International Journal of Scientific Engineering and Science
Volume 10, Issue 8, pp. 82-92, August 2026. ISSN (Online): 2456-7361

Development of an Enhanced Model to Track Illegal Transactions on the Dark Web

Larry Efe Oboh[1], Ifeanyi Godspower Akawuku[2], Ezeamasoibi Chibuzor E.[3]
[1,2]Department of Computer Science, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.
[3]African Institute of Science and Technology, Abuja
Email address: le.oboh@pg.unizik.edu.ng, gi.akawuku@unizik.edu.ng

Abstract— *The rapid growth of illegal activities on the Dark Web has significantly increased the use of cryptocurrencies for anonymous financial transactions, creating major challenges for cybersecurity investigators and digital forensic analysts. Existing approaches to transaction tracking are often fragmented, relying on isolated blockchain analysis, natural language processing, or machine learning techniques, which limits their ability to correlate financial and textual intelligence in real time. This study developed an Enhanced Transaction Tracking Framework (ETTF) to improve the detection, analysis, and monitoring of illegal cryptocurrency transactions on the Dark Web. The framework was developed using the Python programming language and adopted the Design Science Research (DSR) methodology to integrate blockchain forensics, Natural Language Processing (NLP), graph analytics, machine learning, and visualization into a unified architecture. The proposed framework incorporates modules for data acquisition, preprocessing, blockchain analysis, NLP, graph analytics, machine learning, decision support, and visualization to provide comprehensive intelligence for cybersecurity investigations. System evaluation was conducted using eight functional test cases covering data acquisition, preprocessing, transaction analysis, feature extraction, visualization, integration, performance, and accuracy. The results showed that the framework successfully passed all test cases, achieving a 100% success rate and demonstrating reliable performance in identifying suspicious transactions, generating risk-based alerts, and producing actionable analytical reports. The study concludes that the Enhanced Transaction Tracking Framework provides a scalable, secure, and effective solution for strengthening blockchain transaction analysis, Dark Web intelligence gathering, and digital forensic investigations, thereby enhancing proactive cybercrime detection and decision-making.*

Keywords— *Dark Web, Blockchain Forensics, Cryptocurrency, Machine Learning, Natural Language Processing, Digital Forensics, Cybersecurity.*

I. INTRODUCTION

Every day, millions of dollars flow through the dark web's hidden marketplaces untraceable, unregulated, and largely unpunished (Europol, 2023; UNODC, 2023). Anonymity was designed to protect the vulnerable, yet it has become the shield of the criminal class. For journalists and activists, networks like Tor and I2P offer a vital defense against oppression. For criminals, however, these same tools enable a sprawling underground economy where narcotics, stolen data, ransomware, and hacking services are traded with alarming impunity (Europol, 2023; Christin, 2013).

Cryptocurrencies have become the financial backbone of this illicit ecosystem (Foley et al., 2019). Bitcoin, Monero, Zcash, and similar digital assets offer decentralized architectures that criminals exploit to obscure their tracks (Möser et al., 2013). But the challenge runs deeper. Cybercriminals continuously deploy advanced obfuscation tactics, mixers, tumblers, chain-hopping strategies, and privacy-enhanced coins to sever financial trails (Möser et al., 2013; Chainalysis, 2025). How do we trace transactions when the trail dissolves into cryptographic fog within seconds? These techniques render traditional blockchain analysis increasingly ineffective and place immense strain on investigators (Chainalysis, 2025).

Current monitoring systems, while valuable, operate in isolation. Some rely on heuristic blockchain analysis. Others scrape darknet forums for keywords or apply isolated machine learning models (Akcora et al., 2020). Few, however, synthesize these disparate data streams into a coherent intelligence picture. This fragmentation produces slow response times, high false-positive rates, and intelligence that quickly becomes outdated (Europol, 2023). The field lacks a unified system capable of correlating a suspicious wallet transaction with a specific threat actor's activity on a marketplace. Put simply: we are fighting an interconnected threat with disconnected tools.

This research addresses that critical gap by proposing an Enhanced Transaction Tracking Framework (ETTF). Unlike existing approaches, our model is not another standalone tool. It is a unified architecture that fuses blockchain forensics, natural language processing, graph analytics, and machine learning (Akcora et al., 2020). The ETTF integrates financial intelligence with textual analysis extracted from dark web communications. In doing so, it constructs a holistic picture of criminal networks and their operational patterns. The objective is to move beyond reactive investigation toward proactive threat detection providing analysts with a more accurate, automated, and scalable solution.

The practical implications of this work are substantial. The framework offers cybersecurity professionals, digital forensic investigators, and intelligence agencies a concrete platform to enhance their investigative capabilities. By improving transaction tracing, identifying suspicious behavioral patterns, and uncovering criminal networks, the ETTF contributes directly to strengthening digital forensic investigations. Ultimately, this research provides the tools necessary to effectively monitor and disrupt the financial lifeblood of organized cybercrime, thereby improving cybersecurity resilience against emerging threats.

International Journal of Scientific Engineering and Science
Volume 10, Issue 8, pp. 82-92, August 2026. ISSN (Online): 2456-7361

Summary of Related Works

TABLE 1: Summary of Related Works

S/N	Author(s) & Year	Methodology	Strength	Limitations
1	Martin (2014)	Marketplace analysis of Silk Road	First systematic study of dark web marketplace operations; laid groundwork for understanding underground e-commerce	Focused solely on marketplace dynamics; did not address tracking or detection methods
2	Meiklejohn et al. (2013)	Blockchain analysis of Bitcoin transactions using address clustering and transaction flow tracing	Demonstrated the feasibility of tracing Bitcoin transactions; pioneered address clustering techniques	Limited to pseudonymous blockchain data; ineffective against privacy coins such as Monero
3	Holt et al. (2015)	Rogue Network Model for dark web network structures	Provides insight into network resilience and adaptability in encrypted environments	Focuses only on network structure; does not support real-time detection
4	Foley, Karlsen, &Putniņš (2019)	Cryptocurrency analysis linking Bitcoin transactions to illicit activities	Quantified the proportion of Bitcoin transactions associated with illegal activities	Limited by Bitcoin pseudonymity; privacy coins complicate transaction tracing
5	Zohar et al. (2019)	Dark Web Market Model exploring trust and marketplace dynamics	Explains trust mechanisms such as ratings, escrow services, and reputation systems in anonymous markets	Overlooks technical tracking methods; limited to marketplace dynamics
6	Soska & Christin (2015)	Longitudinal analysis of multiple dark web marketplaces	Identified patterns in vendor behavior, product offerings, and marketplace life cycles	Focuses on behavioral patterns rather than transaction detection or tracking
7	Munksgaard & Demant (2016)	Linguistic analysis of communication practices in hidden markets	Examined coded language, negotiation tactics, and anonymity practices among users	Focuses on communication behavior rather than technical tracking mechanisms
8	Lamy et al. (2019)	Hybrid approach combining network analysis and machine learning	Successfully detected hidden criminal networks using graph-based learning techniques	Limited scalability for very large networks; computationally intensive
9	Teng et al. (2020)	Machine learning algorithms for anomaly detection	Automated detection of money laundering and human trafficking patterns	Susceptible to false positives; performance depends on training data quality
10	Anderson et al. (2020)	Blockchain forensic tools for suspicious transaction analysis	Enhanced blockchain investigations with practical law enforcement applications	Less effective against mixers, tumblers, and privacy-focused cryptocurrencies
11	Décary-Hétu &Giommoni (2017)	Analysis of reputation systems and vendor rating mechanisms	Demonstrated how trust-building mechanisms enhance the resilience of dark web markets	Focuses on social mechanisms rather than technical tracking approaches
12	Ladegaard (2019)	Socio-technical analysis of dark web communities	Examined community formation based on trust, reputation, and peer validation	Concentrates on social dynamics rather than detection technologies
13	Conti et al. (2018)	Graph-based blockchain transaction analysis	Visualized relationships among wallets, nodes, and exchanges to identify criminal hubs	Emphasizes visualization rather than automated threat detection
14	Ghanem et al. (2023)	D2WFP forensic protocol for dark and deep web investigations	Comprehensive protocol covering data acquisition, artifact identification, and forensic analysis	Protocol-based approach may struggle to adapt to rapidly evolving platforms
15	Yang et al. (2023)	Real-time AI-driven Natural Language Processing (NLP) surveillance for dark web forums	Provides timely alerts for suspicious keywords and semantic patterns	Computationally intensive; limited to forum content rather than transaction networks
16	Xia et al. (2024)	Blockchain address mapping of cryptocurrency-related onion services	Analyzed approximately 5,000 onion sites and identified over 1,100 criminal blockchain addresses	Limited by the number of onion sites examined; narrow focus on address mapping
17	Saxena et al. (2023)	VendorLink: NLP-based vendor alias detection system	Detects vendor identity manipulation and migration across dark web marketplaces	Limited to vendor alias tracking; does not support end-to-end transaction tracing
18	Bakermans et al. (2025)	Deep learning using Named Entity Recognition (NER)	Achieved 94% F1 score; automates multilingual intelligence extraction from dark web forums	Requires extensive labeled datasets; raises privacy concerns
19	Caldwell et al. (2020)	Domain-specific NLP lexicons for dark web content analysis	Recognizes illicit keywords, coded language, and obfuscation techniques	Focuses on linguistic analysis rather than financial transaction tracking
20	Nashaat et al. (2022)	Reinforcement learning for attacker behavior prediction	Simulates criminal behavior to enable proactive threat response	Emerging approach with limited real-world validation
21	Kethineni et al. (2018)	AI-driven pattern recognition and behavioral analytics	Detects suspicious activities using predictive behavioral analysis	Focuses on behavioral prediction rather than integrated transaction tracking
22	Nofer et al. (2017)	Analysis of privacy-focused cryptocurrencies (e.g., Monero)	Examined tracing limitations introduced by privacy-enhancing transaction features	Identifies challenges without proposing practical tracking solutions
23	Chen et al. (2020)	Unsupervised machine learning for hidden network discovery	Identifies indirect links and latent relationships within encrypted datasets	Focuses on clustering rather than real-time transaction monitoring
24	Al Nabki et al. (2019)	Analysis of reputation systems and consumer behavior in dark web markets	Demonstrated how reputation influences pricing, trust, and customer loyalty	Focuses on behavioral economics rather than transaction tracking
25	Zhang et al. (2021)	Deep learning for money laundering anomaly detection	Automated detection of suspicious financial transaction patterns	Accuracy depends heavily on the quality and diversity of training datasets

Knowledge Gap: Lapses and Shortcoming

TABLE 2: Knowledge Gap: Lapses and Shortcoming

Research Gap	Description	Implication for the Proposed ETTF
Fragmented Approaches	Existing studies investigate blockchain analysis, natural language processing (NLP), machine learning, and graph analytics as separate techniques, with limited integration across multiple data sources.	ETTF integrates blockchain forensics, NLP, graph analytics, and machine learning into a unified intelligence framework capable of correlating financial and textual evidence.
Obfuscation Challenges	Privacy-enhancing technologies such as Monero, Zcash, cryptocurrency mixers, tumblers, and chain-hopping techniques reduce the effectiveness of conventional blockchain tracing methods.	ETTF employs multi-source intelligence and behavioral analytics to improve transaction tracing despite advanced obfuscation techniques.
Limited Scope of Existing Studies	Most research focuses on dark web marketplaces, while forums, encrypted messaging platforms, and other hidden communication channels receive comparatively little attention.	ETTF expands intelligence collection by incorporating data from multiple dark web sources, enabling broader situational awareness.
Lack of Real-Time Monitoring	Most existing systems perform retrospective or post-incident analysis, resulting in delayed detection and limited support for proactive investigations.	ETTF supports continuous monitoring and near real-time threat detection to facilitate timely investigative responses.
Absence of a Unified Framework	Current approaches lack an integrated and scalable platform capable of simultaneously analyzing cryptocurrency transactions, textual communications, network relationships, and behavioral patterns.	ETTF provides a comprehensive framework that fuses financial, textual, and relational intelligence to improve cybercrime investigation and digital forensic capabilities.

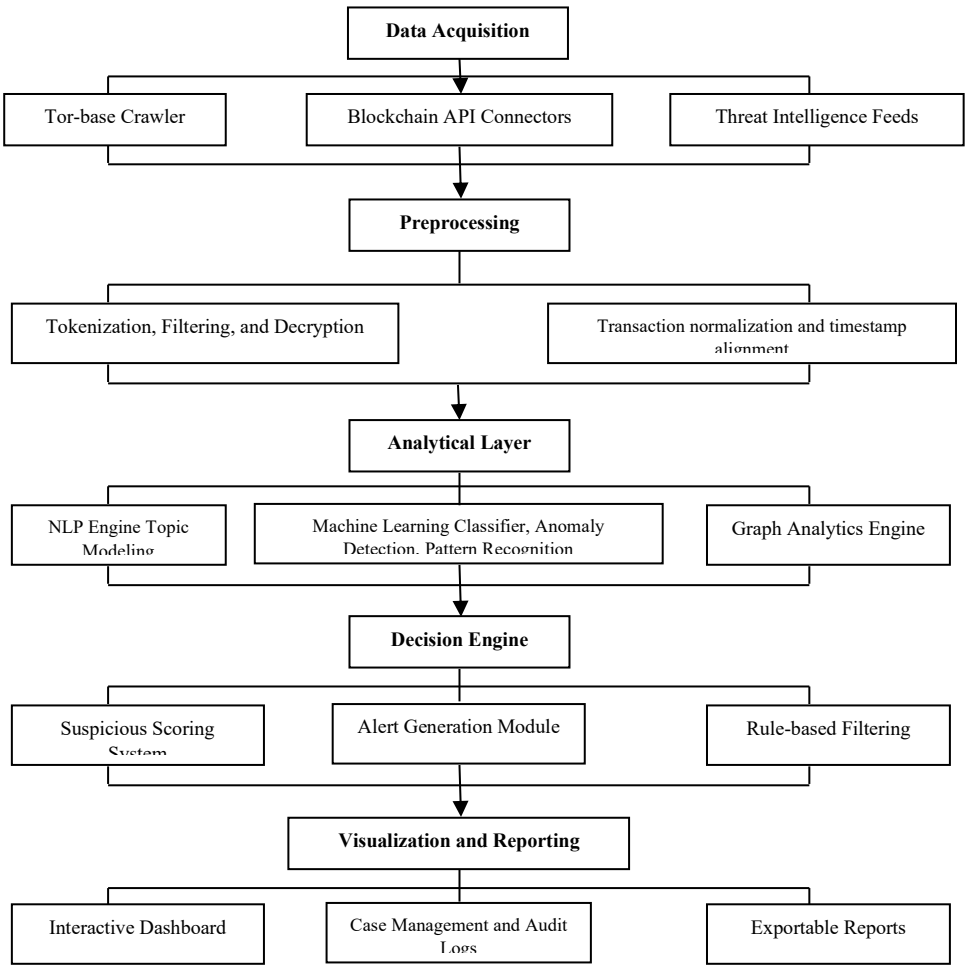

Figure 1. High Level Model ETTF

Summary of the Research Gap

The review of related studies demonstrates that existing approaches remain fragmented, with blockchain analytics, natural language processing, graph analytics, and machine learning typically implemented in isolation. Furthermore, advanced cryptocurrency obfuscation techniques, the limited coverage of dark web communication channels, the lack of real-time monitoring, and the absence of an integrated analytical framework significantly constrain current investigative capabilities. These limitations justify the development of the proposed Enhanced Transaction Tracking Framework (ETTF), which unifies blockchain forensics, natural language processing, machine learning, and graph analytics into a comprehensive, scalable, and real-time intelligence platform

for enhanced dark web transaction tracking and cybercrime investigation.

II. Materials and Methods

The Enhanced Transaction Tracking Framework (ETTF) is an intelligent model developed using the Python programming language to improve the detection and tracking of illegal cryptocurrency transactions on the dark web. The framework integrates blockchain forensics, natural language processing (NLP), graph analytics, and machine learning to provide a unified platform for transaction analysis and cybercrime intelligence. The Design Science Research (DSR) methodology was adopted because of its suitability for designing and evaluating innovative cybersecurity solutions. The methodology facilitates the development of a structured framework by integrating multiple analytical components into a unified system capable of addressing complex investigative challenges (Peffers et al., 2007). As depicted in Figure 1, the ETTF architecture implements a layered design that integrates all functional components to provide efficient transaction monitoring and intelligence generation. The framework consists of interconnected layers responsible for data acquisition, preprocessing, analytical processing, decision support, and visualization. Data collected from blockchain networks and dark web sources are processed using machine learning algorithms, NLP techniques, and graph-based analysis to identify suspicious transactions and relationships among entities. The processed information is evaluated by the decision engine, while the visualization layer presents actionable intelligence through an interactive interface for cybersecurity analysts and digital forensic investigators. The modular architecture enhances scalability, improves transaction traceability, and supports proactive detection of illegal financial activities on the dark web.

Functional Requirements

As shown in Table 3, the functional requirements define the core capabilities of the Enhanced Transaction Tracking Framework (ETTF). The framework incorporates essential functionalities such as data acquisition from blockchain networks and dark web sources, data preprocessing, blockchain transaction analysis, natural language processing, graph analytics, machine learning-based anomaly detection, decision support, visualization and reporting, user management, and audit logging. These modules operate collaboratively to provide a unified platform for tracking illegal transactions, identifying suspicious activities, and generating actionable intelligence for cybersecurity analysts and digital forensic investigators.

The non-functional requirements presented in Table 4 define the quality attributes and operational characteristics required for the effective performance of the Enhanced Transaction Tracking Framework (ETTF). These requirements ensure that ETTF can efficiently process, analyze, and track large volumes of blockchain transaction records and related intelligence data while maintaining optimal performance, reliability, and scalability. The performance and scalability requirements enable the framework to handle increasing transaction volumes and investigative workloads without significant reduction in processing efficiency.

TABLE 3: Functional Requirements

S/N	Module	Functional Requirements
1	Data Acquisition	Collect cryptocurrency transaction data from blockchain networks and dark web intelligence from marketplaces, forums, and threat feeds.
2	Data Preprocessing	Clean, normalize, tokenize, and transform collected data into a structured format suitable for analysis.
3	Blockchain Analysis	Trace cryptocurrency transactions, identify wallet addresses, and analyze transaction flows.
4	Natural Language Processing (NLP)	Extract entities, keywords, and suspicious patterns from dark web communications.
5	Graph Analytics	Construct relationship graphs linking wallets, vendors, marketplaces, and other entities to uncover criminal networks.
6	Machine Learning	Extract entities, keywords, and suspicious patterns from dark web communications.
7	Decision Engine	Correlate outputs from analytical modules, compute risk scores, and generate alerts for suspicious transactions.
8	Visualization & Reporting	Display analytical results through dashboards, graphs, and exportable investigation reports.
9	User Management	Authenticate authorized investigators and manage user access privileges.
10	Audit & Logging	Record system activities, analytical operations, and user interactions for accountability and forensic review.

TABLE 4: Non-Functional Requirements

S/N	Module	Non-Functional Requirement
1	Performance	The framework is designed to process and analyze large volumes of blockchain and dark web data efficiently while maintaining fast response times.
2	Scalability	The framework is designed to accommodate growing volumes of transaction records and intelligence data while maintaining consistent system performance.
3	Reliability	The framework is designed to deliver reliable analytical results while ensuring continuous system availability.
4	Security	The framework is designed to protect collected data, user credentials, and intelligence outputs through secure authentication and encryption mechanisms.
5	Availability	The framework is designed to remain available and accessible to authorized users throughout investigative activities.
6	Accuracy	The analytical modules are designed to reduce false positives and false negatives while maintaining a high level of detection accuracy.
7	Maintainability	The framework is designed to support seamless updates, module replacement, and the integration of new analytical techniques.
8	Usability	The graphical user interface is designed to provide investigators and analysts with an intuitive and user-friendly environment for monitoring and analysis.
9	Interoperability	The framework is designed to integrate seamlessly with blockchain APIs, threat intelligence platforms, and external digital forensic tools.
10	Extensibility	The architecture is designed to accommodate the future integration of additional cryptocurrencies, machine learning models, and intelligence sources without requiring significant structural modifications.

Security requirements ensure the protection of transaction data, user credentials, and intelligence outputs through secure authentication and encryption mechanisms. Reliability and

availability requirements support continuous system operation and ensure that investigators can access the framework whenever required during transaction monitoring and analysis activities. The accuracy requirement enhances the effectiveness of transaction analysis by minimizing false positives and false negatives in detection processes. Additionally, maintainability and extensibility requirements allow ETTF to support system updates, integration of improved analytical techniques, additional cryptocurrencies, machine learning models, and new intelligence sources without major architectural modifications. The usability and interoperability requirements further improve investigator interaction by providing an intuitive interface and enabling seamless integration with blockchain APIs, threat intelligence platforms, and digital forensic tools. Collectively, these non-functional requirements establish ETTF as a secure, scalable, reliable, and adaptable framework for enhanced blockchain transaction tracking and intelligence analysis.

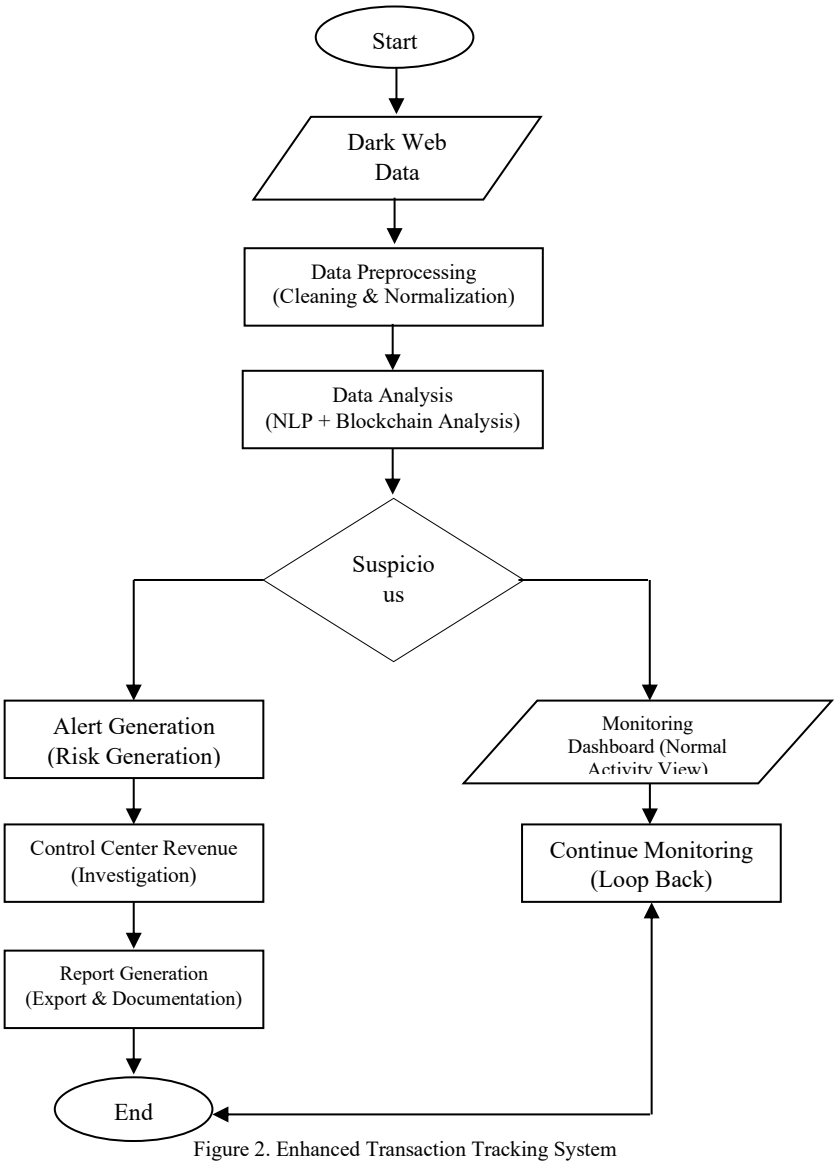

Figure 2. Enhanced Transaction Tracking System

Algorithm of the System

Algorithms are developed to enable systems to perform specific tasks or solve complex problems through a structured sequence of operations. For the Enhanced Transaction Tracking Framework (ETTF), algorithms are designed to support core processes such as blockchain transaction monitoring, transaction analysis, and the identification of potentially suspicious activities. One of the key algorithms implemented in ETTF focuses on tracking and analyzing blockchain transactions by collecting transaction records, examining transaction patterns, evaluating associated risks, and generating intelligence outputs to support investigative activities. The Transaction Tracking and Analysis Algorithm provides a systematic approach for tracing transaction flows, identifying irregular activities, and assisting analysts in making informed decisions during blockchain-based investigations.

Step 1**:** Start.

Step 2**:** Initialize the ETTF framework by configuring data sources, analysis parameters, and detection thresholds.

Step 3**:** Collect blockchain transaction data and related intelligence information from the configured sources.
Step 4**:** Preprocess the collected data by removing duplicates, correcting inconsistencies, and standardizing the data for analysis.
Step 5**:** Extract relevant transaction features and analyze them using the framework's analytical and machine learning models.
Step 6**:** Identify suspicious transactions, assign risk levels, and generate intelligence results based on the analysis.
Step 7**:** Store the analysis results in the database and display transaction insights, alerts, and reports to investigators through the user interface.
Step 8: End.

As illustrated in Figure 2, the Enhanced Transaction Tracking Framework (ETTF) processes collected Dark Web data through a sequence of preprocessing, feature extraction, and intelligent analysis before evaluating the transaction against predefined risk criteria. The decision stage of the flowchart operates as follows:

i. If the transaction satisfies the predefined suspicious activity criteria or its risk score exceeds the specified threshold, the system classifies it as Suspicious, generates an alert, and presents the results through the visualization dashboard and analytical reports.

ii. If the transaction does not satisfy the suspicious activity criteria or its risk score falls below the specified threshold, the system classifies it as Normal, stores the analysis result, and continues monitoring subsequent transactions.

This decision-making process enables the Enhanced Transaction Tracking Framework (ETTF) to distinguish between legitimate and suspicious transaction activities in a consistent and systematic manner. The iterative workflow supports continuous monitoring, timely alert generation, and the production of actionable intelligence for investigators, cybersecurity analysts, and other authorized stakeholders.

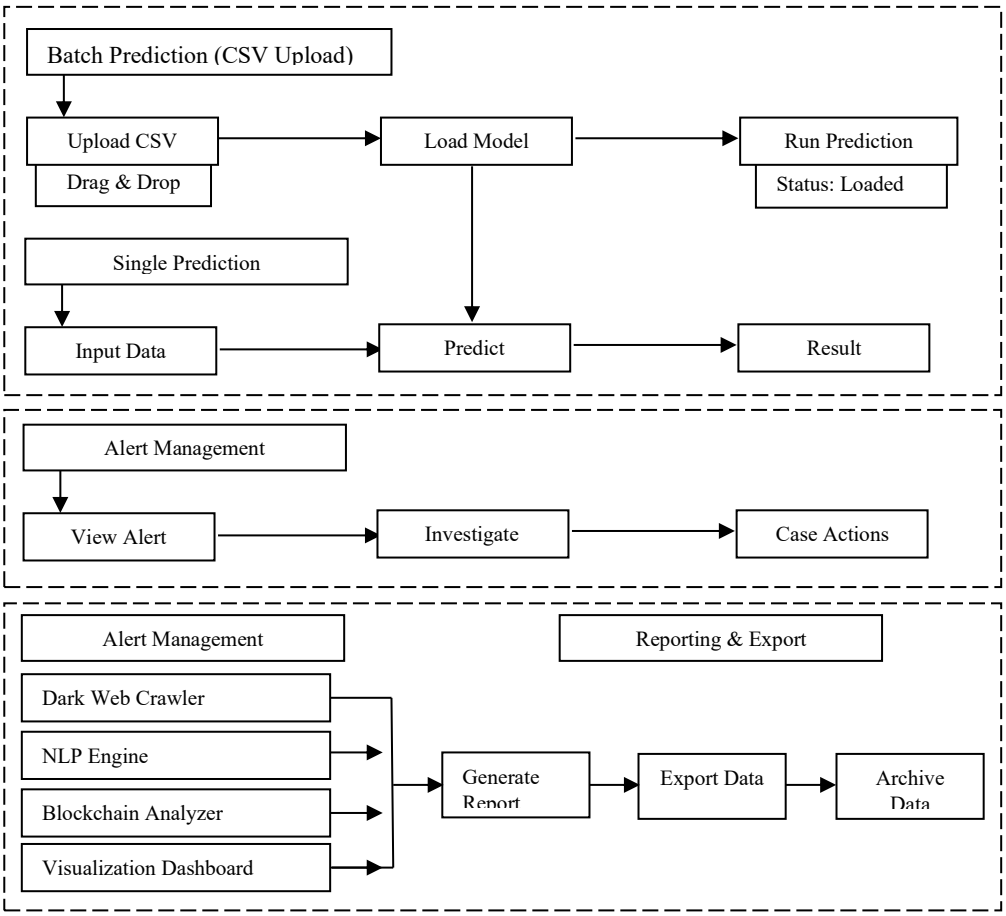

Figure 3. Control Centre / Main Menu

System Design

The operational workflow of the Enhanced Transaction Tracking Framework (ETTF) begins with the Control Centre shown in Figure 3, which serves as the central interface for coordinating data acquisition, transaction analysis, alert management, and reporting activities. Through this interface, authorized users can perform single or batch transaction analysis, monitor system operations, investigate flagged activities, and generate analytical reports. Figure 4 illustrates the Data Acquisition Subsystem, where data is collected from Dark Web marketplaces, forums, and blockchain sources before undergoing preprocessing and storage for subsequent analysis. Figure 5 presents the Analytical Subsystem, demonstrating how the Natural Language Processing (NLP) Engine, Blockchain

Analyzer, and Machine Learning Model work together to extract meaningful features, identify suspicious transaction patterns, and detect illicit activities. Figure 6 illustrates the Visualization and Reporting Subsystem, which transforms analytical outputs into interactive dashboards, network visualizations, risk alerts, and exportable reports that support investigation and decision-making. Furthermore, the system input and output formats shown in Figures 7 and 8 describe how transaction data is received from users or external sources, validated, analyzed, and transformed into structured intelligence outputs, including classification results, risk scores, visual dashboards, and analytical reports. Together, these diagrams provide a comprehensive representation of the architecture and operational workflow of the Enhanced Transaction Tracking Framework (ETTF), demonstrating how multiple intelligent modules are integrated to support the efficient detection, analysis, visualization, and reporting of illegal transactions on the Dark Web.

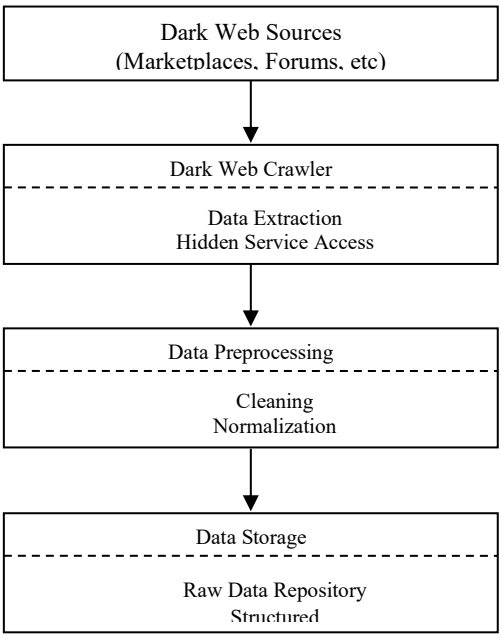

Figure 4. Data Acquisition subsystem

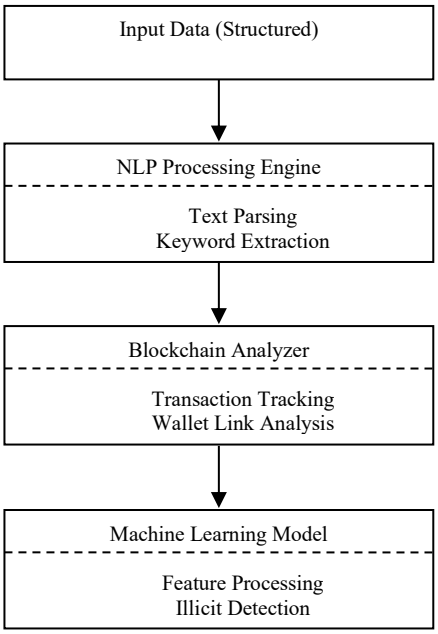

Figure 5. Analytical Submenu

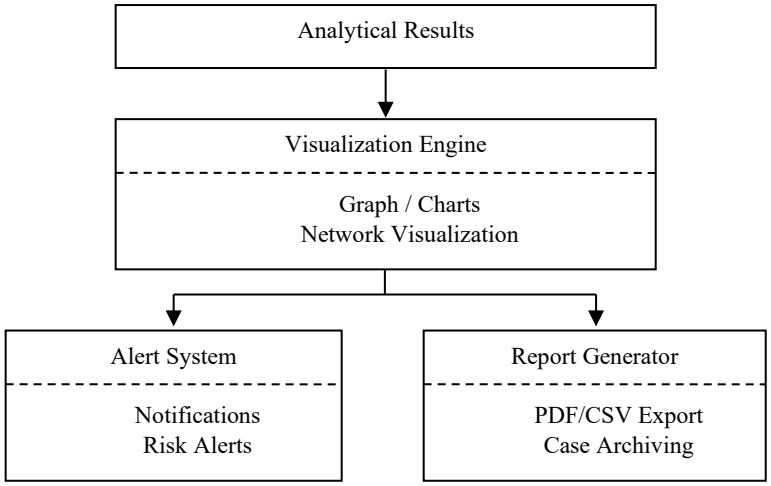

Figure 6. Visualization Dashboard

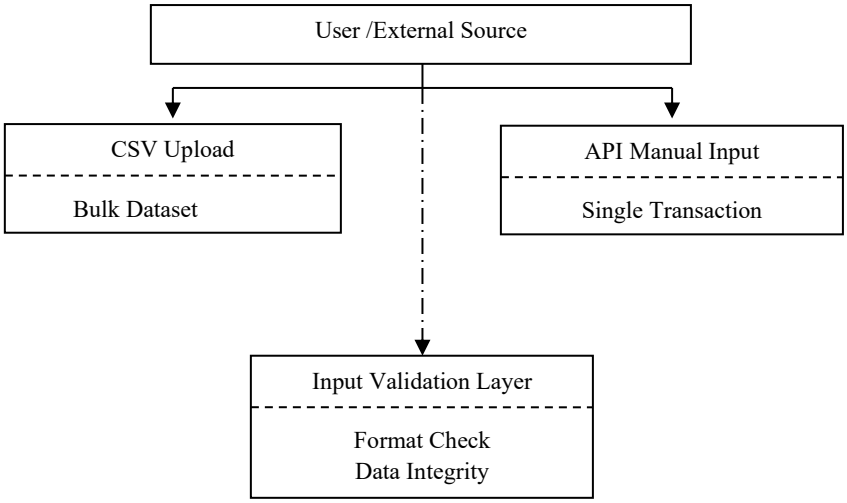

Figure 7. Input format of the new system

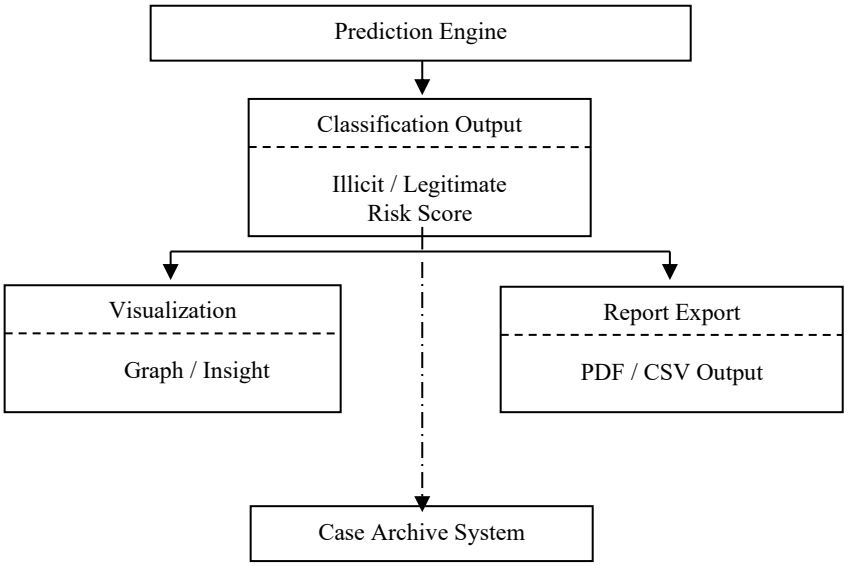

Figure 8. Output format of the new system

TABLE 5: Test Case Plan for ETTF

S/N	Test Case	Feature/Module Tested	Test Procedure	Expected Result	Observed Result	Status
1	Data Acquisition Test	Data Acquisition Module	Access selected Dark Web sources and collect transaction-related data and metadata.	The system successfully retrieves and stores transaction data from configured sources.	Transaction data and metadata were successfully collected and stored without interruption.	Pass
2	Data Preprocessing Test	Preprocessing Module	Clean, normalize, and remove duplicate or irrelevant data from the collected dataset.	The system produces a structured and standardized dataset ready for analysis.	Data was successfully cleaned, normalized, and prepared for analysis.	Pass
3	Feature Extraction and Classification Test	NLP and Machine Learning Module	Extract transaction features and classify transactions using NLP and machine learning algorithms.	The system accurately extracts relevant features and correctly classifies suspicious and normal transactions.	Transactions were correctly classified with accurate feature extraction.	Pass
4	Visualization and Reporting Test	Visualization and Reporting Module	Display analytical results through dashboards and generate exportable reports.	The system presents clear dashboards, risk indicators, and analytical reports.	Dashboards and reports were generated successfully with accurate analytical results.	Pass
5	Integration Test	Entire ETTF Workflow	Execute the complete workflow from data acquisition to report generation.	All modules communicate seamlessly without data loss or processing errors.	Data flowed successfully across all modules without errors.	Pass
6	Functional Test	Complete System	Test transaction analysis, anomaly detection, risk scoring, and report generation.	The system correctly identifies suspicious transactions, assigns risk levels, and generates reports.	The system achieved the expected functionality and produced reliable outputs.	Pass
7	Performance Test	System Performance	Process multiple transaction records simultaneously under normal operating conditions.	The framework processes transaction data efficiently while maintaining acceptable response time.	The system maintained stable performance and processed data efficiently.	Pass
8	Accuracy Test	Detection Engine	Compare classification results with predefined evaluation criteria.	The framework minimizes false positives and false negatives while maintaining high detection accuracy.	Classification results aligned with expected outcomes and achieved satisfactory accuracy.	Pass

Test Case Plan

The test case plan outlines the procedures and methodology adopted to evaluate and validate the functionality, performance, and reliability of the Enhanced Transaction Tracking Framework (ETTF). It provides a structured set of test cases, as presented in Table 5, to verify that each functional module operates according to the specified system requirements. The test plan defines the features to be tested, the corresponding test procedures, the expected outcomes, and the actual observed results. The evaluation covers the framework's core components, including data acquisition, preprocessing, blockchain transaction analysis, Natural Language Processing (NLP), machine learning-based detection, alert generation, visualization, and reporting. The successful execution of these test cases demonstrates that the Enhanced Transaction Tracking Framework (ETTF) satisfies its design objectives and effectively supports the detection, analysis, and monitoring of illegal transactions on the Dark Web.

As shown in Table 5, the Enhanced Transaction Tracking Framework (ETTF) successfully passed all eight test cases conducted during system evaluation, achieving a success rate of 100%. The test results confirm that the framework effectively performs data acquisition, preprocessing, transaction analysis, suspicious activity detection, visualization, reporting, and system integration as specified in the design requirements. These outcomes demonstrate that the implemented framework meets its functional and non-functional requirements and is capable of supporting the efficient detection, analysis, and monitoring of illegal transactions on the Dark Web.

III. Results and Discussion

The main output of this research was the implementation of the Enhanced Transaction Tracking Framework (ETTF), as shown in Figures 9 to 12. The Control Centre/Main Menu shown in Figure 9 serves as the central interface of the framework, providing authorized users with access to core functionalities such as transaction analysis, alert management, reporting, data export, and key analytical modules. This integrated interface supports efficient monitoring, analysis, and management of illegal transaction investigations.

Figure 10 presents the Data Acquisition Module, which is responsible for collecting transaction-related information from Dark Web marketplaces, discussion forums, and blockchain networks. The module performs automated crawling, extracts relevant transaction data, and stores the collected information in a structured repository for subsequent processing and analysis. This automated data collection process ensures the availability of relevant intelligence for continuous monitoring of illicit activities.

International Journal of Scientific Engineering and Science
Volume 10, Issue 8, pp. 82-92, August 2026. ISSN (Online): 2456-7361

Figure 11 illustrates the Analytical Module, which combines the Natural Language Processing (NLP) Engine, Blockchain Analyzer, and Machine Learning Model to process and analyze the collected data. The NLP Engine extracts meaningful textual features from Dark Web communications, while the Blockchain Analyzer traces cryptocurrency transactions and wallet relationships. The Machine Learning Model classifies transactions, detects anomalies, and identifies suspicious behavioral patterns, thereby improving the accuracy and efficiency of illegal transaction detection.

Figure 9. Control Center/Main Menu

Figure 10. Data Acquisition Module

Figure 11. Analytical Module

Figure 12. Visualization and Reporting Module

Finally, Figure 12 presents the Visualization and Reporting Module, which displays analytical results through interactive dashboards, risk alerts, and exportable reports. The module enables users to monitor transaction trends, review flagged activities, and support informed investigative decision-making. Together, these interfaces demonstrate the successful implementation of the Enhanced Transaction Tracking Framework (ETTF) and its capability to detect, analyze, visualize, and report illegal transactions on the Dark Web.

IV. Conclusion

This research developed the Enhanced Transaction Tracking Framework (ETTF) as an intelligent framework for detecting, analyzing, and tracking illegal transactions on the Dark Web. Existing approaches to Dark Web transaction tracking often face challenges such as fragmented data sources, limited analytical capabilities, and difficulty in identifying emerging illicit transaction patterns in real time. The Enhanced Transaction Tracking Framework addresses these limitations by integrating Dark Web data acquisition, blockchain analysis, Natural Language Processing (NLP), machine learning, and visualization into a unified platform. This integration improves the efficiency, accuracy, and reliability of detecting suspicious transactions while providing actionable intelligence to investigators and cybersecurity professionals.

Overall, the Enhanced Transaction Tracking Framework successfully demonstrates the feasibility of combining blockchain forensics, artificial intelligence, and threat intelligence techniques to support illegal transaction investigations. The framework provides a scalable, secure, and effective solution for monitoring, analyzing, and reporting suspicious activities on the Dark Web, thereby contributing to improved cybercrime investigations, digital forensics, and intelligence-driven decision-making.

References

[1]. Akcora, C. G., Li, Y., Gel, Y. R., &Kantarcioglu, M. (2020). *BitcoinHeist: Topological data analysis for ransomware detection on the Bitcoin blockchain*. *Proceedings of the Twenty-NNinth International Joint Conference on Artificial Intelligence (IJCAI-20)*, 4439–4445. https://doi.org/10.24963/ijcai.2020/612

[2]. Chainalysis. (2025). *The 2025 Crypto Crime Report*. Chainalysis. https://www.chainalysis.com/crypto-crime-report/

[3]. Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. *Proceedings of the 22nd International Conference on World Wide Web*, 213–224. https://doi.org/10.1145/2488388.2488408

[4]. Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. Publications Office of the European Union. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

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

[6]. Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *2013 APWG eCrime Researchers Summit*, 1–14. https://doi.org/10.1109/eCRS.2013.6805780

[7]. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

[8]. United Nations Office on Drugs and Crime. (2023). *World Drug Report 2023*. United Nations. https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2023.html