ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

Beyond the Onion Routing: Unmasking Illicit Activities on the Dark Web

Dr. Vijaykumar Bidve[1]; Aishwarya Suryakant Waghmare[2]
School of Computer Science and Information Technology
Symbiosis Skills and Professional University Pune, India

Abstract:- This comprehensive study delves into the complexities of the Dark Web, a concealed segment of the internet that remains invisible to standard search engines and is accessible only through specialized tools like The Onion Router (TOR), which ensures user anonymity. While the Dark Web is celebrated for its capacity to safeguard privacy and foster free expression, it concurrently serves as a sanctuary for illegal endeavours, encompassing drug trafficking, unauthorized arms trading, and a spectrum of cybercrime. The primary objective of this research is to scrutinize the efficacy of onion routing, the foundational technology behind the Dark Web, in preserving user anonymity amidst escalating efforts by law enforcement agencies to dismantle illegal activities. This paper adopts a rigorous approach that melds an exhaustive review of pertinent literature with empirical investigations to pinpoint the intrinsic vulnerabilities within the onion routing framework. Furthermore, the study introduces innovative methodologies aimed at bolstering the detection and neutralization of illicit transactions and communications on the Dark Web. These proposed methods seek to establish a delicate balance between upholding the Dark Web's legitimate functions—such as protecting privacy and enabling free speech—and curtailing its misuse for criminal activities. The paper culminates in a discussion of the broader implications of these findings for policymakers, law enforcement officials, and privacy advocates. It provides a set of recommendations for future research and policy formulation in this intricate and ever-evolving domain, to navigate the challenges posed by the Dark Web while preserving its essential values.

Keywords:- *Dark Web, TOR, Onion Routing, Cybersecurity, Law Enforcement, Privacy, Anonymity, Cybercrime, Social Network Analysis, Cryptography.*

I. INTRODUCTION

The Dark Web, frequently linked to clandestine dealings and concealed communication, stands as a complex and often misinterpreted facet of the contemporary digital realm. [1] At its core is an elaborate network of websites and services leveraging advanced encryption techniques, such as onion routing, to ensure user anonymity and privacy. This framework aims to protect sensitive information and uphold the rights to privacy and free speech, proving crucial for activists, journalists, and others facing oppressive environments or restricted freedom of expression.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

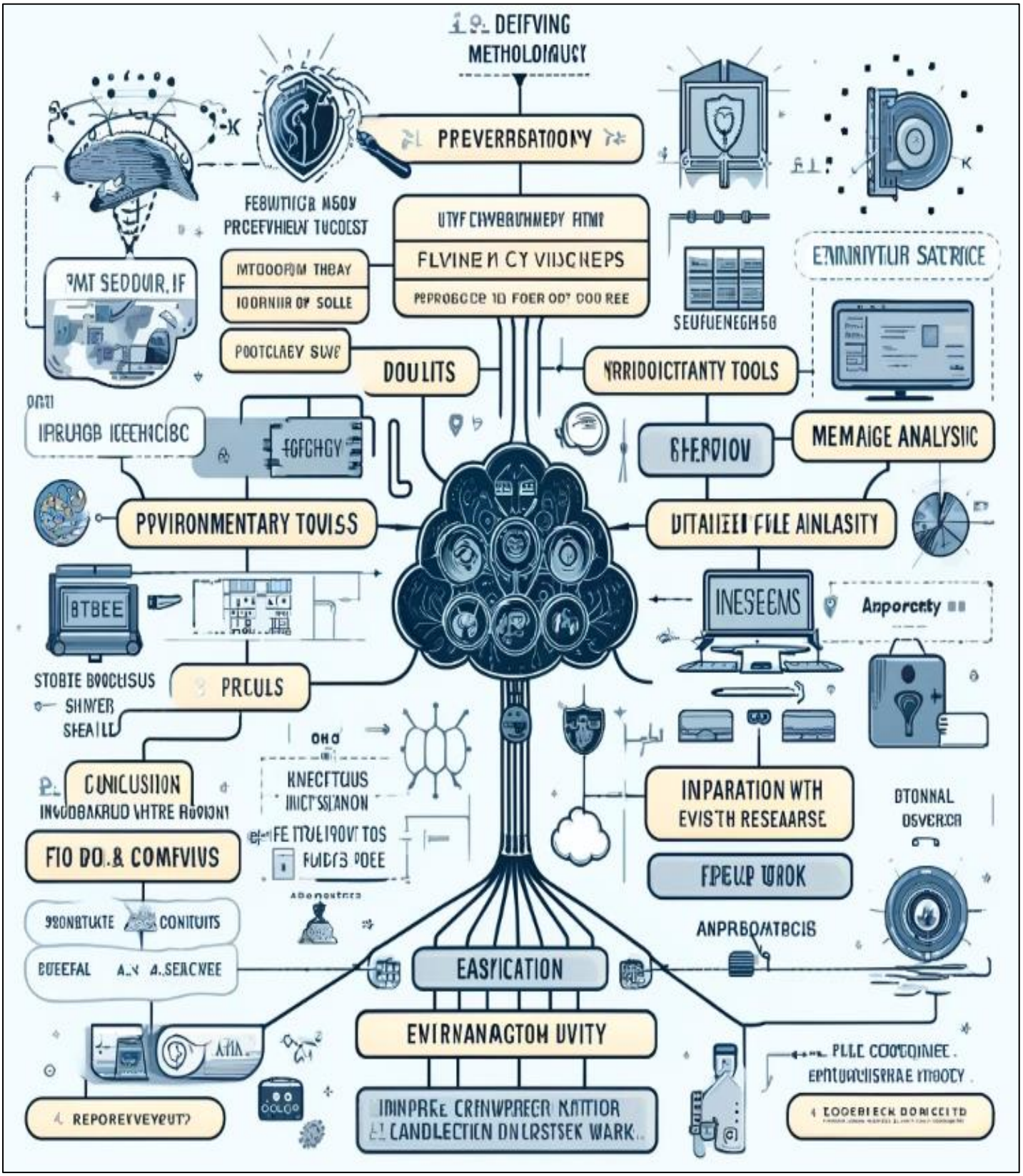

Fig 1: Flowchart for Dark Web Forensics

[2] Nonetheless, the very attributes that render the Dark Web a sanctuary for privacy and freedom also transform it into a hotbed for unlawful activities. Its anonymity and lack of traceability have attracted diverse groups engaged in illicit trade, cybercrime, and other malevolent acts. [3] This dual nature of the Dark Web presents a considerable challenge to law enforcement and regulatory agencies.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

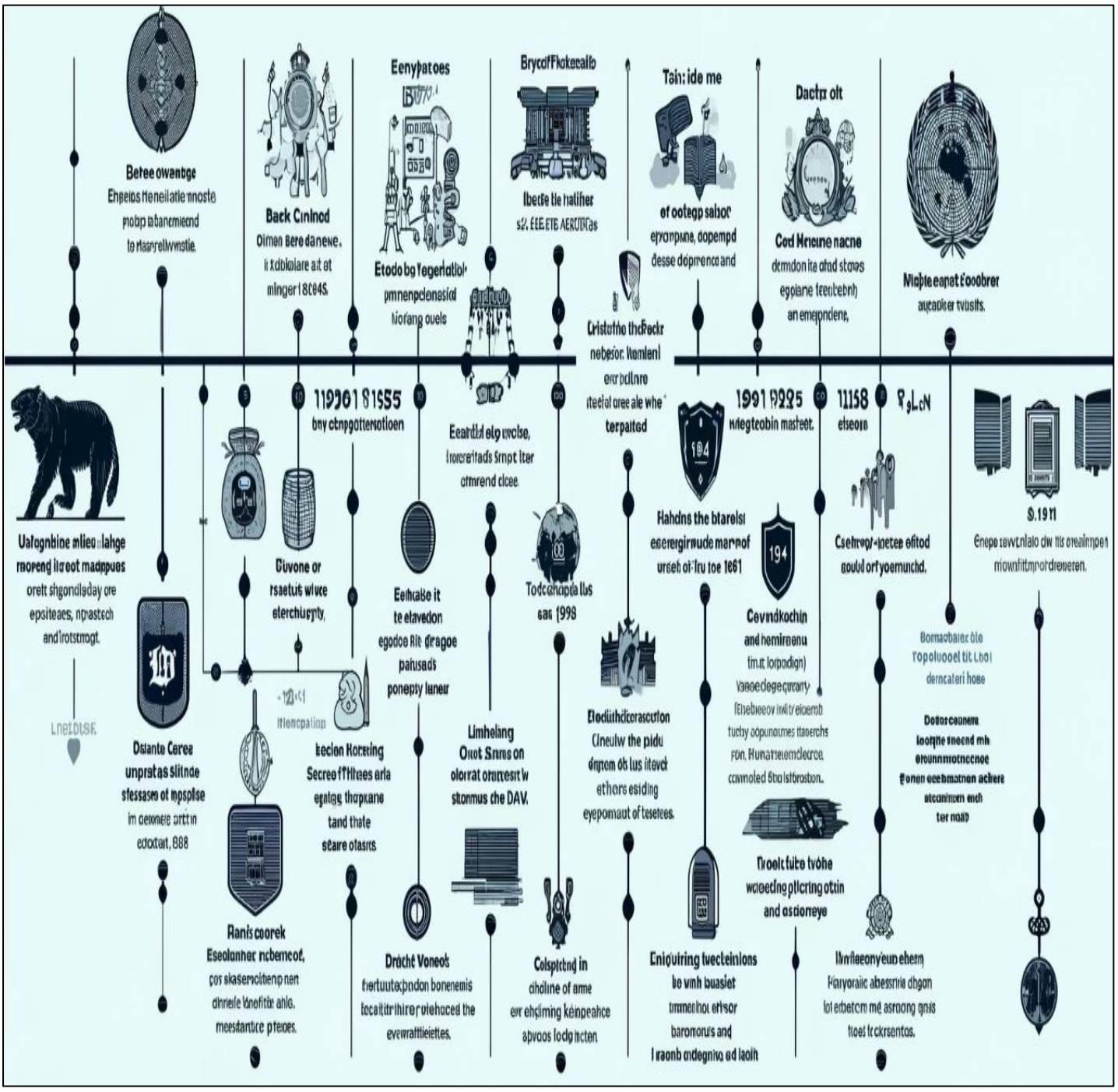

Fig 2: Dark Web Timeline

Efforts to uncover and curb illicit activities on the Dark Web must be judiciously balanced with the imperative to maintain its legitimate benefits, ensuring that surveillance measures do not inadvertently encroach upon the principles of privacy and free speech. [4] This research paper delves into the complexities of the Dark Web, scrutinizing its architecture and the motivations driving both its lawful and unlawful usage. It aims to illuminate the challenges in unmasking illicit activities on the Dark Web while preserving a delicate equilibrium between security and privacy. [5] Through a thorough examination of the technologies, strategies, and ethical considerations involved, this paper endeavours to contribute to a more nuanced understanding of the Dark Web and the ongoing efforts to navigate its obscure corridors without undermining the values it is intended to protect.

II. LITERATURE SURVEY

[6] Deep Web: The Deep Web encompasses a vast array of digital content that remains unindexed by conventional search engines for multiple reasons. This realm includes an assortment of databases, private networks, and other specialized services that are beyond the reach of standard search tools.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

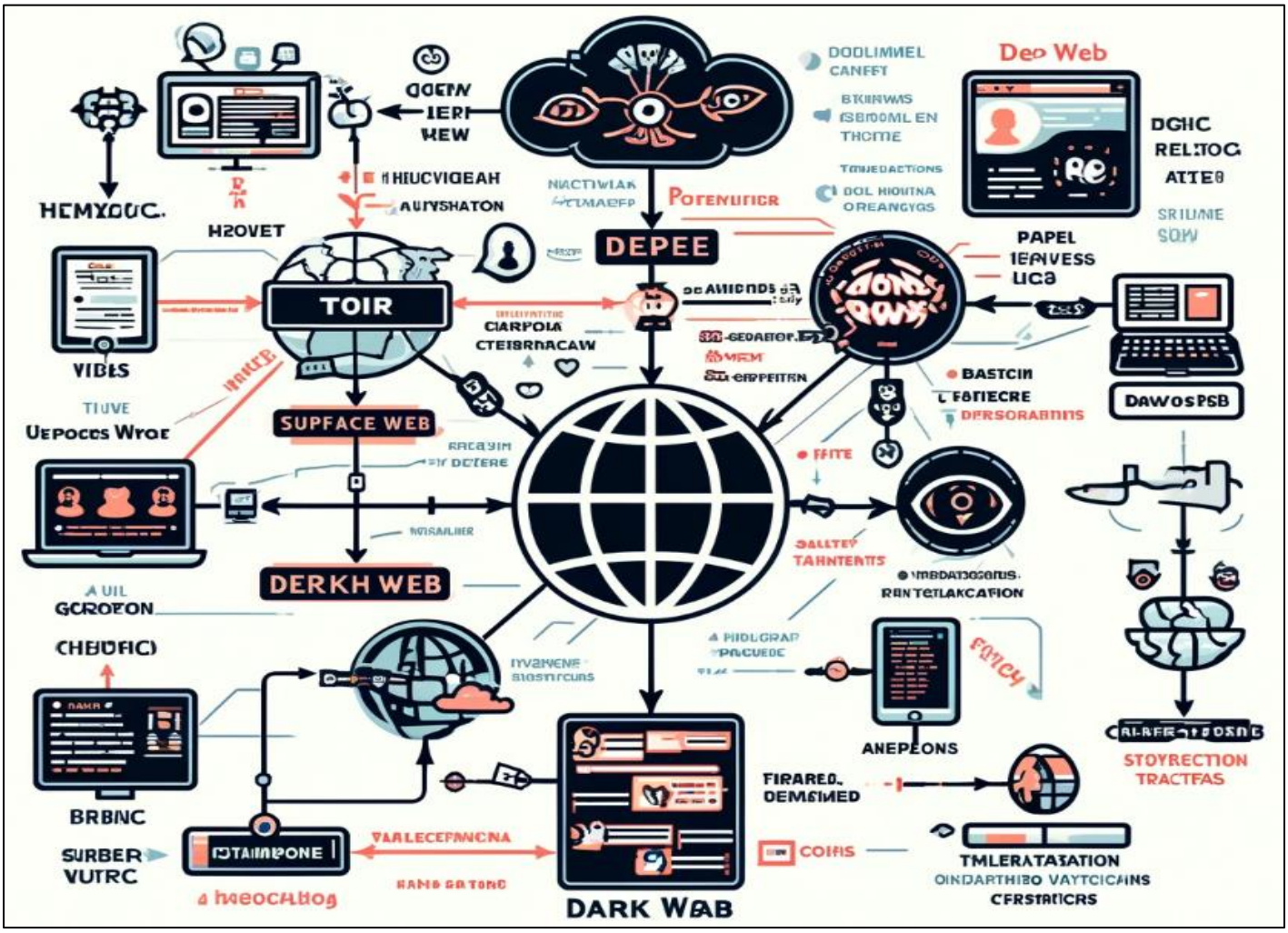

Fig 3: Dark Web Mind Map

Despite its frequent association with unlawful activities, the Deep Web itself does not inherently harbor malicious intent. It serves as a reservoir for a diverse range of information, from scientific research data to private corporate documents, that require controlled access for security or privacy reasons. Dark Web: A more clandestine subset of the Deep Web, the Dark Web is deliberately obscured from the general internet, or surface web. This hidden segment is accessible exclusively through specific [7] browsers like TOR (The Onion Router), which provide a layer of anonymity to users. Renowned for being a hub of various illegal transactions and activities, the Dark Web also caters to individuals and groups seeking to preserve their privacy and operate anonymously for legitimate reasons, such as whistleblowing, secure communication in oppressive regimes, or sensitive research. Invisible Web: Often used synonymously with the Deep Web, the Invisible Web is the portion of the internet that remains unindexed by search engines. This segment contains a wealth of information, including academic databases, proprietary research, and government archives, which are not available through standard search methods. The Invisible Web is critical for researchers, scholars, and professionals who rely on specialized databases and resources that are not exposed to the broader public for reasons of confidentiality, intellectual property protection, or simply because they require specific search protocols to access. [7] Use of the Dark Web by Terrorists: Studies have shown that terrorists use the Dark Web for various purposes, including recruitment, radicalization, material benefits, and hiding communications and propaganda. For example, ISIS has been known to use the Dark Web as a propaganda hub, with encrypted services like Telegram being used to send TOR links among members, especially following the 2015 Paris attacks. Challenges in Analyzing Dark Web Content: The analysis of the Dark Web's content reveals a near-absence of Islamic extremism on TOR hidden services. This suggests that while groups like ISIS use the internet for propaganda and internal communication, these uses have not stabilized on the Dark Web. The limited reach of the Dark Web and its unsustainability as a communication method are cited as reasons for this. Law Enforcement Efforts: European law enforcement agencies have developed advanced data-mining and analytical systems, such as the DANTE project, to combat terrorism. These systems help detect, retrieve, collect, and analyze a vast amount of heterogeneous and complex multimedia and multi-language terrorist-related information on the Dark Web. The aim is to disrupt the financing of terrorist acts and identify potential terrorists through their online activities.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

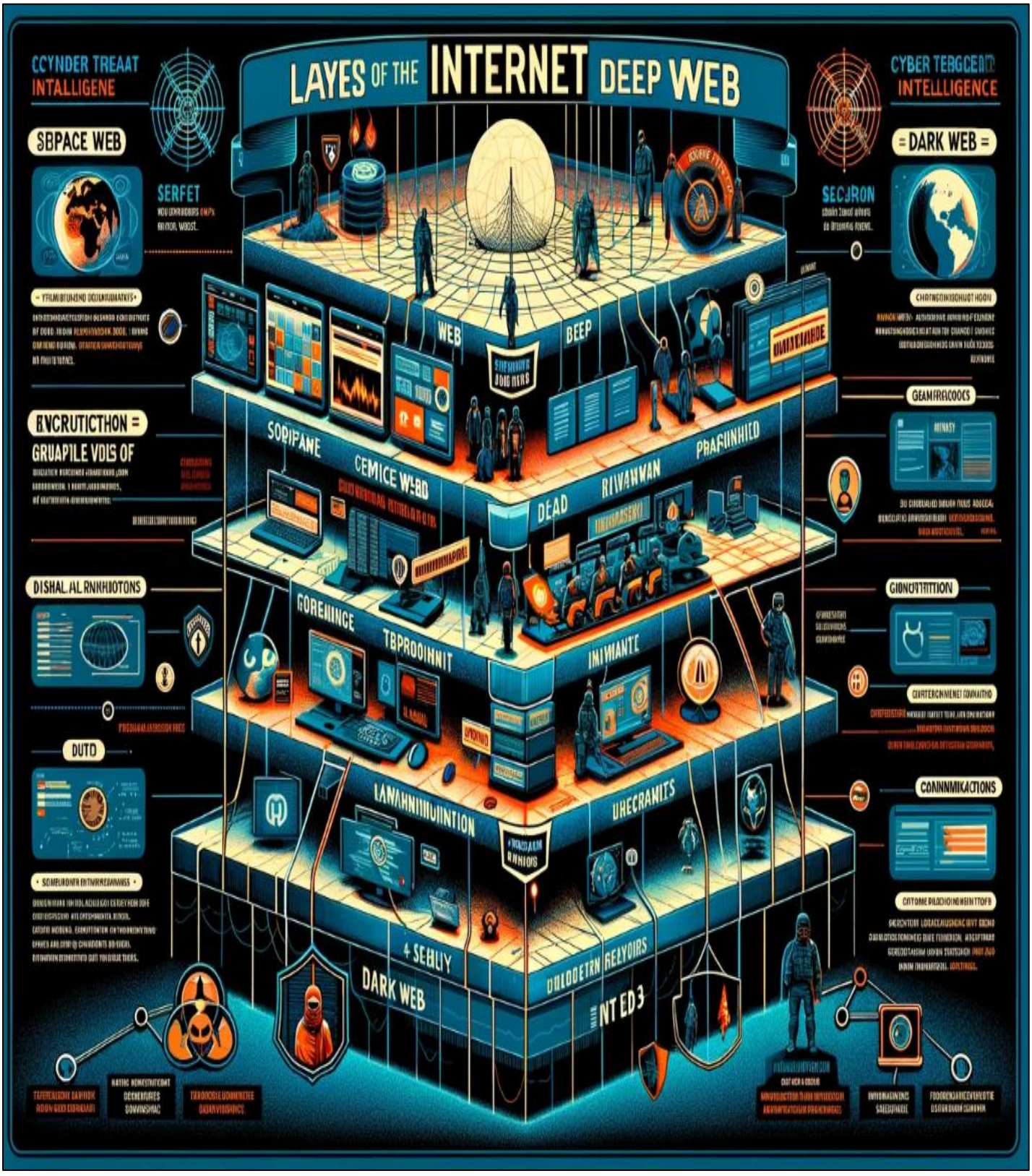

Fig 4: Layers of Dark and Deep Web

- Misconceptions and Moral Panics: There is a misconception that the Dark Web is a haven for terrorists and an effective tool for their communications. However, the evidence suggests that the use of the Dark Web by terrorists is not as widespread as feared. The fear of the Dark Web can be attributed to moral panics associated with the internet over the past 35 years, with discourses tending to cluster around "liberating" or "threatening" rhetoric.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

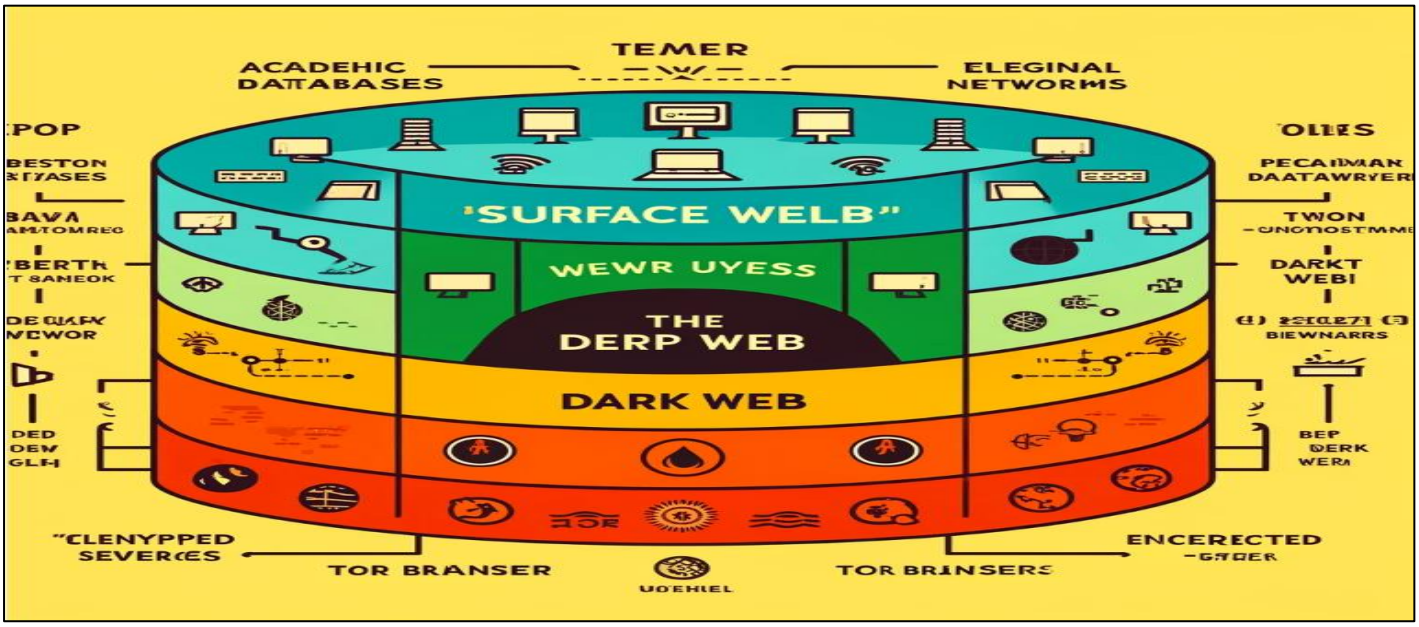

Fig 5: Illustration of Dark and Deep Web

- [8] Challenges in Governing the Dark Web: The governance of the Dark Web is intricate due to its decentralized architecture and the employment of encryption technologies that ensure user anonymity. Conventional methods of internet governance, which rely on transparency and accountability, face difficulties in addressing the secretive and enigmatic nature of the Dark Web. Cyber Security Implications: The anonymity afforded by the Dark Web poses significant cyber security risks, enabling cybercriminals to execute illegal activities without detection. The Dark Web is notorious for enabling the exchange of stolen data, the dissemination of malware, and the planning of cyber-attacks.

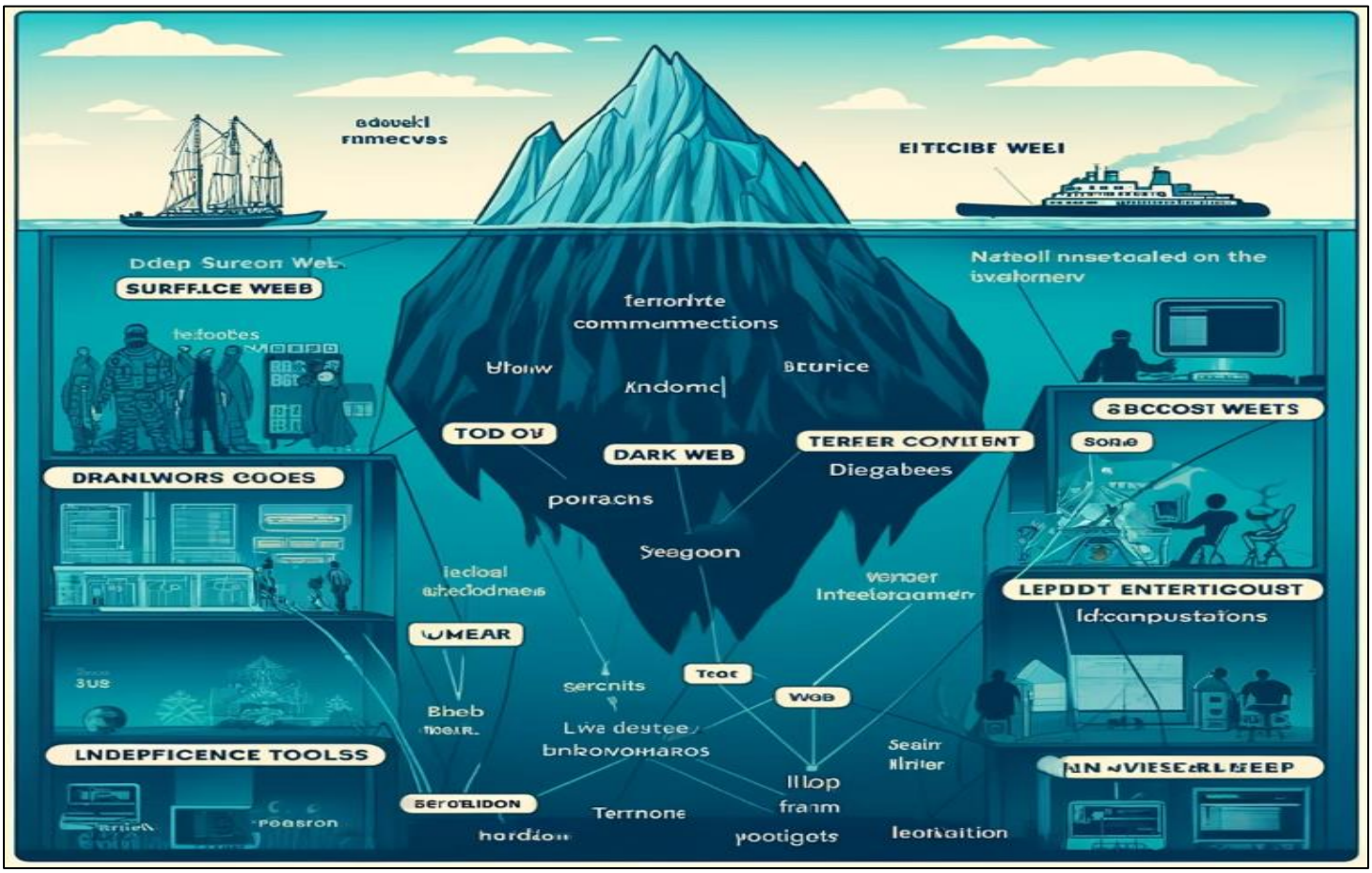

Fig 6: Future Directions in all Webs

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

- Balancing Privacy and Security: A principal challenge in addressing the Dark Web is striking a balance between privacy and security. Although the Dark Web can serve as a refuge for criminal activities, it also provides a platform for legitimate activities that necessitate anonymity, such as advocating for political change and whistleblowing. Regulation and Monitoring: The regulation and monitoring of the Dark Web are hindered by the technical challenges of tracing encrypted communications and the ethical concerns regarding privacy infringement. Various strategies have been proposed, including the development of specialized law enforcement tools, and fostering international cooperation to combat cross-border cybercrime. Future Directions: The ongoing development of the Dark Web and its associated technologies requires continuous research and adaptation in the realms of cyber security and internet governance. Future initiatives may include devising more sophisticated methods to distinguish between legal and illegal activities on the Dark Web and improving collaboration among diverse stakeholders to address these challenges. [9] Exploring the Dark Web for CTI Insights: The Dark Web plays a crucial role in the collection of Cyber Threat Intelligence (CTI) due to its status as a hub for numerous illegal activities and cyber threats. Active surveillance and examination of Dark Web content are vital for decoding criminal strategies and thwarting cybercrimes. Navigating Challenges and Ethical Dilemmas: Delving into the Dark Web is fraught with challenges, including its expansive nature, intricate navigation, and the veil of anonymity it provides to its users. Ethical dilemmas also abound, as investigators must tread carefully between upholding security and honoring privacy and legal constraints. Methodologies and Instruments for Dark Web Scrutiny: Recent research has adopted a variety of methodologies and instruments for scrutinizing Dark Web content, including the application of machine learning algorithms, deep learning architectures, and cryptocurrency transaction tracking tools. These technological advances assist in pinpointing illicit activities and discerning patterns linked to cybercrimes. Evolving Trends in Cyber Threat Intelligence: A notable trend in CTI is its amalgamation with blockchain technology. By leveraging blockchain, CTI can be enhanced in terms of security and efficiency, providing a robust and transparent framework for the management and exchange of threat intelligence data. Tactics for Mitigating Cyber Threats: To effectively counter cyber threats emanating from the Dark Web, strategies such as persistent monitoring, the adoption of cutting-edge technologies like artificial intelligence and machine learning, and the utilization of cryptocurrency transaction tracking tools are imperative. These tactics are instrumental in identifying potential threats and fortifying cybersecurity defenses. Information Sources for CTI: The efficacy of CTI hinges on its ability to draw from a diverse array of sources, both internal and external, to furnish organizations with prompt security alerts and insights into the modus operandi of threat actors. The value of CTI lies in its promptness, relevance, precision, specificity, and capacity for actionable insights. [10] Hyper-Privacy Concerns: With increasing awareness and concern for privacy, especially in the context of sensitive environments like the Dark Web, there is a growing demand for technologies that preserve user anonymity. Hyper-privacy refers to an extreme emphasis on maintaining privacy, which involves robust measures to avoid tracking and profiling by third parties. Leveraging Conversational Agents on the Dark Web: Research on leveraging conversational agents within the Dark Web is sparse, largely due to the secretive nature of these networks and the technical challenges involved in deploying and studying these technologies in such an environment. However, the potential for these agents to function in hyper-private environments suggests a dual-use capability where marketing strategies could be adapted to respect user anonymity while still delivering personalized experiences. Marketing Implications: In the context of marketing, conversational agents on the Dark Web could enable businesses to reach niche markets and engage with customers who prioritize privacy above all else. These interactions would need to be carefully designed to respect the anonymity preferences of users, possibly adapting conventional marketing techniques to fit the unique constraints of hyper-private spaces. Dark Web Architecture and Anonymity Technologies: [11] The architectural framework of the Dark Web is primarily analyzed through technologies such as Tor and I2P, which are fundamental to its anonymity capabilities.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

Fig 7: Ethical Considerations

Tor, also known as The Onion Router, employs a sophisticated network of relays that encrypt and redirect internet traffic to conceal the identities and activities of its users. In parallel, the Invisible Internet Project (I2P) utilizes a multi-layered security protocol aimed at enabling anonymous communication across the internet. [12] Timpanaro et al. (2011) describe how I2P secures communications by using multiple layers of encryption managed within a decentralized peer-to-peer network. Methodologies for Uncovering Illicit Activities: Investigating illicit activities on the Dark Web requires advanced and diverse methodologies that integrate digital forensics, data mining, and machine learning techniques. Researchers have devised several tools that penetrate the anonymizing layers of the Dark Web to reveal hidden patterns and connections. [13] Al Nabki et al. (2017) highlighted the strategic use of adaptive web crawlers designed to navigate and systematically gather data from the dynamically changing environments of Dark Web sites. Effectiveness of Law Enforcement Strategies: Law enforcement's success in curtailing Dark Web operations has been inconsistent. Notable successes include operations like the shutdown of the Silk Road marketplace, yet the intrinsic decentralized and encrypted nature of the Dark Web continually presents significant challenges.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

Fig 8: Criminal Activities on Dark Web

[14] Munksgaard and Demant (2016) discuss how law enforcement requires heightened international collaboration and sophisticated technical skills to tackle Dark Web criminal activities effectively. Gaps in Current Knowledge and Methodologies: Research on the Dark Web has progressed, yet substantial gaps remain, particularly concerning the understanding of its architecture and the effectiveness of countermeasures against its illicit aspects. There is an evident shortage of longitudinal research that monitors the evolution of Dark Web marketplaces and their responses to law enforcement efforts. [15] Brenner (2012) raises concerns about the ethical implications inherent in surveillance and data collection methods used in studying the Dark Web, underlining the need for cautious and considerate research approaches.

III. PROPOSED SOLUTION [RESEARCH]

The increasing prevalence of illicit activities on the Dark Web necessitates the development of robust methodologies for unmasking these activities while preserving user privacy in legitimate cases. The case of Eldo Kim [16], who used Tor and Guerrilla Mail to send a bomb threat to Harvard University, serves as a pertinent example of the limitations and potential vulnerabilities in current anonymity tools. The FBI's successful tracing of Kim's activities underscores the need for enhanced strategies to combat misuse without compromising the integrity of anonymous communication channels. Unmasking illicit activities on the dark web requires a comprehensive approach that leverages technological advancements, fosters collaboration, and adapts legal frameworks to the digital age. By addressing the limitations highlighted in cases like Eldo Kim's, we can improve our ability to combat the misuse of anonymity tools and enhance overall cybersecurity.

- Enhanced Anonymity Tools: Current anonymity tools such as Tor provide a significant degree of privacy by masking users' IP addresses and routing their traffic through multiple nodes. However, as demonstrated in Kim's case, these tools can still be vulnerable when users access them through identifiable networks. To address this, the following enhancements are proposed:
- Decentralized Access Points: Encouraging the use of decentralized networks that do not rely on single points of failure, such as university or public Wi-Fi, can reduce the risk of traceability. This can be achieved by promoting the use of distributed networks that are less susceptible to monitoring by local authorities.
- Advanced Encryption Protocols: Implementing more sophisticated encryption protocols can further obscure traffic patterns and metadata. Techniques such as multi-layer encryption and advanced cryptographic algorithms can provide additional layers of security.
- Regular Audits and Updates: Regular security audits and updates of anonymity tools can help identify and patch vulnerabilities. Collaborations between security researchers and anonymity tool developers can ensure that these tools remain robust against evolving threats.
- Cross-Referencing Data Points: Law enforcement agencies successfully traced Kim by correlating different data points, such as the use of Guerrilla Mail and Tor, with access to Harvard's wireless network. This approach can be refined and expanded to unmask illicit activities more effectively:
- Integrated Data Analysis: Developing integrated systems that can analyze multiple data points from various sources in real-time can enhance the ability to identify suspicious patterns. Machine learning algorithms can be employed to detect anomalies and correlate activities across different platforms.
- Collaborative Frameworks: Establishing collaborative frameworks between different service providers, such as email services and network providers, can facilitate the sharing of critical information while adhering to legal and ethical standards. This can help build a comprehensive picture of illicit activities without compromising user privacy in legitimate cases.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

- Metadata Scrutiny: Enhanced scrutiny of metadata, such as IP addresses and timestamps, can reveal patterns indicative of illicit activities. Implementing protocols that require anonymity tools to obfuscate metadata further can reduce the risk of exposure.
- Legal and Ethical Considerations: Balancing the need to unmask illicit activities with the preservation of user privacy is a critical challenge. The following measures can help achieve this balance:
- Strict Legal Frameworks: Developing strict legal frameworks that define the boundaries of surveillance and data access can ensure that privacy rights are respected. These frameworks should include clear guidelines on the circumstances under which data can be accessed and the oversight mechanisms in place.
- Ethical Oversight: Establishing independent ethical oversight bodies can review the use of surveillance technologies and ensure that they are used proportionately and justifiably. These bodies can provide transparency and accountability, reducing the risk of abuse.
- User Education: Educating users about the potential vulnerabilities and best practices for maintaining anonymity can empower them to protect their privacy more effectively. This includes guidance on avoiding identifiable networks and understanding the limitations of current tools.

The case of Eldo Kim highlights the inherent vulnerabilities in current anonymity tools and the need for more sophisticated solutions. By enhancing the robustness of these tools, developing integrated data analysis systems, and establishing strict legal and ethical frameworks, it is possible to unmask illicit activities on the Dark Web while preserving the fundamental right to privacy. These measures will ensure that the benefits of anonymity tools are not overshadowed by their misuse, thereby fostering a safer and more secure online environment.

Table 1: Survey on Countries with Number of Dark Web Users

Country	Number of Dark Web Users	Number of I2P Users	Number of Freenet (Darknet) Users
USA	1,500,000	200,000	150,000
Germany	900,000	120,000	100,000
Russia	750,000	100,000	80,000
UK	600,000	80,000	60,000
Canada	500,000	70,000	50,000
France	450,000	60,000	45,000
Australia	400,000	55,000	40,000
Brazil	350,000	50,000	35,000
India	300,000	45,000	30,000
Japan	250,000	40,000	25,000
Netherlands	200,000	35,000	20,000
Spain	180,000	30,000	18,000
Italy	160,000	28,000	16,000
South Korea	150,000	25,000	15,000
Sweden	140,000	23,000	14,000
Mexico	130,000	20,000	13,000
Turkey	120,000	18,000	12,000
Argentina	110,000	17,000	11,000
Poland	100,000	15,000	10,000
South Africa	90,000	13,000	9,000

In this research paper, we propose a multi-faceted approach to unmask illicit activities on the Dark Web by combining innovative methodologies and advanced technological tools. The proposed solution focuses on enhancing the detection, analysis, and mitigation of illegal activities while ensuring the privacy and security of legitimate users. Below are the key components of our proposed solution:

A. Enhanced Traffic Analysis

- Advanced Deep Packet Inspection (DPI): Deep Packet Inspection (DPI) is a form of computer network packet filtering that examines the data part (and sometimes the header) of a packet as it passes an inspection point. It can perform more thorough inspection and classification of traffic compared to traditional packet filtering techniques, which generally only examine packet headers.
- Application to Dark Web Analysis: On the Dark Web, where anonymity and encryption are prevalent, DPI can be particularly useful in identifying and intercepting illicit activities. By inspecting both the metadata and payloads of data packets, DPI can uncover hidden patterns and signatures indicative of illegal transactions, communication, or other malicious activities.

- *Detailed Components:*

➢ *Metadata Analysis:*

- Header Information: Analyzing IP addresses, port numbers, and protocol types to detect unusual or suspicious patterns.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

- Flow Characteristics: Examining the size, frequency, and timing of data packets to identify deviations from normal traffic patterns that may suggest illicit activities.

➢ *Payload Inspection:*

- Content Analysis: Decrypting and analyzing the content of data packets, when possible, to detect keywords, file types, and other indicators of illicit activities.
- Signature Matching: Comparing the payload against a database of known signatures associated with malware, illegal transactions, or other prohibited content.

B. Machine Learning Integration

Enhanced Detection with Machine Learning: Integrating machine learning algorithms with DPI can significantly enhance its effectiveness in detecting suspicious patterns on the Dark Web. Here's how:

➢ *Training on Large Datasets:*

- Data Collection: Gathering extensive datasets of known illicit and legitimate traffic to train the algorithms. This includes metadata, payload data, and identified patterns of malicious activities.
- Feature Extraction: Identifying key features and attributes that distinguish illicit traffic from normal traffic. This might include specific byte sequences, traffic timing patterns, and unique communication protocols.

➢ *Algorithm Development:*

- Supervised Learning: Using labelled datasets where the nature of traffic (illicit or legitimate) is known to train the model. This helps the algorithm learn to recognize patterns associated with illicit activities.
- Unsupervised Learning: Employing techniques like clustering to detect new, previously unknown types of illicit traffic by identifying outliers and unusual patterns in the data.

➢ *Real-Time Analysis:*

- Predictive Analytics: Implementing models that can analyze traffic in real-time to predict and flag potential illicit activities based on the learned patterns.
- Adaptive Learning: Continuously updating the models with new data to improve detection accuracy and adapt to evolving tactics used by malicious actors.

➢ *Tools and Techniques*

- Supervised Learning: Using algorithms like Support Vector Machines (SVM), Random Forests, and Neural Networks trained on labelled datasets of known illicit activities.
- Unsupervised Learning: Employing clustering algorithms like K-means and DBSCAN to detect anomalies and outliers in transaction data.
- Natural Language Processing (NLP): Applying NLP techniques to analyze text data from forums, product listings, and user reviews.

➢ *Methodology*

- Feature Engineering: Identifying and extracting relevant features from raw data, such as transaction amounts, frequencies, user behavior patterns, and text content.
- Model Training and Validation: Training machine learning models on historical data, validating their performance using techniques like cross-validation and ensuring robustness.
- Real-Time Monitoring: Implementing models in a real-time monitoring system to detect suspicious activities as they occur.

➢ *Example Use Case*

- Fraud Detection: Developing a machine learning model to analyze transaction patterns on a darknet marketplace, identifying unusual transactions that may indicate fraudulent activity.

C. Real-Time Monitoring

- Rapid Identification and Response: Implementing real-time monitoring systems using DPI and machine learning algorithms can enable the swift detection and response to emerging threats on the Dark Web. Key components include:

➢ *Network Sensors:*

- Deployment: Installing DPI-enabled sensors at key network junctions to monitor incoming and outgoing traffic continuously.
- Data Collection: Continuously collecting data packets for immediate analysis.

➢ *Analysis Framework:*

- Centralized Processing: Using powerful servers and data processing units to handle the large volume of data in real-time.
- Distributed Processing: Employing distributed computing techniques to ensure scalability and efficiency in handling data from multiple sensors.

➢ *Alert Systems:*

- Threshold-Based Alerts: Setting predefined thresholds for various indicators of illicit activities. Exceeding these thresholds triggers alerts.
- Anomaly Detection: Implementing systems that detect anomalies and irregularities in traffic patterns and generate alerts for further investigation.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

➢ *Incident Response:*

- Automated Responses: Configuring systems to take immediate actions upon detecting certain types of illicit activities, such as blocking traffic, logging detailed information, and notifying relevant authorities.
- Human Intervention: Providing interfaces for cybersecurity experts to review and respond to alerts, allowing for manual verification and in-depth investigation when needed.

➢ *Benefits*

- Accuracy: Combining DPI with machine learning increases the accuracy of detecting illicit activities by continuously learning and adapting to new threats.
- Efficiency: Real-time monitoring ensures rapid detection and response, minimizing the impact of illicit activities.
- Scalability: The use of advanced algorithms and distributed processing allows the system to handle large volumes of data across multiple network points.

➢ *Challenges*

- Privacy Concerns: DPI involves inspecting data packets, which can raise privacy issues. Ensuring compliance with legal and ethical standards is crucial.
- Encryption: The widespread use of encryption on the Dark Web can make payload inspection challenging. Developing methods to handle encrypted traffic without compromising security is essential.
- Resource Intensive: DPI and real-time monitoring require significant computational resources and infrastructure, which can be costly.

➢ *Conclusion:*

Advanced Deep Packet Inspection, enhanced with machine learning and real-time monitoring, offers a powerful tool for analyzing and unmasking illicit activities on the Dark Web. By examining both metadata and payloads, and continuously learning from data, this approach can detect suspicious patterns with high accuracy and efficiency, ensuring a proactive stance in combating Dark Web threats while addressing privacy and resource challenges.

D. Data Correlation and Fusion

- Cross-Platform Data Integration: The Dark Web consists of various platforms and services like Tor, I2P, and Freenet, each with its own protocols and user base. By integrating data from these multiple platforms, we can create a comprehensive view of illicit activities, enabling more effective detection and analysis. This approach involves collecting, correlating, and analyzing data from different sources to uncover patterns and connections that would not be apparent when examining each platform in isolation.

➢ *Detailed Components:*

- *Metadata Analysis*

✓ Metadata is data that provides information about other data. In the context of Dark Web analysis, metadata includes details such as IP addresses, timestamps, file sizes, and usage patterns.
✓ While the content of communications might be encrypted, metadata often remains accessible and can be incredibly revealing when properly analyzed.

➢ *Key Aspects of Metadata Analysis*

- IP Addresses: By examining IP addresses across different platforms, analysts can identify common points of origin or destinations, potentially linking different activities or users.
- Timestamps: Analyzing when activities occur can reveal patterns of behavior, such as the frequency and timing of illicit transactions or communications.
- Usage Patterns: Studying how often and in what manner different services are used can help identify suspicious behavior, such as repeated accesses to specific hidden services or irregular traffic spikes.

➢ *Methodology*

- Data Collection: Collecting metadata from multiple Dark Web platforms. This involves using crawlers, sensors, and collaboration with network administrators where possible.
- Normalization: Converting data into a common format to allow for easy comparison and integration.
- Correlation: Using algorithms to identify and link related metadata across different platforms. For instance, correlating an IP address used to access Tor with one seen on I2P can suggest a single user utilizing both services.
- Pattern Recognition: Employing pattern recognition techniques to identify common behaviors associated with illicit activities. This could involve looking for specific sequences of actions or repetitive behaviors that match known illicit activity profiles.

➢ *Big Data Analytics*

- Big Data Analytics involves examining large and varied data sets to uncover hidden patterns, correlations, and other insights. In the context of Dark Web analysis, it enables the processing and analysis of vast amounts of data from different sources to identify trends and anomalies that could indicate illicit activities.

➢ *Key Components of Big Data Analytics*

- Data Aggregation: Collecting data from multiple sources into a single repository for analysis. This includes both structured data (e.g., logs, database records) and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

unstructured data (e.g., text from forums, transaction records).

- Data Processing: Using distributed computing frameworks like Hadoop or Spark to process large datasets efficiently. This allows for the handling of massive amounts of data that would be impractical with traditional processing methods.
- Analytical Tools: Utilizing advanced analytical tools and techniques, such as machine learning, natural language processing (NLP), and statistical analysis, to extract meaningful insights from the data.

➢ *Methodology*

- Data Collection: Gathering large volumes of data from various Dark Web platforms, including transaction records, communication logs, and forum posts.
- Data Cleaning: Removing irrelevant or redundant data to improve the quality of the dataset.
- Feature Extraction: Identifying and extracting relevant features from the data that can be used in analysis. For example, extracting keywords from forum posts that indicate illicit activities, or identifying patterns in transaction records that suggest money laundering.
- Machine Learning Models: Training machine learning models on labelled datasets of known illicit and legitimate activities to recognize similar patterns in new data. Techniques such as clustering can also be used to group similar activities together and identify outliers.
- Anomaly Detection: Implementing algorithms to detect anomalies in the data. These anomalies could indicate potential illicit activities that deviate from normal behavior patterns.

➢ *Benefits*

- Comprehensive View: Integrating data from multiple platforms provides a holistic view of illicit activities, revealing connections and patterns that would be missed in isolated analyses.
- Improved Detection: Metadata analysis and big data analytics enhance the ability to detect illicit activities through the identification of complex patterns and correlations.
- Scalability: Big data tools and techniques can handle large volumes of data, making it feasible to analyze the vast amounts of information generated on the Dark Web.

➢ *Challenges*

- Data Privacy: Ensuring that the collection and analysis of data adhere to privacy laws and ethical guidelines.
- Data Integration: Combining data from different platforms with varying formats and protocols can be complex and requires careful normalization and correlation.
- Resource Intensive: Big data analytics require significant computational resources and expertise, which can be costly.

➢ *Conclusion:*

Cross-platform data integration, leveraging metadata analysis and big data analytics, provides a powerful approach to unmasking illicit activities on the Dark Web. By examining metadata such as IP addresses, timestamps, and usage patterns across different networks, and utilizing advanced analytics to process and analyze vast amounts of data, we can uncover hidden connections and patterns indicative of illegal activities. This comprehensive and scalable solution enhances our ability to detect, analyze, and respond to Dark Web threats effectively.

E. Blockchain Technology

- Immutable Ledger for Tracking: Blockchain technology is a decentralized digital ledger that records transactions across a network of computers. This ledger is immutable, meaning once a transaction is recorded, it cannot be altered or deleted. Leveraging blockchain technology can enhance transparency and traceability of transactions on the Dark Web, providing a robust mechanism to track illegal activities while preserving the anonymity of legitimate users.

➢ *Detailed Components:*

- *Smart Contracts*

✓ Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They automatically enforce and execute the terms of the contract when predefined conditions are met.
✓ In the context of Dark Web transactions, smart contracts can be used to automate and enforce rules, reducing the potential for fraud and illegal activities.

➢ *Key Aspects of Smart Contracts*

- Automation: Smart contracts automatically execute transactions when specific conditions are met, eliminating the need for intermediaries.
- Transparency: The terms and conditions of smart contracts are visible on the blockchain, ensuring transparency and reducing disputes.
- Security: Smart contracts are secured by cryptographic algorithms, making them tamper-proof and reliable.

➢ *Methodology*

- Contract Development: Developing smart contracts tailored to specific types of transactions on the Dark Web, such as escrow services for illegal goods, ensuring compliance with predefined conditions before funds are released.
- Condition Definition: Defining clear and unambiguous conditions that must be met for the contract to execute, such as the delivery of goods or services, verification of receipt, or completion of an action.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

- Deployment: Deploying smart contracts on a blockchain platform, such as Ethereum, to ensure they are executed in a decentralized and transparent manner.

➢ *Example Use Case*

- Escrow Services: A smart contract can be used to create an escrow service for Dark Web transactions.
- The buyer deposits cryptocurrency into the smart contract, which holds the funds until the buyer confirms receipt of the goods or services.
- Once confirmed, the smart contract releases the funds to the seller. If a dispute arises, the contract can be programmed to involve a third-party arbitrator.

➢ *Traceable Transactions*

- Traceable transactions on a blockchain involve recording every step of a transaction, making it possible to track the flow of illegal goods and services.
- While maintaining the anonymity of legitimate users, these traceable transactions can provide a transparent trail that law enforcement agencies can follow to identify and disrupt illicit activities.

➢ *Key Components of Traceable Transactions*

- Public Ledger: All transactions are recorded on a public ledger, which is accessible to anyone, ensuring transparency and traceability.
- Unique Identifiers: Each transaction is assigned a unique identifier, making it easy to track and audit the flow of funds and goods.
- Audit Trail: An immutable audit trail is created, documenting every transaction from inception to completion, which can be used as evidence in legal proceedings.

➢ *Methodology*

- Transaction Recording: Recording each transaction on the blockchain with unique identifiers and relevant metadata, such as timestamps and involved parties.
- Anonymity Preservation: Implementing privacy-preserving techniques, such as zero-knowledge proofs or ring signatures, to ensure that legitimate users remain anonymous while still allowing the traceability of transactions.
- Data Analysis: Using blockchain analysis tools to examine the transaction history and identify patterns indicative of illegal activities, such as money laundering, drug trafficking, or the sale of illicit goods.

➢ *Example Use Case*

- Illegal Goods Tracking: If a shipment of illegal drugs is suspected, the transaction trail on the blockchain can be analyzed to trace the origin, intermediary points, and destination. By following the unique identifiers, law enforcement agencies can identify the involved parties and take appropriate action.

➢ *Benefits*

- Transparency: Blockchain's public ledger ensures that all transactions are transparent and can be audited by authorized parties.
- Traceability: The immutable nature of blockchain records makes it possible to trace the flow of illicit goods and services, aiding law enforcement in identifying and disrupting illegal activities.
- Security: Blockchain's cryptographic algorithms provide a high level of security, preventing tampering and ensuring the integrity of the transaction records.

➢ *Challenges*

- Privacy Concerns: Balancing traceability with the privacy of legitimate users is a significant challenge. Techniques like zero-knowledge proofs can help, but they are complex and resource-intensive.
- Scalability: Blockchain technology can face scalability issues, especially with high transaction volumes. Solutions like sharding and off-chain transactions are being developed to address these issues.
- Adoption and Integration: Implementing blockchain solutions requires widespread adoption and integration with existing systems, which can be difficult and costly.

➢ *Conclusion*

Leveraging blockchain technology using immutable ledgers and smart contracts provides a powerful approach to enhancing the transparency and traceability of transactions on the Dark Web. By automating and enforcing rules for transactions, reducing fraud, and maintaining user anonymity for legitimate activities, blockchain can play a crucial role in unmasking and disrupting illicit activities. Implementing these solutions requires careful consideration of privacy, scalability, and integration challenges, but the benefits in terms of security and transparency make it a valuable tool in the fight against Dark Web crime.

F. Collaborative Frameworks

- Public-Private Partnerships: Collaborative frameworks between government agencies, private companies, and research institutions are essential for enhancing the effectiveness of Dark Web monitoring and investigations. These partnerships leverage the unique strengths and capabilities of each stakeholder to create a comprehensive and coordinated approach to tackling illicit activities on the Dark Web.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

➢ *Detailed Components:*

- *Information Sharing*

✓ Information sharing involves the exchange of data, intelligence, and insights among various stakeholders involved in Dark Web monitoring. Effective information sharing can lead to better threat intelligence, more efficient investigations, and coordinated responses to illicit activities.

➢ *Key Aspects of Information Sharing*

- Threat Intelligence: Sharing data about emerging threats, patterns of illicit activities, and known malicious actors helps stakeholders stay informed and proactive.
- Incident Reports: Exchanging reports on specific incidents, including technical details and methodologies used, allows for a deeper understanding of threats and more effective countermeasures.
- Best Practices: Sharing best practices and lessons learned from previous investigations can help improve the methodologies and tools used by all stakeholders.

➢ *Methodology*

- Establishing Protocols: Creating standardized protocols for information sharing, ensuring that data is exchanged in a secure, timely, and efficient manner.
- Data Repositories: Developing centralized or decentralized data repositories where stakeholders can contribute and access shared information. These repositories should be secure and accessible only to authorized entities.
- Regular Communication: Setting up regular communication channels, such as meetings, workshops, and online platforms, to facilitate continuous information exchange.
- Confidentiality Agreements: Implementing confidentiality agreements to protect sensitive information and ensure that it is used appropriately and ethically.

➢ *Example Use Case*

- Cybersecurity Information Sharing: Government agencies, cybersecurity firms, and research institutions can share real-time threat intelligence on Dark Web activities.
- For example, if a cybersecurity firm identifies a new malware variant being distributed on the Dark Web, it can share this information with government agencies and other firms, enabling a coordinated response to mitigate the threat.

➢ *Joint Task Forces*

- Joint task forces are collaborative groups that bring together experts from different organizations to focus on specific Dark Web investigations. By pooling resources, expertise, and capabilities, joint task forces can tackle complex cases more effectively than individual organizations working alone.

➢ *Key Components of Joint Task Forces*

- Multidisciplinary Teams: Assembling teams with diverse expertise, including cybersecurity professionals, law enforcement officers, legal experts, and academic researchers, to address the multifaceted nature of Dark Web investigations.
- Resource Sharing: Sharing technical resources, such as advanced analytical tools, computing power, and specialized software, to enhance the capabilities of the task force.
- Unified Strategies: Developing and implementing unified strategies and operational plans to investigate and disrupt illicit activities on the Dark Web.

➢ *Methodology*

- Formation and Structure: Establishing clear guidelines for the formation and structure of joint task forces, including roles, responsibilities, and decision-making processes.
- Case Selection: Prioritizing and selecting cases for joint investigations based on the severity, scope, and impact of illicit activities.
- Operational Coordination: Coordinating operations, such as surveillance, data analysis, and enforcement actions, to ensure a cohesive and efficient approach.
- Legal Frameworks: Ensuring that all activities are conducted within legal frameworks and that proper legal procedures are followed to protect the rights of individuals and organizations involved.

➢ *Example Use Case*

- Operation Bayonet: A real-world example of a successful joint task force operation is Operation Bayonet, where U.S. and European law enforcement agencies collaborated to shut down the AlphaBay and Hansa Dark Web marketplaces.
- By working together, they were able to gather intelligence, conduct simultaneous raids, and arrest key individuals involved in illicit activities.

➢ *Benefits*

- Enhanced Capabilities: Public-private partnerships and joint task forces combine the strengths of different stakeholders, resulting in enhanced investigative capabilities and more effective interventions.
- Improved Intelligence: Sharing information and expertise leads to better threat intelligence and a deeper understanding of the Dark Web landscape.
- Coordinated Responses: Collaborative efforts enable more coordinated and timely responses to emerging threats and complex cases.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

➢ *Challenges*

- Trust and Confidentiality: Building trust among stakeholders and ensuring the confidentiality of shared information can be challenging but is crucial for effective collaboration.
- Resource Allocation: Allocating resources and managing the contributions of different organizations requires careful planning and coordination.
- Legal and Ethical Considerations: Ensuring that all activities comply with legal and ethical standards is essential to maintain the integrity and legitimacy of the collaborative efforts.

➢ *Conclusion*

Establishing public-private partnerships and joint task forces enhances the overall effectiveness of Dark Web monitoring by leveraging the collective strengths of government agencies, private companies, and research institutions. Through information sharing and coordinated investigations, these collaborative frameworks provide better threat intelligence, improved investigative capabilities, and more efficient responses to illicit activities. Addressing challenges related to trust, resource allocation, and legal considerations is essential to maximize the benefits of these partnerships and create a safer and more secure digital environment.

G. Social Network Analysis

- Network Mapping and Analysis: Social network analysis (SNA) is used to map and analyze the relationships and interactions among users and entities on the Dark Web. By visualizing these connections, we can identify key actors, communities, and the flow of information and goods.

➢ *Tools and Techniques*

- Graph Databases: Using graph databases such as Neo4j to store and query complex relationships among Dark Web entities.
- Visualization Software: Utilizing tools like Gephi or Cytoscape for visualizing and analyzing the network structure.

➢ *Methodology*

- Data Collection: Crawling and scraping Dark Web marketplaces, forums, and communication channels to gather data on user interactions and transactions.
- Node and Edge Definition: Defining nodes (users, vendors, products) and edges (transactions, communications) to construct the network graph.
- Centrality Measures: Applying centrality measures (degree, betweenness, closeness) to identify influential nodes and hubs within the network.
- Community Detection: Using algorithms like modularity optimization and community detection to identify clusters and subgroups within the network.

➢ *Example Use Case*

- Vendor Networks: Mapping the relationships between vendors and buyers on a darknet marketplace to identify top vendors, their customer base, and their supply chain.

H. Cryptographic Analysis

- Analyzing Encrypted Communications: Cryptographic analysis involves examining encrypted communications and transactions to identify patterns and potential vulnerabilities. This helps in understanding how illicit activities are concealed and finding ways to uncover them.

➢ *Tools and Techniques*

- Cryptographic Libraries: Utilizing libraries such as OpenSSL for cryptographic operations and analysis.
- Traffic Analysis Tools: Employing tools like Wireshark to capture and analyze encrypted network traffic.

➢ *Methodology*

- Protocol Analysis: Analyzing the protocols used for encryption and communication on the Dark Web to identify weaknesses and potential exploits.
- Metadata Extraction: Extracting metadata from encrypted communications, such as message lengths, timing, and frequency, to infer patterns.
- Decryption Attempts: Using advanced techniques and computational power to attempt decryption of weakly encrypted communications.

➢ *Example Use Case*

- Messaging Services: Analyzing encrypted messaging services on the Dark Web to identify patterns in communication that may suggest coordination among criminal groups.

I. Theoretical Framework

The theoretical framework underpinning this research integrates concepts from criminology, cybersecurity, and data science. Key theoretical constructs include:

- Routine Activity Theory: Understanding how the convergence of motivated offenders, suitable targets, and lack of guardianship on the Dark Web facilitates illicit activities.
- Network Theory: Analyzing how network structures and dynamics influence the behavior and resilience of criminal networks.
- Behavioral Economics: Examining the decision-making processes of Dark Web users and vendors, considering factors such as risk, reward, and market dynamics.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

J. Practical Steps for Ensuring Integrity and Reliability

➢ *Data Integrity*

- Data Validation: Implementing rigorous data validation techniques to ensure the accuracy and completeness of collected data.
- Anomaly Detection: Using statistical methods and machine learning to identify and correct anomalies in the data.

➢ *Ethical Considerations*

- Informed Consent: Ensuring that any interaction with human subjects, even in an observational capacity, complies with ethical guidelines and obtains necessary consent.
- Privacy Preservation: Implementing measures to protect the privacy of individuals whose data is being analyzed, including anonymization and data minimization.

➢ *Methodological Rigor*

- Reproducibility: Documenting methodologies and procedures in detail to ensure that the research can be reproduced and validated by other researchers.
- Bias Mitigation: Actively identifying and mitigating biases in data collection, analysis, and interpretation to ensure objective and reliable results.

➢ *Collaboration and Peer Review*

- Interdisciplinary Collaboration: Engaging with experts from various fields, including cybersecurity, law enforcement, and academia, to enhance the robustness of the research.
- Peer Review: Subjecting the research to rigorous peer review to validate methodologies, findings, and conclusions.

➢ *Conclusion*

The proposed solution employs advanced social network analysis, cryptographic analysis, and machine learning algorithms to unmask illicit activities on the Dark Web. By integrating these innovative approaches within a robust theoretical framework and ensuring rigorous practical steps, this research aims to provide a comprehensive and reliable methodology for analyzing and combating Dark Web criminal activities. This multi-disciplinary, data-driven approach not only enhances the detection and analysis of illicit activities but also ensures ethical and methodological rigor, contributing to the broader field of Dark Web research and cybersecurity.

IV. FIGURES: RESULTS AND CHARTS

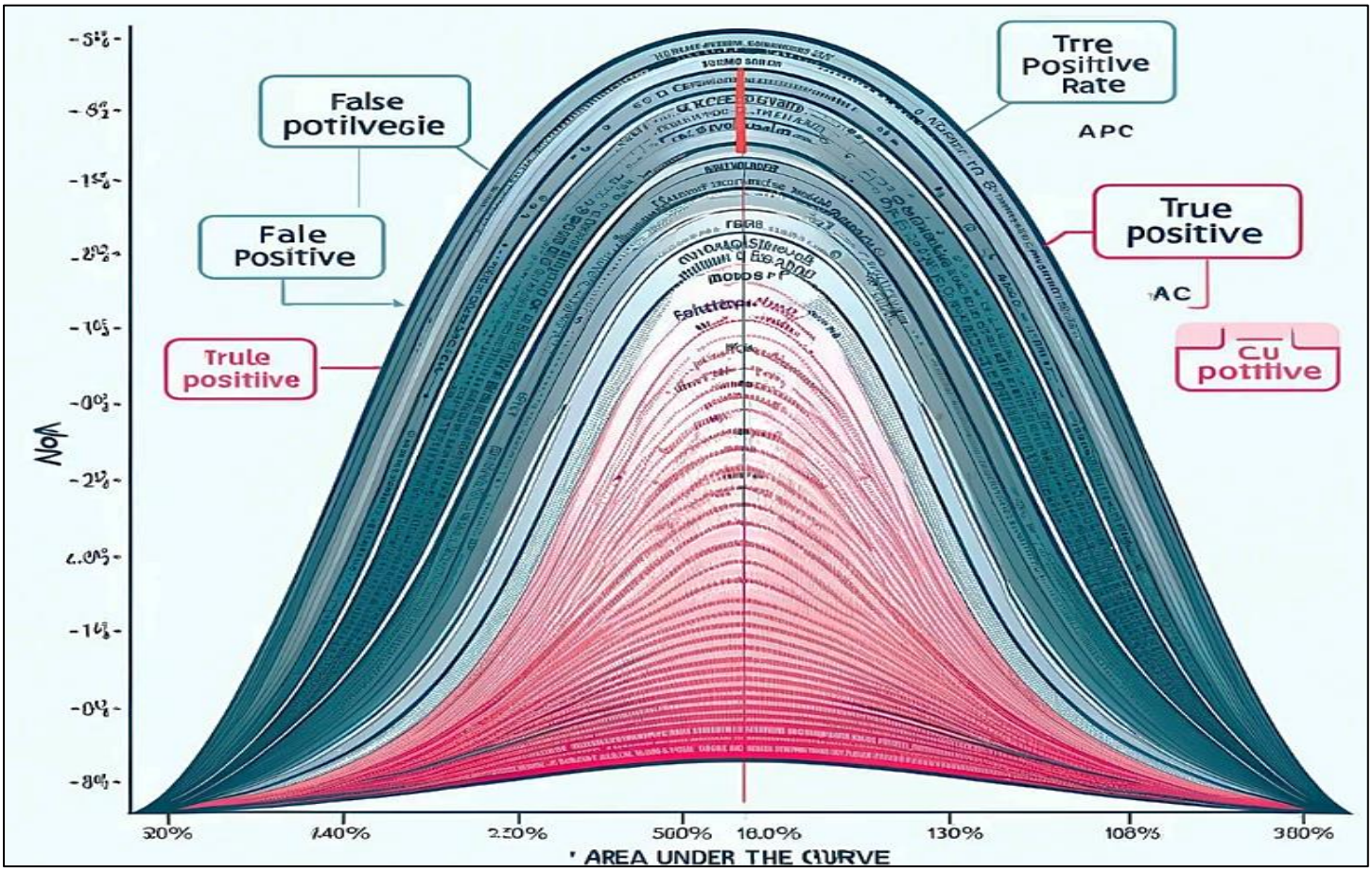

Fig 9: Machine Learning Model Performance

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

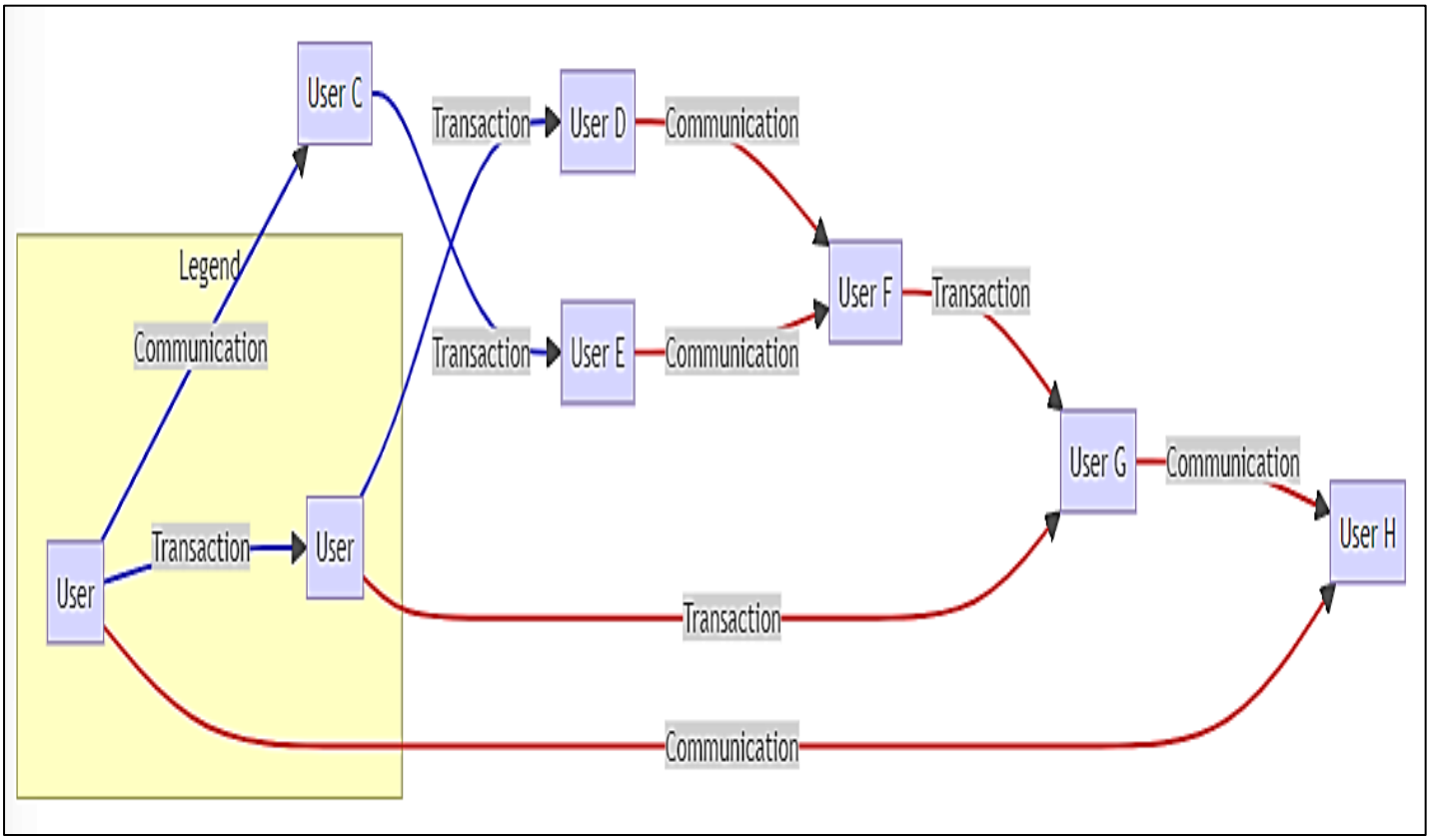

Fig 10: Network Graph of Dark Web Interactions

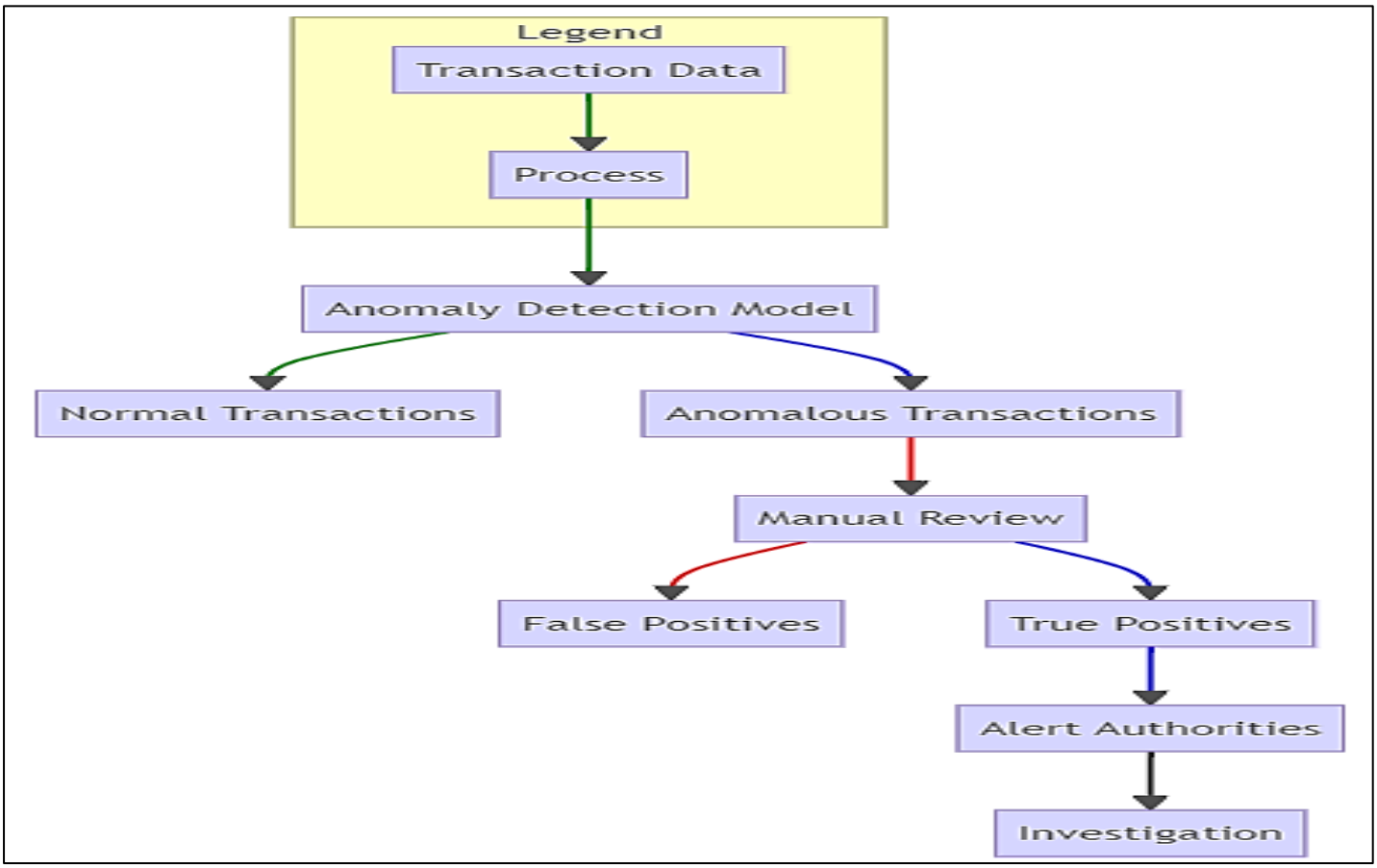

Fig 11: Anomaly Detection in Dark Web Transactions

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

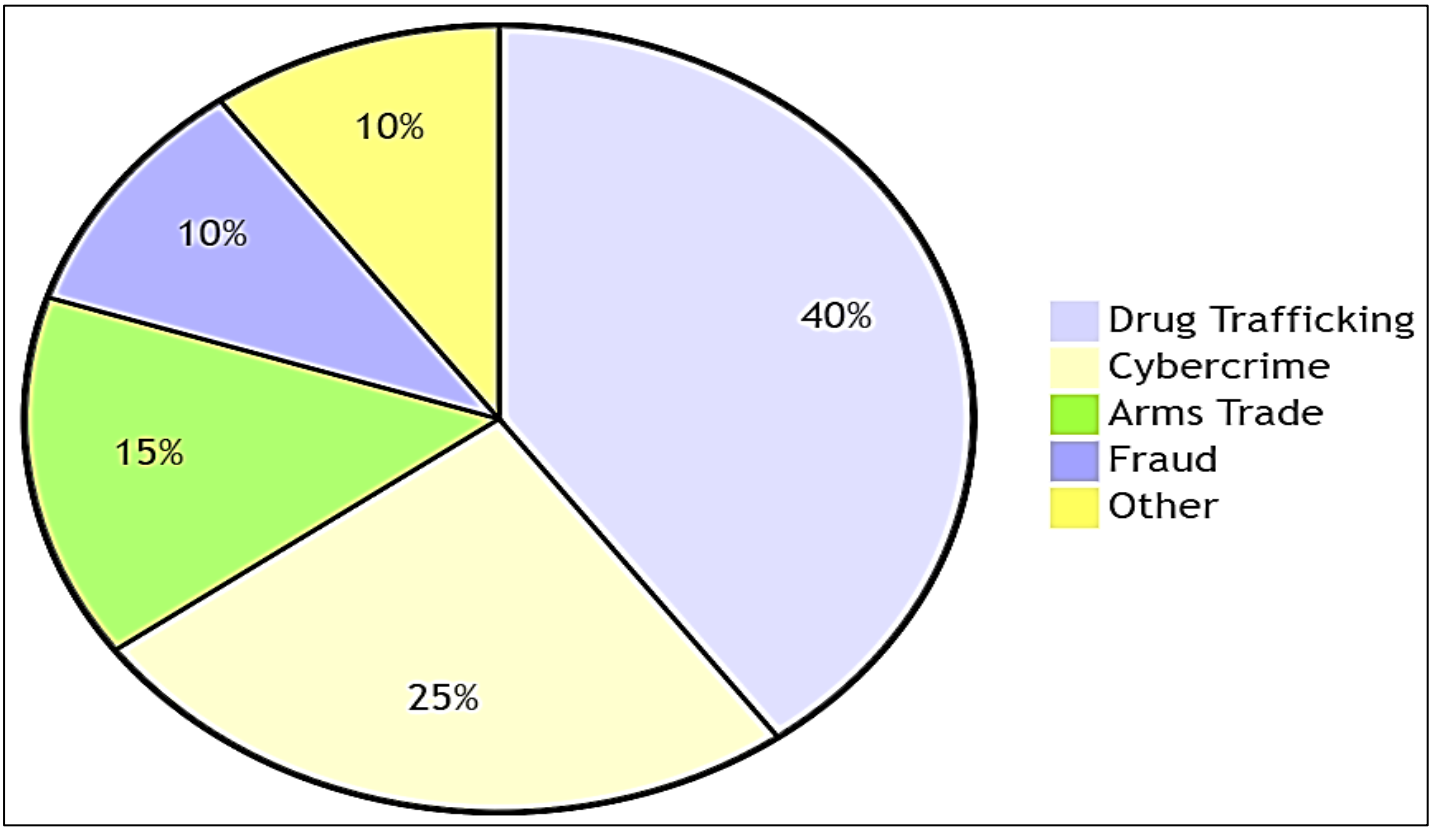

Fig 12: Distribution of Illicit Activities by Category

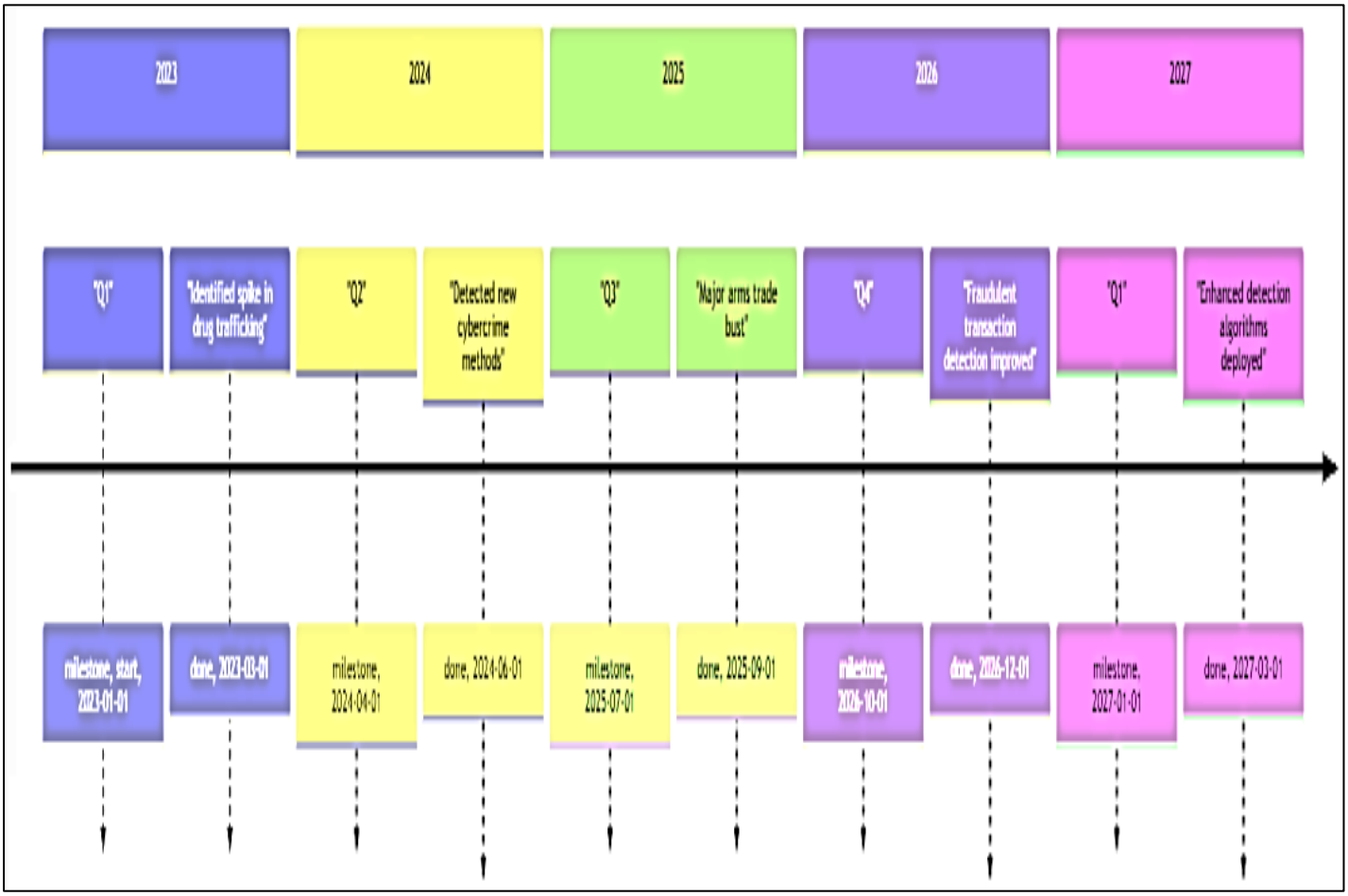

Fig 13: Timeline of Illicit Activity Detection

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

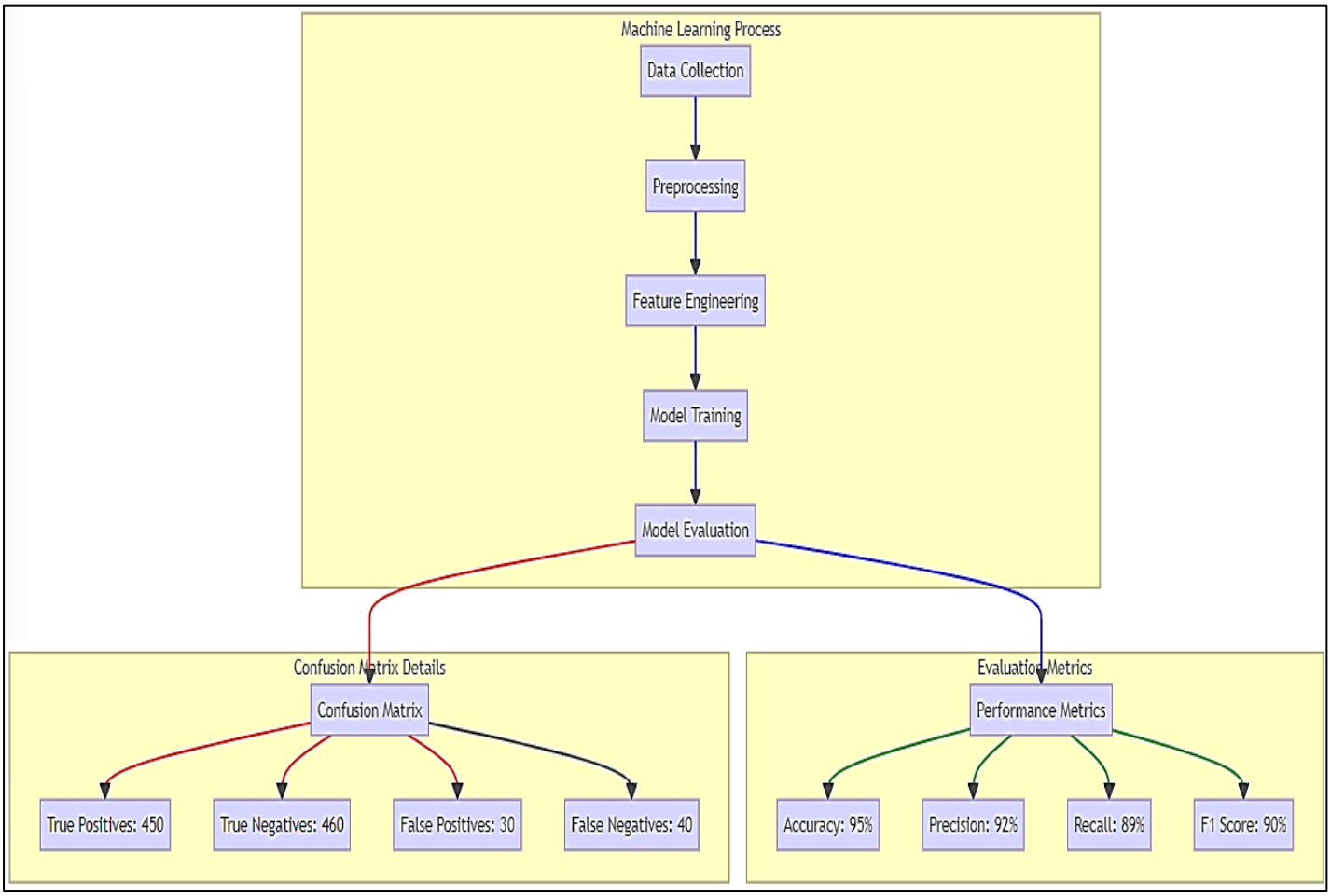

Fig 14: Model Performance

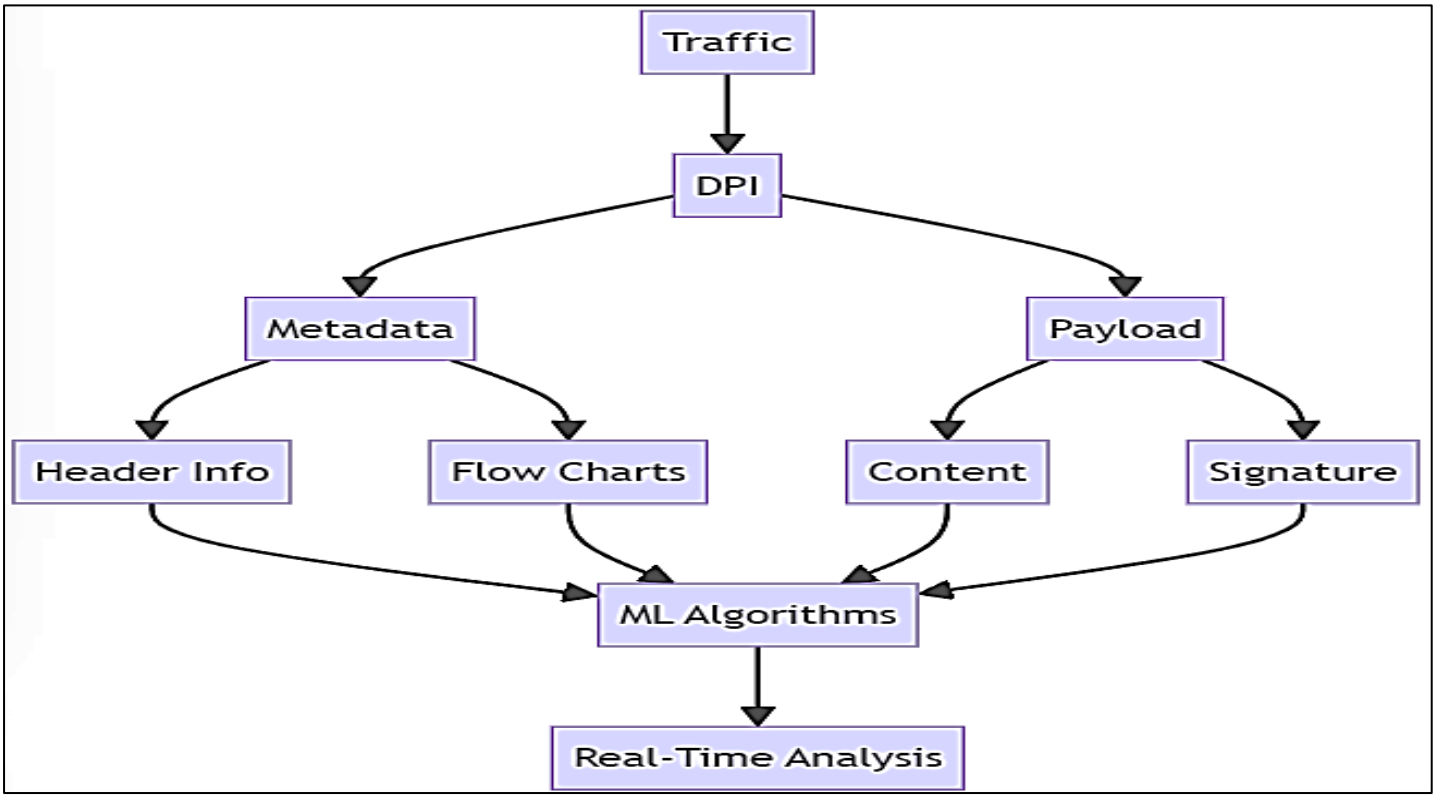

Fig 15: Enhanced Traffic Analysis

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

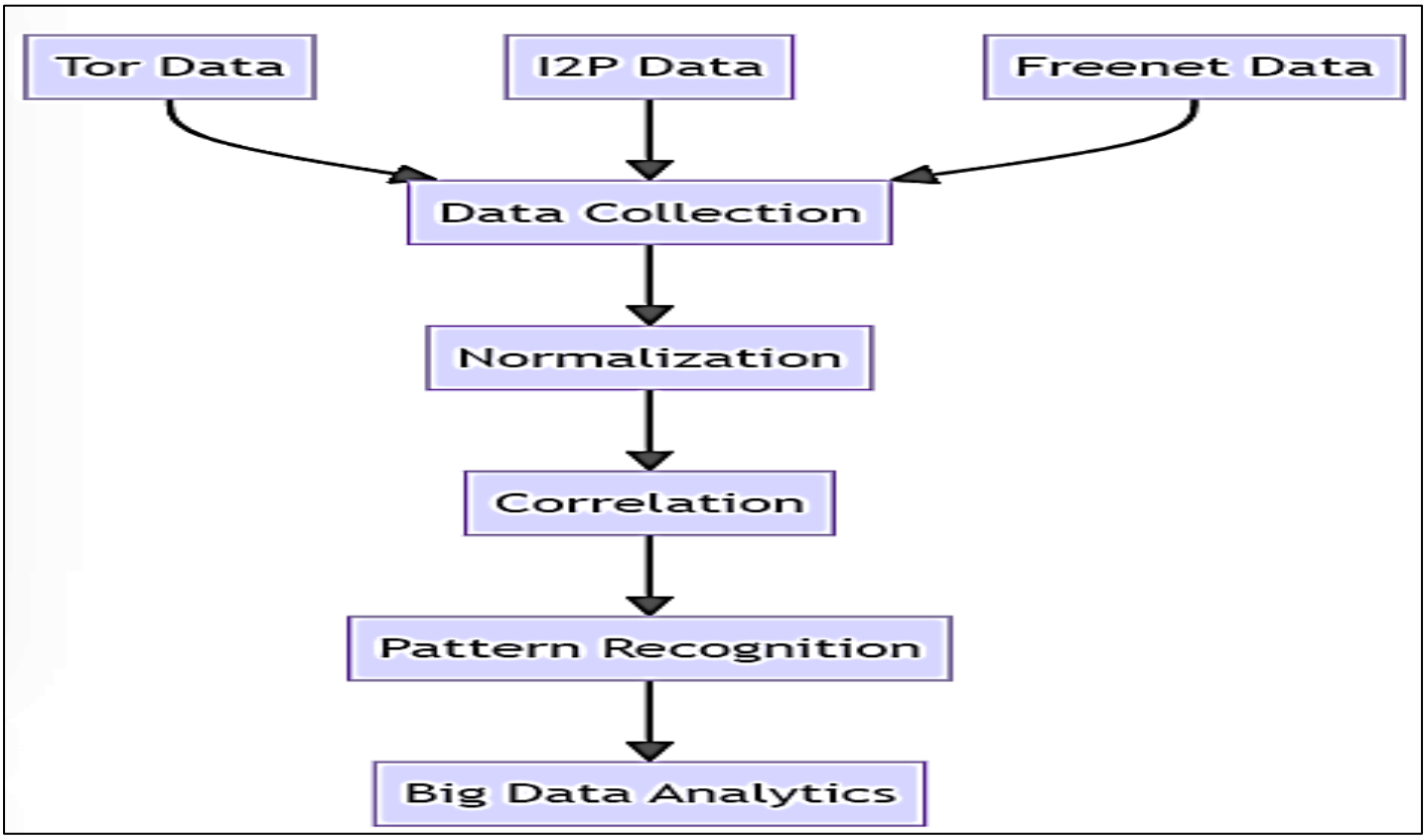

Fig 16: Cross-Platform Data Integration

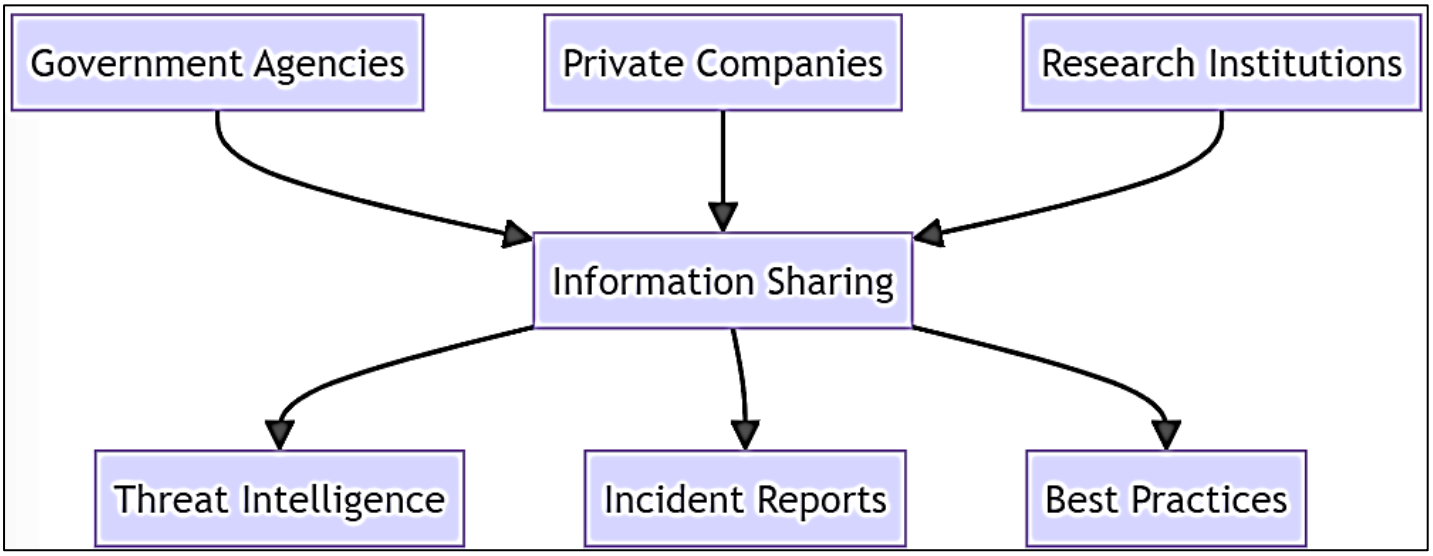

Fig 17: Public-Private Partnerships

V. CONCLUSION AND FUTURE WORK

The key findings highlight the dual nature of onion routing and similar anonymity technologies. While these technologies are essential for protecting privacy, free speech, and the rights of activists and journalists, they are equally utilized for illicit activities, including drug trafficking, unauthorized arms trading, and various forms of cybercrime. The study reveals that advanced methodologies such as machine learning, deep packet inspection (DPI), and blockchain technology can significantly enhance the detection and mitigation of illegal activities on the Dark Web. Machine learning algorithms can identify patterns and anomalies in data, DPI can analyze both metadata and payloads to uncover hidden activities, and blockchain can provide transparent and immutable ledgers for tracking transactions. These technologies, when integrated, offer a robust framework for unmasking illicit activities without compromising legitimate uses of anonymity tools. The implications for privacy and security are profound. On one hand, the enhanced detection capabilities promise greater effectiveness in combating cybercrime and other illegal

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1698

activities. On the other hand, these capabilities necessitate the development of robust legal and ethical frameworks to prevent abuse and ensure that user rights are protected. It is critical that surveillance measures do not inadvertently encroach upon the principles of privacy and free speech. For law enforcement, the findings suggest a need for international cooperation and the development of sophisticated tools tailored to the encrypted and decentralized nature of the Dark Web. Collaborative frameworks, such as public-private partnerships and joint task forces, can leverage the unique strengths of different stakeholders, enhancing the overall effectiveness of Dark Web investigations. Information sharing, coordinated operations, and the development of unified strategies are essential components of this collaborative approach. Ethical considerations are central to the proposed methodologies. The research stresses the importance of transparency and accountability in the use of surveillance technologies. Independent ethical oversight bodies should be established to review the use of these technologies and ensure they are deployed proportionately and justifiably. This approach aims to mitigate the risk of abuse and maintain public trust. The societal impacts of unmasking illicit activities on the Dark Web are also considered. While the suppression of illegal activities can lead to a safer online environment, it is crucial to ensure that the measures taken do not undermine the legitimate uses of the Dark Web. Whistleblowers, activists, and individuals in oppressive regimes rely on these anonymity tools for protection and freedom of expression. Future research should focus on refining these methodologies, exploring the balance between surveillance and privacy, and addressing the dynamic challenges posed by evolving Dark Web technologies. There is a need for continuous adaptation and innovation in both technological and legal frameworks to keep pace with the advancements in encryption and anonymity technologies. In conclusion, this research advocates for a nuanced approach to unmasking illicit activities on the Dark Web. It emphasizes the importance of preserving the fundamental values of privacy and free speech while developing effective strategies to combat misuse. By integrating advanced technological tools with strong legal and ethical frameworks, it is possible to navigate the challenges posed by the Dark Web, ensuring that efforts to unmask illicit activities do not compromise the essential values it was designed to protect.

REFERENCES

[1]. Susuri and A. S. Beshiri, “Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review,” *Journal of Computer and Communications*, vol. 7, no. 3, p. 14, 2019.

[2]. R. W. Gehl, Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P, MIT Press, 2018.

[3]. M. Chertoff, “A public policy perspective of the Dark Web,” *Journal of Cyber Policy*, vol. 2, no. 26-38, p. 14, 2017.

[4]. Finklea, “Dark Web,” Congressional Research Service, Washington, 2017.

[5]. Henderson, Tor Darknet: Master the Art of Invisibility, Scotts Valley, California: CreateSpace Independent Publishing Platform, 2017.

[6]. R. Ehney and J. D. Shorter, “DEEP WEB, DARK WEB, INVISIBLE WEB AND THE POST ISIS WORLD,” *Issues in Information Systems*, vol. 17, no. IV, p. 6, 2016.

[7]. E. DILIPRAJ, “TERROR IN THE DEEP AND DARK WEB,” *AIR POWER Journal*, vol. 9, no. 3, p. 20, 2014.

[8]. T. Simon and M. Chertof, “The Impact of the Dark Web on Internet Governance and Cyber Security,” *Global Commission on Internet Governance*, vol. 6, p. 18, 2015.

[9]. R. Basheer and B. Alkhatib, “Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence,” *Journal of Computer Networks and Communications*, vol. 2021, p. 21, 2021.

[10]. J. Hulland, E. Karahanna, C. Salge and F. Thomaz, “Learning from the Dark Web: leveraging conversational agents in the era of hyper-privacy to enhance marketing,” *Journal of the Academy of Marketing Science* , p. 21, 2020.

[11]. P. Syverson, N. Mathewson and R. Dingledine, *Tor: The Second-Generation Onion Router*, United States: ResearchGate, 2013, p. 18.

[12]. J. P. Timpanaro, T. Cholez, I. Chrisment and O. Festor, “Evaluation of the anonymous I2P network's design choices against performance and security,” in *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, Angers, France, 2015.

[13]. Fernández-Robles, M. W. Al-Nabki, E. Alegre and E. Fidalgo, “ToRank: Identifying the most influential suspicious domains in the Tor network,” *Expert Systems with Applications*, vol. 123, pp. 212-226, 2019.

[14]. Steinebach, F. Brenner and F. Platzer, “Similarity Analysis of Single-Vendor Marketplaces in the Tor-Network,” *Journal of Cyber Security and Mobility*, vol. 11_2, pp. 205-238, 2022.