. (2023). *The transformation of digital technology: Its impact on human communication*. https://doi.org/10.11594/futscipress39m

[2] Raman, R., Nair, V. K., Nedungadi, P., Ray, I., & Achuthan, K. (2023). Darkweb research: Past, present, and future trends and mapping to sustainable development goals. *Heliyon, 9*(11), e20562. https://doi.org/10.1016/j.heliyon.2023.e20562

[3] Elangovan, R. (2020). The dark web: Hidden access to internet today. In *Applying methods of scientific inquiry into intelligence, security, and counterterrorism* (Chapter 8). IGI Global. https://doi.org/10.4018/978-1-5225-9715-5.ch008

[4] Wang, Y., Arief, B., & Hernandez-Castro, J. (2024). Secure in the dark? An in-depth analysis of dark web markets security. *Research Square*. https://doi.org/10.21203/rs.3.rs-5010611/v1

[5] Kaur, S., & Randhawa, S. (2020). Dark web: A web of crimes. *Wireless Personal Communications, 112*, 2705–2717. https://doi.org/10.1007/s11277-020-07143-2

[6] Castro, M., Druschel, P., Ganesh, A., Rowstron, A., & Wallach, D. (2003). Secure routing for structured peer-to-peer overlay networks. *ACM SIGOPS Operating Systems Review, 36*(SI), 299–314. https://doi.org/10.1145/844128.844156

[7] Yadav, D., Bhushan, B., & Saxena, S. (2020). The dark web: A dive into the darkest side of the internet. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3598902

[8] Chetry, A., & Sharma, U. (2023). Anonymity in decentralized apps: Study of implications for cybercrime investigations. *International Journal of Experimental Research and Review, 32*, 195–205. https://doi.org/10.52756/ijerr.2023.v32.017

[9] He, S., He, Y., & Li, M. (2019). Classification of illegal activities on the dark web. In *Proceedings of the 2019 2nd International Conference on Information Science and Systems* (pp. 73–78). ACM. https://doi.org/10.1145/3322645.3322691

[10] Sebastian, G. (2023). Do ChatGPT and other AI chatbots pose a cybersecurity risk? An exploratory study. *International Journal of Security and Privacy in Pervasive Computing, 15*(1), 1–11. https://doi.org/10.4018/IJSPPC.320225

[11] Clarke, I., Sandberg, O., Wiley, B., & Hong, T. W. (2001). Freenet: A distributed anonymous information storage and retrieval system. In Designing privacy enhancing technologies (pp. 46–66). Springer. https://doi.org/10.1007/3-540-44702-4_4

[12] Zantout, R. N., & Haraty, R. A. (2011). I2P data communication system. In Proceedings of the 7th International Conference on Information Technology (pp. 1–6). IEEE. https://doi.org/10.1109/ITNG.2010.102

[13] Rastog., R. S., Batra, I., & Yadav Rastogi, R. (2020). Exploring the hidden part of the web: A study on dark web and its threats. Journal of Cybersecurity and Privacy, 1(1), 23–38. https://doi.org/10.3390/jcp1010002

[14] Rose, E. (2025). Artificial intelligence and deepfakes: Keeping children safe in schools. Journal of Family and Child Health, 2(1), 44–52. https://doi.org/10.12968/jfch.2025.2.1.44

[15] El-Kady, R. (2025). Decoding the dark: AI and ML in Dark Web cybercrime and cryptocurrency forensics. International Cybersecurity Law Review. https://doi.org/10.1365/s43439-025-00145-5

[16] Tran, D., Salamatian, K., Fukuda, K., & Kaafar, M. A. (2023). Exposing IPFS: Privacy and security analysis of the Interplanetary File System. Proceedings on Privacy Enhancing

Technologies, 2023(1), 147–166. https://doi.org/10.56553/popets-2023-0020

[17] Valois, P. H. V., Macedo, J., Ribeiro, L. S. F., dos Santos, J. A., & Avila, S. (2024). Leveraging self-supervised learning for scene classification in child sexual abuse imagery. Proceedings on Privacy Enhancing Technologies, 2024(1), 147–166. https://doi.org/10.56553/popets-2024-0020

[18] Foley, S., Karlsen, J., & Putnins, T. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies, 32*(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

[19] Okocha, D., Isah, J., & Akpe, S. (2023). Social media: A gateway for online child grooming. In *Handbook of Research on Digital Violence and Discrimination Studies* (pp. xx–xx). IGI Global. https://doi.org/10.4018/978-1-6684-5991-1.ch009

[20] Leipnik, M. R., Ye, X., & Wu, L. (2013). Jurisdictional boundaries and crime analysis: Policy and practice. *Regional Science Policy & Practice, 5*(1), 45–66. https://doi.org/10.1111/j.1757-7802.2012.01086.x

[21] Klabbers, R. E., Hughes, A., Dank, M., O'Laughlin, K. N., Rogers, M., & Stoklosa, H. (2023). Human trafficking risk factors, health impacts, and opportunities for intervention in Uganda: A qualitative analysis. *Global Health Research and Policy, 8*(1), 52. https://doi.org/10.1186/s41256-023-00332-z

[22] Saglam, R. B., Nurse, J. R. C., & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications, 66*, 103163. https://doi.org/10.1016/j.jisa.2022.103163

[23] Yemets, O., Voronov, I., & Hribov, M. (2024). Legal aspects of international cooperation in combating organised crime. *Naukovij Vìsnik Nacìonal'noï Akademìï Vnutrìšnìh Sprav, 29*, 20–30. https://doi.org/10.56215/naia-herald/1.2024.20

[24] Desai, V., & Shikalgar, A. (2023). A review on "IPFS based decentralized social media platform". *International Journal of Computer Science and Mobile Computing, 12*(5), 12–16. https://doi.org/10.47760/ijcsmc.2023.v12i05.003

[25] Bhuse, V. (2023). Review of end-to-end encryption for social media. *Proceedings of the International Conference on Cyber Warfare and Security, 18*, 35–37. https://doi.org/10.34190/iccws.18.1.1017

[26] Gannon, C., Blokland, A., Huikuri, S., Babchishin, K., & Lehmann, R. (2023). Child sexual abuse material on the darknet. *Forensische Psychiatrie, Psychologie, Kriminologie, 17*, 1–13. https://doi.org/10.1007/s11757-023-00790-8

[27] Adel, A., & Norouzifard, M. (2024). Weaponization of the growing cybercrimes inside the dark net: The question of detection and application. *Big Data and Cognitive Computing, 8*(4), 91. https://doi.org/10.3390/bdcc8080091

[28] Law as a toothless bulldog. *SAGE Open, 12*. https://doi.org/10.1177/21582440211069379

[29] Saleem, J., Islam, M. R., & Islam, Z. (2024). Darknet traffic analysis: A systematic literature review. *IEEE Access, PP*, 1–1. https://doi.org/10.1109/ACCESS.2024.3373769

[30] Abdelberi, C., Manils, P., & Kaafar, D. (2010). Digging into anonymous traffic: A deep analysis of the Tor anonymizing network. In *Proceedings of the 2010 4th International Conference on Network and System Security (NSS 2010)* (pp. 167–174). IEEE. https://doi.org/10.1109/NSS.2010.47

[31] Quinteiro dos Santos, S., Singh, J., Thulasiram, R., Kamali, S., Sirico, L., & Loud, L. (2022). A new era of blockchain-powered decentralized finance (DeFi): A review. In *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1286–1292). IEEE. https://doi.org/10.1109/COMPSAC54236.2022.00203