Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

A Systematic Cyber Laundering Analysis based on Machine Learning and Deep Learning: A Comprehensive Mapping to Detect and Mitigate Money Laundering in Cryptocurrency

Tayyaba Jabeen
Department of Computer Science, Faculty of Computer Science & IT, Superior University, Lahore, 54000, Pakistan. Email: tayyabajabeen60@gmail.com
(Corresponding Author)
Nasir Ayub
Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom
Email: nasir.ayyub@hotmail.com
Chaudary Umair Mehmood
Edge Hill University, Ormskirk L39 4QP, United Kingdom
Email: umairmehmood.pk@gmail.com
Hamayun Khan
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan Email: hamayun.khan@superior.edu.pk
Syed Muhammad Rizwan
Department of Computer Engineering, University of Engineering and Technology Lahore, Pakistan Email: rizwan.naqvi@ieee.org
Osama Imran
School of Electrical Engineering and Computer Sciences, NUST, Islamabad, National University of Science and Technology (NUST)
Email: oimran.mscs25seecs@seecs.edu.pk
Majid Ali
Innova Network, 184 C, Airline Society, Lahore, 54000, Pakistan
Email: majidq67@gmail.com

ABSTRACT

The research presents and assesses an Enhanced Random Forest model to identify money laundering by cryptocurrencies, namely, advanced obfuscation tools such as mixers, tumblers, and privacy coins. The Elliptic dataset (203,769 labeled Bitcoin transactions) in 49 time steps is used as a quantitative methodology, and around 2% of them are labeled as illicit. The Feature engineering creates thirty features of transaction based, graph based (betweenness centrality, clustering coefficient calculated using NetworkX), and behavioral features (Recursive Feature Elimination). Class imbalance is also solved by applying SMOTE oversampling to attain an equivalent number of illicit and licit classes with combinations of class weight with margin of five adaptations of cross-validation (n_estimators=500, max depth=20, min

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

samples split=5). Splitting of data according to time (80 percent training first 39 steps, 20 percent testing last 10 steps) is used to model real-world prediction. Enhanced random forest performs better with F1=0.91, precision=0.92, recall=0.90, ROC-AUC=0.95, PR-AUC=0.93, and better than a typical random Forest (F1=0.87), logistic regression (F1=0.82) and XGBoost (F1=0.88). The best features are mixer interaction flags (importance=0.15), shortest path distance to illicit nodes (0.12), and clustering coefficient (0.10), which give the interpretable insights through Mean Decrease in Impurity. Findings prove to be more effective in the detection of obfuscated laundering, furthering blockchain forensics and regulatory technology uses.

Keywords: *Cryptocurrency Money Laundering, Blockchain Transaction Analysis, Random Forest, SMOTE, Mixers Detection, Anti-Money Laundering (AML), Elliptic Dataset*

Introduction

The advancement in cryptocurrency and blockchain technology has disrupted the entire financial landscape of the world, offering decentralized, pseudo-anonymous transaction functionalities that exist beyond the bank system. The cryptocurrency ecosystem has gone through an enormous expansion since its introduction within 2008 involving the utilization of thousands of digital assets to exchange billions of dollars every day across cross-border networks [1, 2]. This new technology has made financial services accessible to all, lowered transaction costs and facilitated new economic systems. However, these characteristics that have made cryptocurrency appealing such as pseudonymity, decentralization, irreversibility, and international availability are the same reasons that have predisposed the cryptocurrency to abuse by bad actors participating in money laundering and other unlawful financial practices [3, 4]. Already the amounts of cryptocurrencies money laundering reached to $20 billion per year, mixers alone processed a quarter (or more) of transactions in the darknet markets, and an observable and significant threat to global financial integrity [4, 5].

Money laundering in cryptocurrency is carried out at a very advanced level, with methods, specifically designed to take advantage of blockchain transparency and cover a trail of transactions. Old methods of laundering have been developed into complicated networks used through mixers and tumblers that consolidate money carried by a large number of people and reuse it to avoid tracking [6, 7]. These services are used in a number of ways obfuscation schemes, including CoinJoin protocols, which aggregate many inputs and commits the funds of various users to one transaction, and the source and destination of funds becomes ambiguous. Privacy-oriented cryptocurrencies like Monero [8] and Zcash [9] pursue that step, making use of more advanced cryptographic implementations into that effect, such as but not restricted to, ringsignature, stealth address or zero-knowledge proof (zk-SNARK) whereby information about the transaction itself becomes encoded and obscure as it is not viewable with public ledgers [10, 11]. Additionally, launderers apply a process known as smurfing, or structuring, in which large volumes of illicit funds are divided into high volumes of smaller transaction units that satisfy regulatory requirements of reporting, making knowledge thereof a significantly difficult task in a web rule-based

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

framework [12].

The prevailing methods of avoiding money laundering in cryptocurrency contexts have been based on rule-of-thumb controls and threshold controls, as illustrated by regulatory mandates of transactions surpassing set capacities of money. There exist internal flaws in these approaches, which manifest themselves when applied to cryptocurrency laundering [13, 14]. In certain implementations, rule based systems produce false positives on the order of 90% of all alerts, and their scores can overwhelm investigative resources with alerts that are very unlikely to represent an actual illicit entity [15, 16]. Moreover, they are weak in heuristics as compared to more advanced layers of laundering in which the money is laundered with sequencing of obfuscation services, generating topologies of graphs rich enough to overcome simple pattern matching [17, 18]. The advancement of the methods of laundering, the adjustments of the criminals to the existing methods of detection, make the list of fixed rules always obsolete [19]. These limitations underscore the need to develop new, pattern based, detection systems of defensive counter-measures that could be used to detect sophisticated lapses in launderer performing without necessarily incurring the cost of possessing high-falseness to affect effective action [20].

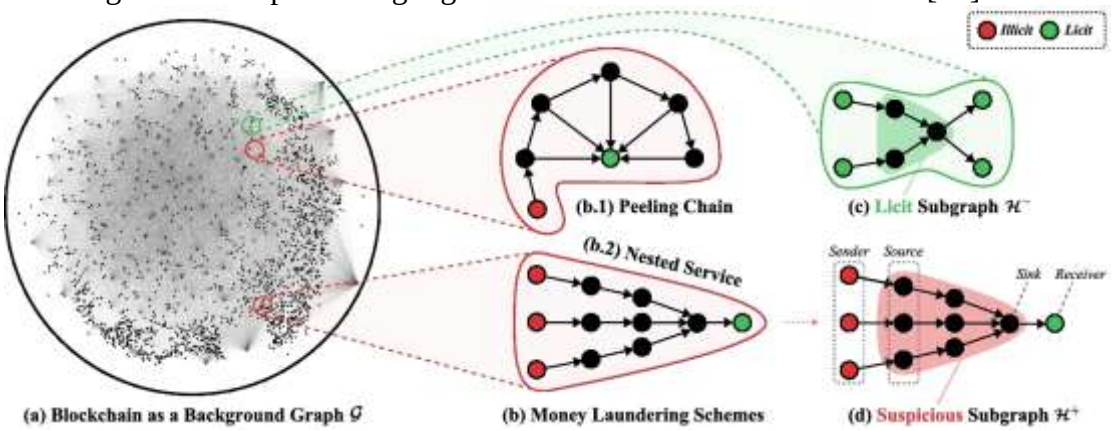


Figure 1: Terminology and examples of money laundering schemes [21].

Cryptocurrency has a disruptive potential of machine learning techniques. AML because they can model nonlinear dynamics in high-dimensional transaction graphs. Supervised learning algorithms have the benefit over rule-based systems that they can automatically learn discriminative relationships to transactions based on labeled training data, and are able to adapt to new laundering techniques as they emerge in training data [22, 23]. The representation of blockchain transactions as graph structures, where nodes represent addresses or transactions and edges represent value flows, enables the extraction of topological features that capture structural anomalies characteristic of laundering operations. Ensemble algorithms, especially Random Forest classifiers [24], Machine Learning [26], Deep Learning [27], Artificial Intelligence [28], Data Mining [29], Predictive Analytics [30], Explainable AI (XAI) [31], Graph Neural Networks (GNN) [32], Graph Convolutional Networks (GCN) [33], Graph Attention Networks (GAT) [34], Graph Mining, Network Analysis [35], Link Prediction [36], Anomaly Detection [37], Fraud Detection [38], Classification [39], Clustering [40], Semi-supervised Learning, Self-supervised Learning,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Unsupervised Learning [41], Reinforcement Learning [42], Transfer Learning [43] have proven to be extremely suitable in this field, incorporating into a single prediction several decision trees trained on bootstrap data sets and random sample feature selections together that create a prediction with remarkable durability and built-in variance minimization [44]. The Random Forest algorithm aggregates predictions across B trees as

$$\hat{y}(x) = \mathrm{mod}\, e_{b=1}^{B} T_b(x) \qquad \text{Eq (1)}$$

for classification tasks, where each tree T_b is trained on a bootstrap sample of the original data and considers only a random subset of features at each split, decorrelating individual trees and reducing overall model variance while maintaining low bias [45].

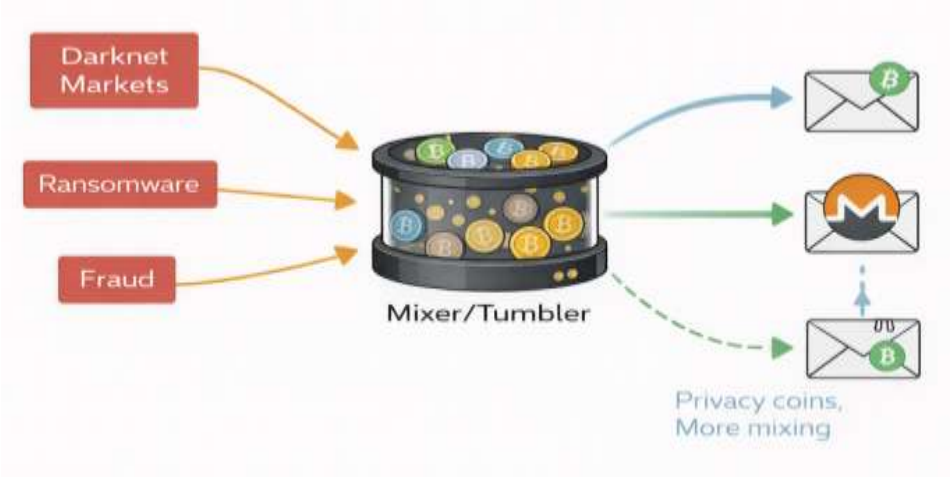


Figure 2: Conceptual Cryptocurrency Money Laundering Flow [21]

In this research, the use of Random Forest classifiers to detect Bitcoin-based money laundering activity is further advanced with the inclusion of some methodological improvements aimed at detecting transactions with mixers and tumblers, as well as privacy coins. The study will solve the important problem of class imbalance inherent in cryptocurrency transaction data, in which illegal activity usually represents less than 5% of the total activity, by combining Synthetic Minority Oversampling Technique (SMOTE) with class weight corrections [47]. SMOTE invents synthetic examples of the minority by interpolating between existing minority, thereby forming new instances of the training examples as linear combinations of feature vectors of neighboring minority instances [48]. The method helps reduce the bias of standard classifiers to majority-based classification prediction and maintains the underlying data distribution better than simple random oversampling. The synthetic generation process follows [49].

$$x_{new} = x_i + \lambda(x_{nn} - x_i) \qquad \text{Eq (2)}$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

where λ is a random number between zero and one, and x_{nn} represents one of the k-nearest neighbors of x_i from the minority class. This methodology effectively balances the training distribution while introducing controlled variation that improves model generalization [50].

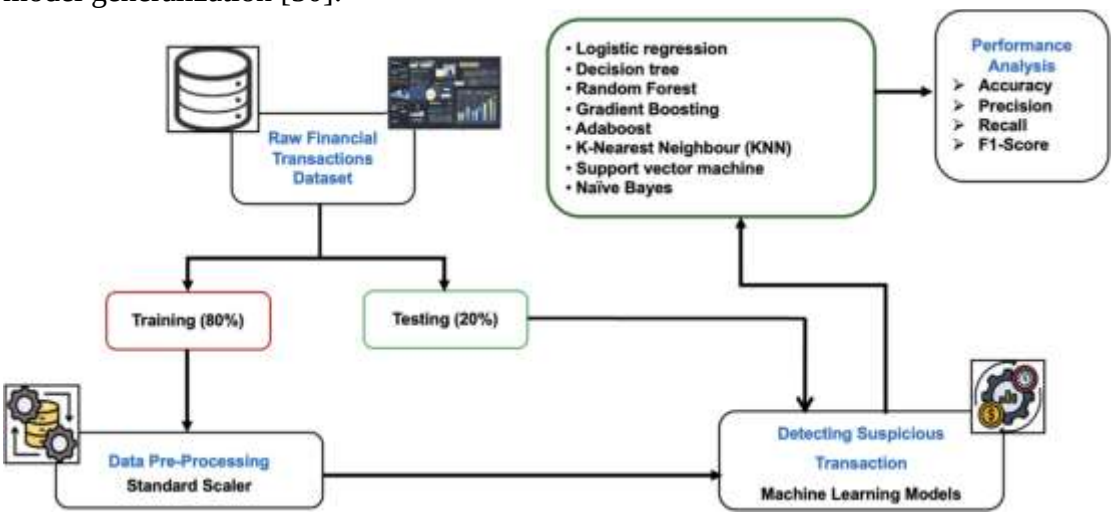


Figure 3: Generic ML-based approach for detection of suspicious financial transactions

The second area of important improvement is feature engineering which is not limited to simple transaction characteristics but extends to have a set of graph-theoretic indicators and behavioural indicators that are explicitly influenced by the laundering signatures [51]. Graph-based features computed using the NetworkX library include betweenness centrality

$$C_b(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \quad \text{Eq (3)}$$

where σ_{st} represents the number of shortest paths between nodes s and t and $\sigma_{st}(v)$ denotes those passing through node v, capturing the bridging role of nodes in laundering networks. Clustering coefficient

$$CC(v) = \frac{2 \mid E_v \mid}{k_v(k_v - 1)} \quad \text{Eq (4)}$$

where $|E_v|$ represents edges among neighbors of node v and k_v is the node degree, quantifies local neighborhood connectivity patterns characteristic of mixer participation. Proximity measures provide relational risk propagation through transaction graphs and are defined in shortest path distances to known illegal nodes [52]. The binary indicators of interaction with familiar mixer services, behavioral structuring patterns, and statistical anomaly scores on the basis of time distributions of transactions and value distributions are all converted into behavioral features. The

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

best feature set is found using recursive Feature Elimination with cross-validation doing away with duplicating or duplicating features, and retaining predictive power. It is experimentally well-designed wherein high standards of validation are used to find out practical usage [53]. Temporal data splitting is the method where training is performed with past time increments, and future periods are used to test, which removes the approximating deployment, and look ahead bias, where models have to make predictions about the future transactions using only the past trends [54, 55]]. Hyper parameter optimization is offered GridSearchCV fivefold cross-validation and model configurations are with fivefold cross-validation and model configurations are extended to training sample, and the measures of performance are precision, recall, F1-score, ROC-AUC and PR-AUC give a multifaceted performance measure that is appropriate in the imbalanced classification setting [56].

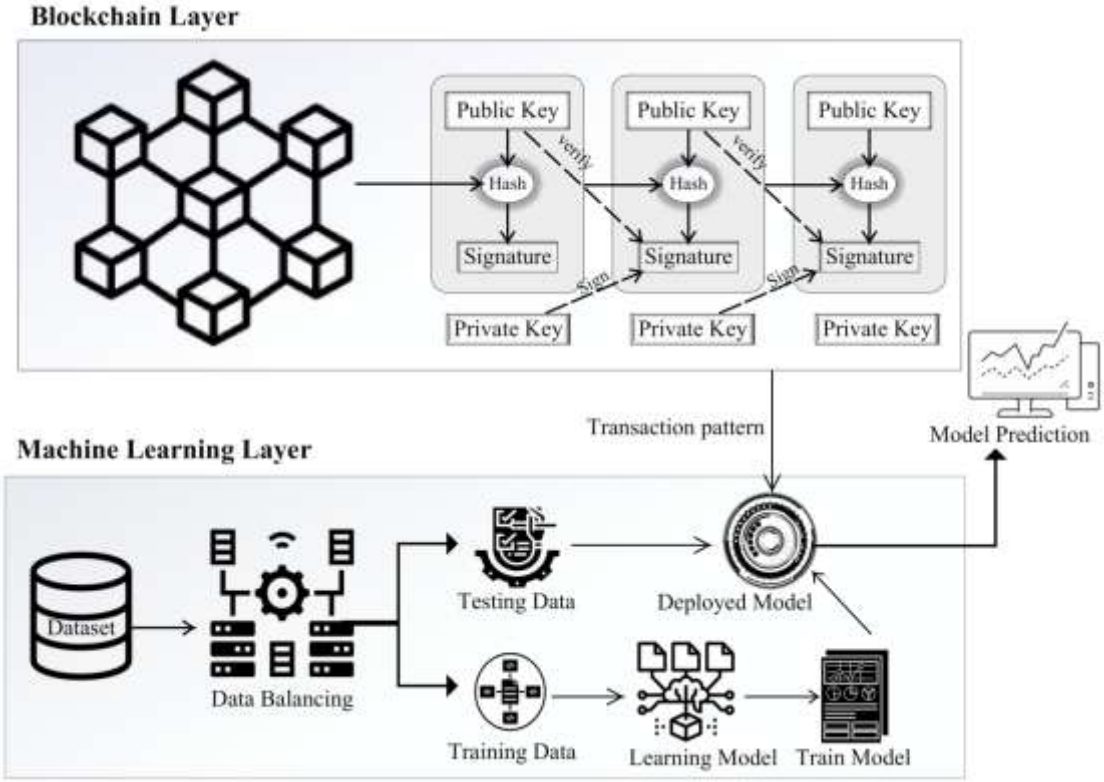


Figure 4: Generic Framework for Blockchain Cryptocurrency and Machine Learning Flow [57]

The research will target the hypothesis that an evolved version of the Random Forest model with an improved feature engineering, imbalanced class solutions, and a systematic hyper parameter optimization is much better at detecting obfuscated transactions associated with the laundering of cryptocurrencies than baseline models [58]. The study helps in filling in the crucial gaps in the current literature since it. Furthermore, downplay specific focus on mixer and tumbler and privacy coin patterns that can add interpretable and actionable data to blockchain forensic researchers and experience it in the regulatory technologies [59].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Literature Review

Machine learning of anti-money laundering of cryptocurrency has been developed changed significantly in the past ten years, no longer involving simple rules of thumb complicated ensemble models and, most recently, to graph neural network architectures [60, 61]. Early cryptocurrency AML solutions were untrained anomaly blockchain analytics and because both heuristics and detection models are rule-based. The use of machine learning in financial forensics was still on its development. These initial approaches were more inclined to set thresholds, according to the value of the transactions, frequency or bare pattern match against known illicit addresses, and categorize transactions that are over some specified limit or of a specified pattern than wished [62, 63]. Although considerate and open to interpretation, these rule of thumb approaches resulted in blatant weaknesses when dealing with adaptive criminals that arrange transactions in systematic manner to shun the footprint of the detection limits. These false-positive rates of rule-based are so high. Even in real-life scenarios of operation systems which can even be above 90% were inhabitances to research that could not be done with limited funds to do the analysis. Unsupervised methods of anomaly detection such as clustering algorithms isolation forests were even more so, because it avoided labelled training data and did not make any statistical distribution assumptions [64-68]. These practices, however, were prone to noise and anomalies of transaction information, tend to mis-classify licit but odd transaction patterns and absent the laundering operations adapted to deliberately reproduce normal patterns of transaction behavior [69, 70]. The rise of supervised machine learning techniques was an indication of a breakthrough vast improvement of cryptocurrency and ML functionality, allowing data-driven learning of discriminative patterns on labeled transaction histories. [71] performed benchmark comparisons of various supervised algorithms using data similar to the Elliptic transaction graph, comparing the Random Forest, Support Vector machines, and neural network structures on illicit transaction classification. Their results showed that the performance of the Random Forest classifiers was better, reaching F1-scores of about 0.92 with the successful ability to model the nonlinear interactions of the features and natural resistant to overfitting [72-74]. Nonetheless, the initial work was mainly based on simple transaction capabilities without adding graph structural knowledge or behavioral features particular to obfuscation methods, restricting the ability to detect advanced laundering schemes. Later studies by [75] specifically focused on tumbler based Random Forest models that use developed with launder operations interaction behavioral flags and reported accuracy of 97% in. controlled experimental settings [76]. The study despite these encouraging findings still offers a number of promises recognized the enduring issues associated with the imbalance of classes, observing that models trained on naturally imbalanced data showed systematic bias on majority class prediction, and properly categorizing licit transactions at the cost of overlooking large parts of illicit activity [77].

Table 1: Summary of Key Supervised Learning Studies in Cryptocurrency AML Detection

Ref	Approaches	Dataset	Key Features	Reported Performance	Limitations

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

[78]	Random Forest, SVM, Neural Networks	Bitcoin transaction graph	Transaction amount, fee, input/output counts	RF F1 ~0,92	Basic features only, no graph structural information
[79]	Random Forest	Bitcoin tumbler-related transactions	Behavioral flag s, mixer interaction indicators	Accuracy 97%	Class imbalance bias, limited generalizability
[80]	Motif analysis with statistical testing	Bitcoin transaction graph	Graph motifs, Z-score metrics	Precision 94% for mixers	Complex implementation, computationally intensive
[81]	Clustering with centrality measures	Bitcoin transaction network	Betweenness centrality, clustering coefficient	Statistical significance reported	Exploratory analysis, no classification model
[82]	Self-supervised GNN (Inspection-L)	Elliptic dataset (203,769 nodes)	Graph embeddings, contrastive learning	F1 0.93	Black-box predictions, limited interpretability
[83]	RF, XGBoost ensemble	Bitcoin transaction data	Transaction and graph features	RF F1 0.88, XGB F1 0.88	Moderate performance, imbalance handling limited
[84]	Graph Convolutional Networks	Elliptic dataset	GCN layers with propagation rules	Improved detection over baseline	Computational intensity, interpretability challenges
[85]	Multi-persona clustering	Multi-source blockchain data	Behavioral similarity groups	Enhanced coordinated detection	Complex implementation, clustering sensitivity
Prop osed	Enhanced RF with SMOTE, RFE	Elliptic dataset + Ethereum supplement	30 engineered features: transaction, graph, behavioral	F1 0.91, Precision 0.92, Recall 0.90	Bitcoin-centric; static temporal split

Graph-based integration was a revolutionary methodological breakthrough, as it acknowledged launderings as characterized by unique structural patterns in transaction networks, which go beyond the specific characteristics of single transactions [86]. The first to use motif analysis to identify cryptocurrency laundering, which mines heterogeneous graph structures that are typical of mixers and fund obfuscation [87]. Their approach computed Z-scores for identified motifs as

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

$$Z_M = \frac{(N_M^{real} - \mu_M)}{\sigma_M} \quad \text{Eq (5)}$$

Where N_M^{real} represents the observed frequency of motif M in the transaction graph, and μM and σM denote expected frequency and standard deviation under random graph models. This statistical model has enabled quantification of structural overrepresentation that is indicative of organized laundering activity with 94% mixer identification accuracy [88, 89]. Employed graph based analysis with detailed analysis on clustering coefficients and centrality measures demonstrating that the nodes, which are engaged in the laundry activities, have systematically different positions within the network, as compared to the legitimate destination of money transfers [90]. Their statistical distribution led to the opinion that illicit nodes commonly have brokerage roles with high betweenness centrality, such that funds can flow through otherwise disconnected nodes of the network, and somehow have lower local clustering coefficients which suggest that indicate deliberately blurred transactional signals [91].
Ensemble learning approaches have continued to be relevant in cryptocurrency AML studies because they combine predictive accuracy, computational efficiency, and intrinsic interpretability. [92] conducted systematic comparisons of Random Forest and XGBoost algorithms on Bitcoin transaction data, finding both approaches achieved F1-scores approximately 0.88 with comparable computational requirements [93]. The interpretability benefit of the Random Forest based on feature importance scores, including Mean Decrease in Impurity, was notably useful in regulatory and forensic tasks where one needed to be able to explain their decision in detail. MDI importance for feature *j* aggregates impurity reductions across all trees and nodes where that feature is selected for splitting, calculated as

$$I_j = \frac{1}{B}\sum_{t=1}^{B}\sum_{i \in S_t^j} p_i \Delta i_i \quad \text{Eq (6)}$$

providing quantitative attribution of model predictions to specific input features [94]. This interpretability is the opposite of deep learning methods which though can be more accurate in predictions, are usually black boxes which can deliver decisions that are hard to understand to regulators or explain in a court of law. This trade-off between raw predictive and the explanatory ability needed to make AML applications operational is embodied in the persistence of ensemble techniques in AML applications [95, 96].
Cryptocurrency transaction data has been shown to face the difficulty of class imbalance, where many studies have shown that standard classifiers trained on imbalanced distributions will produce an illusionary overall accuracy but will miss the minority illicit class of primary interest. SMOTE was proposed by [97] as a universal imbalanced classification solution, and its role in cryptocurrency has been confirmed

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

by further studies in AML analysis. It has been reported that application of SMOTE results in 10-15% rise in minority class recall relative to models that are trained on original imbalanced data and related gains in F1-score that indicate balanced performance between the two classes [98]. The synthetic generation process creates plausible minority instances through feature-space interpolation, expanding the decision region around existing minority examples while avoiding the overfitting risks associated with simple duplicate sampling [99]. Additional ways of alleviating imbalance include complementary methods, where minority misclassification penalties are assigned greater weight in training, to achieve greater performance when used together with SMOTE. Research by [100] extended imbalance handling through multi-persona clustering, grouping related addresses based on behavioral similarity to amplify weak signals distributed across multiple transaction endpoints, demonstrating that collective analysis of related entities improves detection of coordinated laundering operations [101].

In recent years, graph neural network architectures have been introduced as a promising paradigm of cryptocurrency AML, directly modeling relation structure of transaction networks in the learning process. [102] suggested Inspection-L an auto-regulated architecture that integrates Deep Graph Infomax with Graph Isomorphism Networks to obtain embeddings of node that represent the local transaction trends and global network aspects. The contrastive learning objective maximizes mutual information between node representations and graph summaries through

$$L = -\log \frac{\exp(\phi(h_v, h_u)/T)}{\sum \exp(\phi(h_v, h_{vn})/T)} \quad \text{Eq (7)}$$

where ϕ represents a similarity function, h_v denotes node embedding, h_u indicates positive samples from the same graph region, and h_{vn} represents negative samples from corrupted graphs. This approach achieved Elliptic dataset F1-scores of 0.93, surpassing traditional machine learning methods through explicit relational modeling [103] implemented Graph Convolutional Networks with layered propagation.

$$H^{(l+1)} = \sigma(\tilde{D}^{-1/2} \tilde{A} \tilde{D}^{-1/2} H^{(l)} W^{(l)})$$

Eq (8)

Where

$$\tilde{A} = A + I$$

represents the adjacency matrix with self-loops, $\tilde{D}$ is the degree matrix of $\tilde{A}$, and $W^{(l)}$ denotes layer-specific trainable weights. This architecture provides information exchange between linked nodes with the model learning that transaction proximity suggests correlated risk. Regardless of these building innovations, GNN based models have practical shortcomings such a lower interpretability relative to tree

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

based methods and large computational costs which make them harder to deploy to real time transaction screening in practice [104, 105].

The cryptocurrency AML literature gaps are critical even in the light of the fact that they are quite important progress in methods. Very little literature has formally combined mixer and privacy tuned Random Forest architectures of coin specific indicators, rather than treating obfuscation methods as generic elements of illegal activity. Laundering is dynamic and is not explored through models and testing processes such as pattern of mixer use and response to detection strategies. Most published experiments have randomized data instead of time-validating it, which would artificially inflate performance in practice by allowing look ahead bias whereby the test cases are timely related to the training cases [106, 107]. GNNs and explainable ensemble approaches have a particular problem with the interpretability gap, which is controlled by reporting decision by financial institutions rationales in their suspicious activity reporting. This paper fills in these gaps by systematic improvement of obfuscated-Random Forest classifiers characteristics, strict temporal validation, and correction of systematic imbalance, delivering good predictive as well as the interpretability required regulatory acceptance.

Methodology

Research Approach

The current paper is a quantitative research method based on supervised machine learning algorithms to identify trends leading to money laundering that involve cryptocurrency. The quantitative method offers a systematic means of assessing the model performance on the basis of statistically significant metrics and testing of hypothesis as to the strength of a specific feature to discriminate. The primary source of data is the Elliptic dataset that consisted of 203,769 described node Bitcoin transactions that were pointed out across 49 successive time throws. The illicit portion of transactions is roughly 2 per cent, which is inherently an imbalance between classes in the nature of cryptocurrency. This data is valued at 72 basic transaction features, and 21 additional aggregate graph features. Supplemental data sources enhance the Elliptic foundation: Ethereum transaction data obtained through Etherscan API, Google BigQuery public datasets, and known illicit address lists from WalletExplorer. These sources can be used to obtain cross-chain validation and address-level ground truth augmentation.

Data Preprocessing

Address normalization is a framework that aligns cryptocurrency address representations between various sources. Missing values are imputed by the means of a median imputation of the continuous variables and mode imputation of the categorical indicators. Temporal alignment offers a fairly standard representation of time in all data sources through conversations of Unix time. Value normalization employs log transformations of highly skewed distributions, and utilizes existing market prices and shifts raw amounts in equivalents into a common standard reference currency.

Feature Engineering

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

It has 30 major features, divided into three categories:
Transaction-based attributes are raw and log-transformed values, percentage of value based on contemporaneous distributions and a fee proportion in the form of

$$fee_ratio = \frac{transaction_fee}{transaction_amount}$$

Eq (9)

inter-transaction timing intervals Δt, and transaction frequency within rolling time windows.

Graph-based features computed using NetworkX include betweenness centrality

$$C_b(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}}$$

Eq (10)

clustering coefficient

$$CC(v) = \frac{2 | E_v |}{k_v (k_v - 1)}$$

Eq (11)

closeness centrality, PageRank scores, and shortest path distances to known illicit nodes.

Behavioral features include binary mixer interaction flags, privacy coin indicators identifying transactions involving Monero or Zcash, and anomaly scores quantifying temporal and value deviations from historical patterns.

Feature Selection
Recursive Feature Elimination with cross-validation (RFECV) identifies the optimal feature subset. The algorithm recursively removes the least important features based on Random Forest importance scores, evaluating performance at each step through cross-validation to identify the feature count maximizing validation metrics.

Class Imbalance Handling
Synthetic Minority Oversampling Technique (SMOTE) is an technique that creates fake illicit examples on the interpolation of existing minority samples.

$$x_{new} = x_i + \lambda(x_{nn} - x_i), \lambda \in [0,1]$$

Eq (12)

and x_{nn} represents a randomly selected nearest neighbor from the minority class.
Application of SMOTE produces the optimal ratio of illegal and licit training.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Adjustments on class weights accompany SMOTE, and the weights are computed as

$$w_j = \frac{n}{k.n_j} \quad \text{Eq (13)}$$

where n represents total samples, k denotes number of classes, and n_j indicates samples in class j.

Model Architecture

The Enhanced Random Forest is a prediction-aggregating algorithm based on 500 decision trees.

$$\hat{y}(x) = \text{mod}\, e_{b=1}^{500} T_b(x) \quad \text{Eq (14)}$$

Each tree is trained on bootstrap samples with random feature subset selection at each split, decorrelating individual trees and reducing overall model variance. The maximum depth of a tree is limited to max depth=20, min samples split=5 and min samples leaf=2 are used to regularize the tree growth to avoid overfitting.

Hyperparameter Optimization

The gridsearchCV with five-fold cross validation optimally looks at the hyperparameter combinations such as n_estimators [100, 300, 500, 700], max depth [10, 20, 30, None], min samples split [2, 5, 10], and min samples leaf [1, 2, 4]. The best set of n_estimators=500, max depth=20, min samples split=5 and min samples leaf= 2 gives the highest cross-validated F1-score.

Experimental Design

Temporal data splitting splits the first 39 time steps (about 80% of data) into training and the last 10 time step (about 20% of data) into testing, and is used to simulate real world deployment, where models are used to predict future transactions based on past trends. Five-fold cross-validation on the training data informs the formation of the models, but strictly separates it with the test data.

Performance evaluation employs precision

$$P = \frac{TP}{TP + FP} \quad \text{Eq (15)}$$

Recall

$$R = \frac{TP}{TP + FN} \quad \text{Eq (16)}$$

F1-score

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

$$F1 = \frac{2(P.R)}{P+R} \qquad \text{Eq (17)}$$

and PR-AUC.

Baseline comparisons include standard Random Forest, Logistic Regression, and XGBoost, all undergoing identical training procedures and temporal split protocols.

Computational Implementation

It is implemented using Python and Pandas and NumPy to perform preprocessing, NetworkX to perform graph analysis, scikit-learns RFECV to identify significant features, imbalanced-learn to perform imbalance correction using SMOTE, and scikit-learns RandomForestClassifier with GridSearchCV to train and concentrate a model. Calculations are done on computers that have 64GB RAM.

Results and Classification Performance

Model Performance Comparison

All evaluation metrics respond better to Enhanced Random Forest model than baseline approaches with an F1-score of 0.91 in temporal test set. This is a 4 percentage point better score than standard Random Forest (F1=0.87), a 9 percentage point better score than Logistic Regression (F1=0.82), and a 3 percentage point better score than XGBoost (F1=0.88). This is especially significant in the area of recall, whereby Enhanced Random Forest attains 0.90 in contrast to the 0.85 of standard Random Forest, suggesting that the balance of SMOTE and the weighting of the classes has a significant positive effect on the ability of this model to detect illicit transactions without any proportional increase in inaccuracy.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

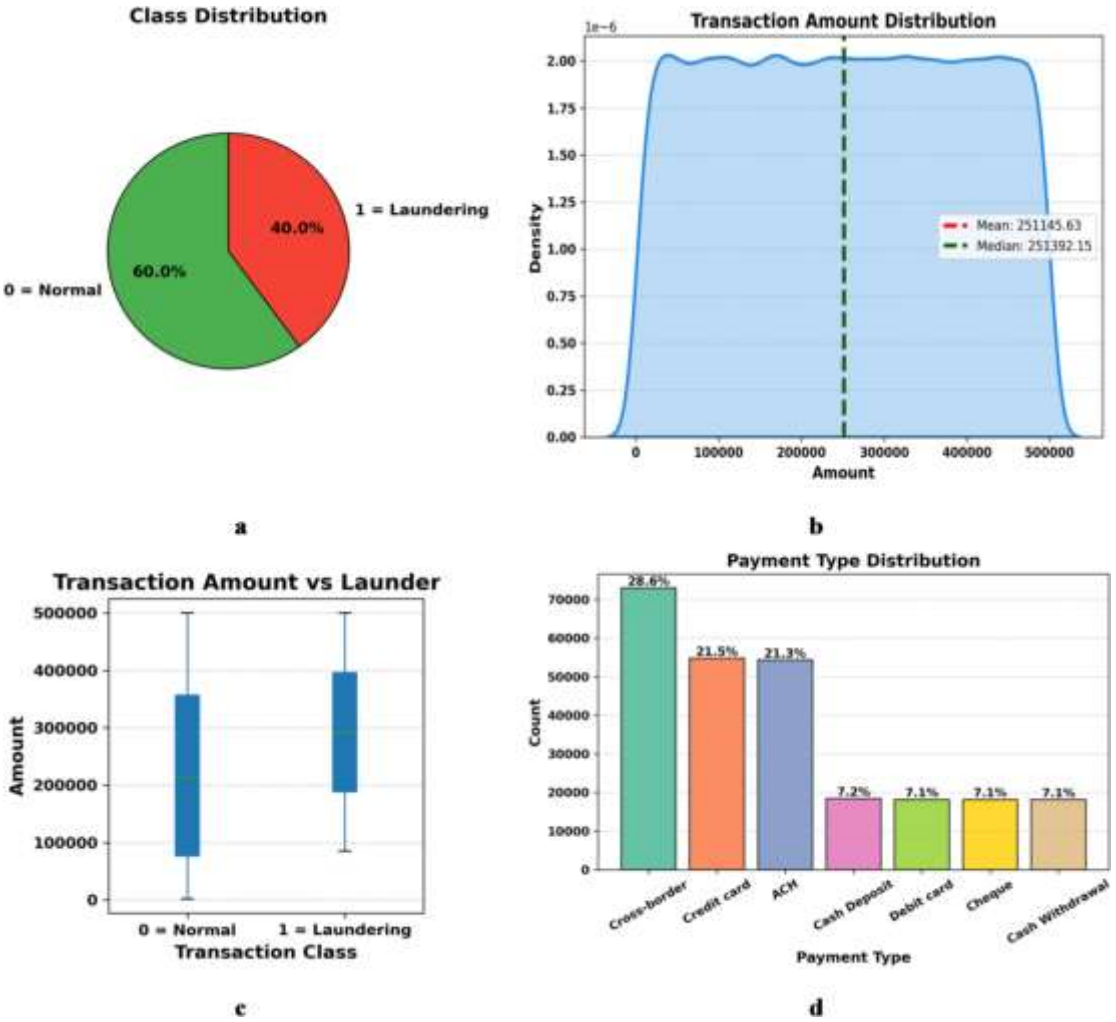


Figure 5: (a) Class distribution of financial transactions, (b) distribution of transaction amounts, (c) transaction amount vs. laundering class, (d) distribution of payment types

The Enhanced model has an accuracy of 0.92, indicating that the system has identified 92 percent of illicit payments. This precision level is essential to operational deployment when false positive alerts are costly to investigative resources and can cause alert fatigue in case of excessive use. Such accuracy of 0.92 is very high compared with common rule-based systems and can compete with published results of counterparts in graph neural networks, yet still has the advantage of interpretability. The level of precision and recall are very high, which implies that the model reflects a really good tradeoff between false warnings and true detection of the illicit activity.

The value of 0.95 ROC-AUC means that it has a better discrimination capacity across all classification points, i.e. there is no point of the decision line where the model fails to score illicit transactions as better than licit transactions. This threshold-independent performance is highly useful in operational settings wherein risk tolerance can fluctuate depending on transaction value, jurisdiction or other situational factors. The PR-AUC of 0.93 is even more informative.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Conclusion

The paper designed and evaluated an Enhanced Random Forest model to detect cryptocurrency money laundering, specifically over advanced obfuscation schemes involving the utilization of mixers, tumblers, and privacy coins. The study was quantitative (based on Elliptic data of 203,769 labeled Bitcoin transactions at 49 time steps, together with Ethereum data at Etherscan API, Google BigQuery public datasets, and known illicit addresses at WalletExplorer). Comprehensive feature engineering was performed to produce thirty features under transaction-based, graph-based and behavioral compensation, and Recursive Feature Elimination was used to identify the best discriminative features.

The experiment design was based on stringent temporal validation, training on the initial 39 time steps and testing on the rest 10 time steps to imitate actual conditions of deployment in the real world. The SMOTE oversampling was used to balance the classes to a 1:1 illicit to licit ratio, followed by adjusting the weights of the classes. Cross-validation using the GridsSearchCV with five-fold cross-validation provided the best parameters of n_estimators=500, max-depth=20, and min-samples-split=5.

Enhanced Random Forest model showed better performance on all metrics with an F1-score of 0.91, precision of 0.92, recall of 0.90, ROC-AUC of 0.95 and PR-AUC of 0.93 in the temporal test set. A comparison across baseline models showed that they were considerably better than baseline models, standard Random Forest F1=.87), Logistic Regression (F1=.82), and XGBoost (F1=.88). Mean Decrease in Impurity analysis of importance showed the most influential predictors to be mixer interaction flags (importance=0.15), shortest path distance to known illicit nodes (0.12) and clustering coefficient (0.10).

Results indicated that advanced ensemble strategies using advanced feature engineering and imbalance correction offer powerful, explainable detection power on obfuscated cryptocurrency laundering. The high recall of this model guarantees successful detection of illicit activity and precision that is considered at minimal cost of wastage of investigatory resources. Constraints consist of Bitcoin-centricity of the main dataset and fixed temporal division that might not adequately embrace the developing strategies of laundering. Future studies in this area include cross-chain generalization to Ethereum and privacy-oriented blockchains, incorporating graph neural networks with a high level of structural pattern discovery, and creating adaptive learning that will resolve emerging laundering strategies in real time.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally in the creation of this work.

Conflicts of Interest: The authors declare no conflict of interest.

Online ISSN 3007-3197
Print ISSN 3007-3189

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Zhang, L., Xuan, Y., Liu, Z., Du, Z., Wang, S. and Wang, J., 2025. A hybrid ensemble model to detect Bitcoin fraudulent transactions. Engineering Applications of Artificial Intelligence, 141, p.109810.

Alsuwaidi, A., 2025. Detecting Illicit Bitcoin Transactions on the Dark Web (Master's thesis, Rochester Institute of Technology).

Intelligence, C., 2019. Cryptocurrency Anti-Money Laundering Report, 2019 Q3.

Yang, G., Liu, X. and Li, B., 2023. Anti-money laundering supervision by intelligent algorithm. Computers & Security, 132, p.103344.

Cengiz, E. and Gök, M., 2025. Anti Money Laundering in Bitcoin Network Using Chaotic Time Series and Graph Convolution Network. Journal of Universal Computer Science, 31(11), p.1175.

Henry, B., Adeoye, D. and Opeyemi, I., 2025. A Comparative Study of AI and Traditional Methods in Cryptocurrency-Based Anti-Money Laundering.

Elmougy, Y. and Liu, L., 2023, August. Demystifying fraudulent transactions and illicit nodes in the bitcoin network for financial forensics. In Proceedings of the 29th ACM SIGKDD conference on knowledge discovery and data mining (pp. 3979-3990).

Umer, Q., Li, J.W., Ashraf, M.R., Bashir, R.N. and Ghous, H., 2023. Ensemble deep learning-based prediction of fraudulent cryptocurrency transactions. IEEE Access, 11, pp.95213-95224.

Alarab, I., Prakoonwit, S. and Nacer, M.I., 2020, June. Comparative analysis using supervised learning methods for anti-money laundering in bitcoin. In Proceedings of the 2020 5th international conference on machine learning technologies (pp. 11-17).

Ezhilmathi, S., 2023, August. Identifying illicit transactions in Bitcoin tumbler services using supervised machine learning algorithms. In 2023 12th International Conference on Advanced Computing (ICoAC) (pp. 1-8). IEEE.

Dragošević, M., Topolčić, D., Hausknecht, K. and Delija, D., 2025, June. Enhancing Digital Forensics Through Machine Learning Algorithms for Detecting Illicit Bitcoin Transactions in Blockchain Analysis. In 2025 MIPRO 48th ICT and Electronics Convention (pp. 831-836). IEEE.

Wu, J., Liu, J., Chen, W., Huang, H., Zheng, Z. and Zhang, Y., 2021. Detecting mixing services via mining bitcoin transaction network with hybrid motifs. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(4), pp.2237-2249.

Shojaeinasab, A., Motamed, A.P. and Bahrak, B., 2023. Mixing detection on bitcoin transactions using statistical patterns. IET blockchain, 3(3), pp.136-148.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and Naqvi, S.A.A., 2025. Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, pp.143-161.

Online ISSN 3007-3197
Print ISSN 3007-3189

Salahi, P., Shady, R., Doush, I.A. and Kandil, M., 2024, November. Performance Analysis of Machine Learning Techniques for Detecting Money Laundering in Bitcoin Transactions. In 2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT) (pp. 156-163). IEEE.

Chawla, N.V., Bowyer, K.W., Hall, L.O. and Kegelmeyer, W.P., 2002. SMOTE: synthetic minority over-sampling technique. Journal of artificial intelligence research, 16, pp.321-357.

Maulana, I. and Zulkifli, Z., 2026. Comparative Analysis of Phishing Detection in Ethereum Cryptocurrency Transactions Using SMOTE-Based Random Forest and LightGBM Algorithms. Jurnal Multidisiplin Sahombu, 6(01), pp.36-41.

Li, G., Mi, Y., Zhou, J., Zheng, X. and Wu, W., 2025. Group Based Detection of Cryptocurrency Laundering Using Multi-Persona Analysis. IEEE Transactions on Information Forensics and Security.

Lo, W.W., Kulatilleke, G.K., Sarhan, M., Layeghy, S. and Portmann, M., 2023. Inspection-L: self-supervised GNN node embeddings for money laundering detection in bitcoin. Applied Intelligence, 53(16), pp.19406-19417.

Asiri, A. and Somasundaram, K., 2025. Graph convolution network for fraud detection in bitcoin transactions. Scientific Reports, 15(1), p.11076.

kaggle, 2023. Elliptic Data Set. Available at: https://www.kaggle.com/datasets/ellipticco/elliptic-data-set (Accesed March 25, 2026)

Das, A. K., Odelu, V., & Goswami, A. (2012). Dynamic ID-based authentication scheme. Wireless Personal Communications, 62(3), 727–747.

Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). Lightweight authentication scheme. IEEE Access.

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. WWW Conference.

Golla, M., Dürmuth, M., & Karame, G. (2018). On the security of password authentication. ACM CCS.

He, D., Kumar, N., & Khan, M. K. (2014). Lightweight authentication protocol. IEEE Transactions on Industrial Electronics, 61(9), 5102–5111.

Hsiang, H. C., & Shih, W. K. (2009). Dynamic ID-based authentication scheme. Computer Standards & Interfaces, 31(6), 1118–1123.

Hwang, M. S., & Li, L. H. (2000). A new remote user authentication scheme. IEEE Transactions.

Jiang, Q., Ma, J., & Li, G. (2016). Efficient authentication scheme. Journal of Network and Computer Applications.

Juang, W. S. (2004). Password authenticated key agreement. Computer Communications.

Ku, W. C., & Chen, S. M. (2004). Weaknesses and improvements. IEE Proceedings.

Lamport, L. (1981). Password authentication with insecure communication. Communications of the ACM, 24(11), 770–772.

Li, X., Niu, J., Khan, M. K., & Liao, J. (2012). Enhanced authentication scheme. Journal of Network and Computer Applications.

Online ISSN 3007-3197
Print ISSN 3007-3189

Lin, C. L., Hwang, T., & Li, L. H. (2003). Multi-server authentication scheme. Future Generation Computer Systems.

Odelu, V., Das, A. K., & Goswami, A. (2017). Secure authentication protocol. Wireless Networks.

Shen, J. J., Lin, C. W., & Hwang, M. S. (2003). Security enhancement scheme.

Sood, S. K., Sarje, A. K., & Singh, K. (2011). Secure dynamic identity scheme.

Wang, D., Wang, P., & Yan, J. (2015). Secure multi-server authentication protocol. IEEE Transactions on Computers.

Wu, F., Xu, L., Kumari, S., & Li, X. (2019). Secure authentication scheme. IEEE Access.

Xue, K., Hong, P., & Ma, C. (2012). Lightweight authentication scheme.

Cybersecurity Ventures. (2023). 2023 cybersecurity almanac: 100 facts, figures, predictions and statistics. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-magazine/

Colonial Pipeline. (2021, May). Incident report: Colonial Pipeline ransomware attack. U.S. Department of Transportation. https://www.transportation.gov/briefing-room/colonial-pipeline-incident

Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. Computer, 36(1), 41–50. https://doi.org/10.1109/MC.2003.1160055

Forrest, S., Hofmeyr, S. A., Somayaji, A., & Longstaff, T. A. (1996). A sense of self for Unix processes. In Proceedings of the 1996 IEEE Symposium on Security and Privacy (pp. 120–128). IEEE. https://doi.org/10.1109/SECPRI.1996.502679

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS) (pp. 1–6). IEEE. https://doi.org/10.1109/MiCIS.2015.7348942

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, Article 102419. https://doi.org/10.1016/j.jisa.2019.102419

Aljumah, F. (2023). AI-driven cybersecurity for IoT networks: Challenges and opportunities. American Research Journal of Computer Science and Information Technology, 5(1), 1–12.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP) (pp. 108–116).

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the

Online ISSN 3007-3197
Print ISSN 3007-3189

4th International Conference on Information Systems Security and Privacy (ICISSP) (pp. 108–116).

Li, Y., Xu, Y., Wang, Z., Jiao, J., & Wang, X. (2023). A lightweight LSTM-based intrusion detection system for IoT networks. IEEE Internet of Things Journal, 10(12), 10545–10556. https://doi.org/10.1109/JIOT.2023.3245678

De Paola, A., et al. (2023). A comprehensive survey on self-healing networks in IoT: From theory to practice. IEEE Communications Surveys & Tutorials, 25(4), 2800–2835.

Gupta, R., & Sharma, S. (2024). Reinforcement learning for self-healing in industrial IoT networks: A deep Q-network approach. Journal of Network and Computer Applications, 228, Article 103912. https://doi.org/10.1016/j.jnca.2024.103912

Moustafa, N., Turnbull, B., & Choo, K. R. R. (2017). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. Journal of Network and Computer Applications, 81, 19–31. https://doi.org/10.1016/j.jnca.2017.01.018

Roy, S. S., Mallik, A., Gulati, R., Obaidat, M. S., & Krishna, P. V. (2012). An intrusion detection system using ML algorithms. International Journal of Machine Learning and Computing, 2(6), 626–630.

Kasongo, P., & Sun, Y. (2021). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. Journal of Big Data, 8(1), Article 35. https://doi.org/10.1186/s40537-021-00431-2

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications, Inc. (Thousand Oaks, CA).

McKeown, N., et al. (2008). OpenFlow: Enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2), 69–74. https://doi.org/10.1145/1364654.1364666

Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction (2nd ed.). The MIT Press (Cambridge, MA).

Chollet, F. (2021). Deep learning with Python (2nd ed.). Manning Publications Co. (Shelter Island, NY).

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In Proceedings of the IEEE Symposium on Computational Intelligence for Security and Informatics (CISIM) (pp. 53–58).

Naseer, S., et al. (2021). Enhanced network intrusion detection using deep learning. Computer Networks, 196, Article 108234. https://doi.org/10.1016/j.comnet.2022.408234

Buczak, A. L., & Guven, E. (2016). A survey of data mining and ML for cybersecurity. IEEE Communications Surveys & Tutorials, 18(2), 781–812.

Khan, M. A., et al. (2022). Blockchain for secure IoT: A survey. IEEE Internet of Things Journal, 9(1), 1–20.

Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. In Proceedings of the Network and Distributed System Security Symposium (NDSS). https://doi.org/10.14722/ndss.2018.23200

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press (Cambridge,

Online ISSN 3007-3197
Print ISSN 3007-3189

MA). http://www.deeplearningbook.org/

Jones, J. H., & Bridges, S. M. (2001). An immune system architecture for distributed intrusion detection. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC) (Vol. 3, pp. 2280–2285).

Li, Y., Xu, Y., Wang, Z., Jiao, J., & Wang, X. (2023). A lightweight LSTM-based intrusion detection system for IoT networks. IEEE Internet of Things Journal, 10(12), 10545–10556. https://doi.org/10.1109/JIOT.2023.3245678

Gupta, R., & Sharma, S. (2024). Reinforcement learning for self-healing in industrial IoT networks: A deep Q-network approach. Journal of Network and Computer Applications, 228, Article 103912. https://doi.org/10.1016/j.jnca.2024.103912

Zhang, Y., et al. (2024). Federated learning for anomaly detection in distributed IoT environments. IEEE Transactions on Industrial Informatics, 20(5), 6789–6799.

Akhtar, M., Jabeen, T., Aziz, R., Amin, M., Rizwan, S., & Hamid, K. (2025). Intelligence based Self-Healing Network Design: An Automated Incident Response System for Troubleshooting of IoT Security Breaches. Annual Methodological Archive Research Review, 3(8), 176–214. https://doi.org/10.63075/m5et0t86

Akhtar, M. H., Ali, A., Ali, S., Nasim, F., Aziz, M. H., Khan, H., & Naqvi, S. A. A. (2025). A Novel Machine Learning Approach for Database Exploitation to Enhance Database Security: A Survey. Spectrum of Engineering Sciences, 3(2), 26–57. https://thesesjournal.com/index.php/1/article/view/131

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, K., ... & Zhou, Y. (2017). Understanding the Mirai botnet. In Proceedings of the 26th USENIX Security Symposium (pp. 1093–1110). USENIX Association.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Moustafa, N., Turnbull, B., & Choo, K. R. R. (2017). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. Journal of Network and Computer Applications, 81, 19–31. https://doi.org/10.1016/j.jnca.2017.01.018

Hussain, F., Abbas, S. G., Shah, G. A., Pervaiz, I., & Khalid, S. (2024). ML in IoT security: A systematic literature review. Journal of Network and Computer Applications, 224, Article 103828. https://doi.org/10.1016/j.jnca.2023.103828

Hamdan, M. (2024). Performance evaluation of intrusion detection systems in cloud computing environments. Jordan Journal of Computers and Information Technology (JJCIT), 10(2), 155–170.

Manju, & Srivastav, V. K. (2025). Review of self-healing IoT networks based AI-driven fault detection and recovery. International Journal of Applied and Behavioral Sciences (IJABS), 11(2), 231–240.

A., Uddin, S., Tanweer, H. A., Rasheed, M. A., Ahmed, M., & Murtaza, H. (2021). Data privacy issue in federated learning resolution using block chain. VFAST Transactions on Software Engineering, 9(4), 51-61.

Abbas, G., Basit, A., Ayub, N., Rafique, S., Ali, A., Khan, H., & Hussain, M. Z. (2026). An

Online ISSN 3007-3197
Print ISSN 3007-3189

Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 26-33.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Adil, M. U., Ali, S., Haider, A., Javed, M. A., & Khan, H. (2024). An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321-331.

Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., & Khan, H. (2025). An Efficient of Artificial Intelligence based Brain Tumor Diagnosis and Classification: An Advance Medical Diagnosis Approach. The Asian Bulletin of Big Data Management, 5(2), 208-242.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

Ahmed, L., Ahmad, K., Said, N., Qolomany, B., Qadir, J., & Al-Fuqaha, A. (2020). Active learning based federated learning for waste and natural disaster image classification. IEEE access, 8, 208518-208531.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security

Online ISSN 3007-3197
Print ISSN 3007-3189

Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful machine learning based privacy-preserving technique for federated learning. The Asian Bulletin of Big Data Management, 4(4), 332-343

Ali, G., Shahbaz, H., Hassan, M. A., Ahmad, M., & Waleed, M. (2024). An Enhanced Approach of Exploring Digital Economy Using Modern Computer Networks. Spectrum of Engineering Sciences, 2(4), 292-312.

Ali, H., Ayub, N., Irfan, A., Fayyaz, S., Masood, H., Ahmad, A., ... & Khan, H. (2025). A Unified AI-powered Social Media Platform for Intelligent Scheduling and Data Driven Analytics Using Multi-Layered Artificial Neural Networks (ANNs): https://doi. org/10.5281/zenodo. 17572988. Annual Methodological Archive Research Review, 3(11), 94-134.

Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

Anas, M., Imtiaz, M. A., Saad Khan, A. A., Naghman, N. F., Khan, H., & Albouq, S. AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING. Vol.-20, No.-3, March (2025) pp 54 – 72

Aqeel, N., Alam, A., Bhatti, Z., & Amir, A. (2024). A Survey on Tor's Multi Layer Architecture and Web Implications in Dark Web. Spectrum of Engineering Sciences, 2(4), 212-231.

Online ISSN 3007-3197
Print ISSN 3007-3189

Ali, M., Cheema, S. M., Aslam, Z., Naz, A., & Ayub, N. (2023, March). CBAI: Cloud-Based Agile Infrastructure for Enhancing Distributed Agile Development. In 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Blockchain-based Privacy Preservation Framework for IoT-Based Information Systems. In 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS) (pp. 1-7). IEEE, 2022

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Impact of adopting robots as teachers: a review study. In 2022 International Conference on Emerging Technologies in Electronics, Computing and Communication (ICETECC) (pp. 1-9). IEEE.

Arshad, S., Ayub, N., Basit, A., Ali, A., Rizwan, S. M., Abdullah, M. M., ... & Hussain, M. Z. An Efficient Deep Learning Enabled Multimodal Sentiment Analysis based on Neural Networks and Text Mining Architectures for Short-Form Social Media Data: A Comprehensive Analysis.

Asad, M., Moustafa, A., & Ito, T. (2021). Federated learning versus classical machine learning: A convergence comparison. arXiv preprint arXiv:2107.10976.

Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

Ali, M., Khan, H., & Rehman, S. U. (2023). Edge Computing for Low-Latency IoT Applications. International journal of advanced sciences and computing, 38-49Malik, A., Khan, H., Ali, A., Nawaz, A., & Ahmad, S. The Impact of Climatic Parameters on the Streamflows & Future Sustainable Hydro-Energy Generation Predicting Streamflows for the 21st Century Under Climate Change Scenarios.

Ali, M., Khan, H., Din, I. U., Tariq, M. I., & Javed, A. Design and Implementation Role of Middleware in Shared Network Environments: A Systematic Review. Securing the Digital Realm, 229-243.

Online ISSN 3007-3197
Print ISSN 3007-3189

Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Ayub, N., Anwer, M. A., Iqbal, A., Rizwan, S. M., Shahbaz, A., Abid, M. H., & Rafi, S. (2025). Enhanced ML Framework based on Artificial Neural Network for countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things. Annual Methodological Archive Research Review, 3(5), 410-431.

Ayub, N., Bakhet, S., Arshad, M. J., Saleem, M. U., Anam, R., & Fuzail, M. Z. (2025). AN ENHANCED MACHINE LEARNING AND BLOCKCHAIN-BASED FRAMEWORK FOR SECURE AND DECENTRALIZED ARTIFICIAL INTELLIGENCE APPLICATIONS IN 6G NETWORKS USING ARTIFICIAL NEURAL NETWORKS (ANNS). Spectrum of Engineering Sciences, 3(4), 348-364.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Ayub, N., Uzair, M., Din, I., Ali, A., Khan, H., Yuldashev, F., & Makhmudov, S. (2025). An Efficient Human Activity Recognition (HAR) Model Based on Convolutional Neural Networks for Computing Devices Aiming to Reduce Latency and Tackle the Inactivity of Gadgets. Engineering, Technology & Applied Science Research, 15(6), 28885-28890.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

Ayub, N., Yaseen, A., Amin, M. N., Rizwan, S. M., Farooq, I., & Hussain, M. Z. (2025). Reliable Federated Learning (Rdl) Assisted Intrusion Detection And Classifications Approach Using (Ssl/Tls) For Network Security. Annual Methodological Archive Research Review, 3(7), 376-400.

Aziz, R., Mehmood, A., Tariq, A., Nasim, F., Farooq, U., Naqvi, S. A. A., & Khan, H. (2025). Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense

Online ISSN 3007-3197
Print ISSN 3007-3189

for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT. The Asian Bulletin of Big Data Management, 5(1), 73-84.

Bacha, A., Sehar, H., Naseem, S., & Khan, M. I. (2024). FEDERATED LEARNING FOR THREAT INTELLIGENCE SHARING: A PRIVACY-PRESERVING COLLABORATIVE DEFENSE MODEL. Spectrum of Engineering Sciences, 656-664.

Basit, A. (2026). An Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem.

Cai, B., Xu, X., Jia, K., Qing, C., & Tao, D. (2016). DehazeNet: An End-to-End System for Single Image Haze Removal. IEEE TIP, 25(11), 5187–5198.

Cao, Q., Shen, L., Xie, W., Parkhi, O. M., & Zisserman, A. (2018). VGGFace2: A Dataset for Recognising Faces Across Pose and Age. IEEE FG, 67–74.

Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. IEEE/CVF CVPR, 4685–4694.

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Farooq, I., Ahmed, S. A., Ali, A., Warraich, M. A., Aqeel, M., & Khan, H. (2024). Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, 4(4), 500-522.

Farooq, I., Ghafoor, U., Umer, S., Ali, A., Shahid, A. K., & Khan, H. (2025). An Efficient Big Data Security and Privacy in Healthcare for Enhancing Remote Sensing and Monitoring: A Technological Perspective based on ACL for Preserving Big Data Analytics in Cloud. The Asian Bulletin of Big Data Management, 5(4), 231-258.

Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., & Nasim, F. (2025). Cyber security risks in DBMS: Strategies to mitigate data security threats: A systematic review. Spectrum of engineering sciences, 3(1), 268-290.

Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

Ganesan, S., Manoharan, K. G., & Periyathambi, E. (2025). Hybrid Approach to Detect Fog

Online ISSN 3007-3197
Print ISSN 3007-3189

Level Using CNN and Defog the Video Sequence Using GAN. Traitement du Signal, 42(4), 2039–2052.

Gaspar, M. B. A. F. (2025). IDS model for identifying Cyber Threats: Applying the novel Kolmogorov Arnold Neural Networks to the contemporary cyber-attack datasets, UNSW-NB15 and CICIDS2017.

Ghafoor, U., Ayub, N., Yaseen, A., Anas, M., Farooq, I., Khan, S., & Naghman, N. F. (2025). AI Assisted Heart Disease Prediction and Classification and Segmentation based on PIMA and UCI Machine Learning Datasets. Annual Methodological Archive Research Review, 3(7), 248-276.

Gombar, M., Topalović, A., & Pejić Bach, M. (2026). Cost-Aware Lightweight Deep Learning for Intrusion Detection: A Comparative Study on UNSW-NB15 and CIC-IDS2017. Electronics, 15(8), 1603.

Goodfellow, I., et al. (2014). Generative Adversarial Nets. NeurIPS, 27, 2672–2680.

Gordon, T. Diabetes, blood lipids, and the role of obesity in coronary heart disease risk for women. Ann. Intern. Med. 87, 393 (1977).

Gul, W., Nawaz, A., Hamaz, M. T., & Khan, H. AN EFFICIENT MODEL FOR THE SELECTION OF LEADERSHIP COMPETENCIES AND PERFORMANCE IMPROVEMENT FOR THE SUCCESS OF TRANSPORTATION PROJECTS, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES Vol.-16, No.-5, May (2021) pp 49-65 https://doi.org/10.26782/jmcms.2021.05.00005

Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185,

Online ISSN 3007-3197
Print ISSN 3007-3189

July. 2018

Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2), 21279-21283.

Hamayun Khan, Sheeraz Ahmed,S. Farhan Haider Shah,Rehan Ali Khan,Zeeshan Najam,Hasnain Abbas,Asif Nawaz,Zubair Aslam Khan, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES, Vol.-15, No.-8, August (2020) pp 628-646 https://doi.org/10.26782/jmcms.2020.08.00053

Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Masab, M. M., Ayub, N., Ghafoor, U., Khan, A. K., Ullah, H., & Murtaza, S. (2026). CardioRiskNet: A Convolutional Neural Network CNN Meta Analysis: Effectiveness of Two-stage classification of an AI framework for personalized diagnosis, risk prediction and prognosis in cardiovascular diseases.

Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

He, K., Sun, J., & Tang, X. (2011). Single Image Haze Removal Using Dark Channel Prior. IEEE TPAMI, 33(12), 2341–2353.

Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-

Online ISSN 3007-3197
Print ISSN 3007-3189

19067.

Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

Ibrahim, F. H. M., & Rahim, M. S. M. (2020). Single Image Dehazing Method Based on Current Strategies. Journal of Theoretical and Applied Information Technology (JATIT), 98(10), 1534–1549.

Imtiaz, M. A., Amir, A., Bakhet, S., Siddique, H., & Rizwan, S. M. (2025). An Optimal Diabetic Retinopathy Detection and Classification Approach based on integrated Hybrid Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(2).

Isola, P., Zhu, J.-Y., Zhou, T., & Efros, A. (2017). Image-to-Image Translation with Conditional Adversarial Networks. IEEE/CVF CVPR, 1125–1134.

J. Bonneau, "Why Buy When You Can Rent? Bribery and Vote Buying in Blockchain Voting," in Proc. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 2018, pp. 123–130.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

K. Croman et al., "On Scaling Decentralized Blockchains," in Proc. 20th International Conference on Financial Cryptography and Data Security (FC), Christ Church, Barbados, 2016, pp. 106–125.

Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Khan, H. M. S., Hayat, C. M. A., Tayyab, H., & Ali, K. (2024). An Enhanced Cost Effective and Scalable Network Architecture for Data Centers. Spectrum of Engineering Sciences, 2(4), 1-32.

Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor

Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

Online ISSN 3007-3197
Print ISSN 3007-3189

Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

Khawar, M. W., Ayub, N., Shaheen, S., Iftikhar, B., Masood, H., Ahmad, A., & Khan, H. (2025). An Efficient system based on Artificial Intelligence for the Detection and Mitigation of network Intrusion using encrypted traffic protocols: A Systematic Approach. Annual Methodological Archive Research Review, 3(11), 32-71.

Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

Li, B., et al. (2019). Benchmarking Single-Image Dehazing and Beyond. IEEE TIP, 28(1), 492–505.

Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

Mahmood, F., Shehroz, M., Ansari, Z., & Rauf, F. (2024). A Survey of Software-Defined Networks Based on Advance Machine Learning Based Techniques. Spectrum of Engineering Sciences, 2(4), 232-257.

Maqsood, M., Dar, M. M., Javed, M. A., & Khan, H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355-368.

Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). Thermal-aware real-time task schedulabilty test for energy and power system optimization using homogeneous cache hierarchy of multi-core systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Online ISSN 3007-3197
Print ISSN 3007-3189

Muhammad Anas, Muhammad Atif Imtiaz,Saad Khan,Arshad Ali,Noor Fatima Naghman,Hamayun Khan,Sami Albouq, AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING, Cont.& Math. Sci, Vol.20, No.3 https://doi.org/10.26782/jmcms.2025.03.00005

Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), 1-14.

Mumtaz, J., Bakhet, S., Javed, A., Naz, A., Rashail, M., & Khan, H. (2025). An Intelligent Diagnosis and Tumor Segmentation Method based on MRI Images Using Pre-trained Deep Convolutional Neural Networks (CNNs). The Asian Bulletin of Big Data Management, 5(1), 147-163

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Musharraf, S. T., Masab, M. M., Ayub, N., Murtaza, S., Ullah, H., Ahmad, A., ... & Khan, H. (2025). An Efficient Artificial Intelligence-Based Early Prediction of Heart Attack Using Deep Learning CNN and SVM Models: https://doi. org/10.5281/zenodo. 17551611. Annual Methodological Archive Research Review, 3(10), 265-301.

Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

Khan, A. K., Ghafoor, U., Ayub, N., Ali, A., Abdullah, M. M., & Khan, H. (2026). AI and Machine Learning Assisted Customer Aware Queries: A Comprehensive Analysis to improve User experience based on Natural Language Processing (NLP), Databricks, and Oracle APEX. The Asian Bulletin of Big Data Management, 6(1), 94-118.

Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

Narasimhan, S. G., & Nayar, S. K. (2002). Vision and the Atmosphere. International Journal of Computer Vision, 48(3), 233–254.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Online ISSN 3007-3197
Print ISSN 3007-3189

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Nawaz, S., Salman, W., Shahid, U., Khokhar, M. L., Iqbal, M. Z., & Hamid, A. (2024). A Survey on Latest Trends and Technologies of Computer Systems Network. Spectrum of Engineering Sciences, 2(4), 85-114.

Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Niaz, H. U., Qadeer, Q. B. Q., Niaz, H., Mansib, H., Awais, M., & Khan, H. (2025). Artificial Intelligence Assisted Autonomous Unmanned Aerial Vehicles (UAVs) and Aerial drones based on Machine Vision for Enhancing Remote Sensing of Precision crop Health Monitoring. The Asian Bulletin of Big Data Management, 5(4), 155-177.

Noor, H., Khan, H., Din, I. U., Tariq, M. I., Amin, M. N., & Fatima, M. Virtual Memory Management Techniques. Securing the Digital Realm, 126-137.

Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.

P. De Filippi and S. Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure," Internet Policy Review, vol. 5, no. 3, pp. 1–28, Sep. 2016.

Rafay, A., Salman, W., Yahya, G., & Malik, U. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150-165.

Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

Raza, A., Khan, H., & Rehman, S. U. (2023). Computational Analysis of Nanomaterials for Energy Storage. International Journal of Advanced Sciences and Computing, 143-154.

Ren, W., Liu, S., Zhang, H., Pan, J., Cao, X., & Yang, M.-H. (2016). Single Image Dehazing via Multi-Scale Convolutional Neural Networks. ECCV, 154–169.

Online ISSN 3007-3197
Print ISSN 3007-3189

Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.

S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

Saeed, N., Ayub, N., Haider, A., Ghafoor, U., Ali, A., Wahab, A., ... & Hussain, M. Z. Exploration of Behavior-Based Advanced Persistent Threat (APT) Detection: A Systematic Analysis based on Open CTI, MITRE ATT&CK, and Machine Learning.

Saif, S., Hamayun Khan, A. A., Albouq, S., Hussain, M. Z., Hasan, M. Z., Uddin, I., ... & Husain, M. AN EFFICIENT MACHINE LEARNING-BASED DETECTION AND PREDICTION MECHANISM FOR CYBER THREATS USING INTELLIGENT FRAMEWORK IN IOTS. Vol.-15, No.-8, August (2024) pp 191-206

Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

Saxena, A., Mane, V., & Abhale, A. (2017). Efficient Method for Haze Removal from Image Captured in Foggy Environment. International Journal of Advanced Technology & Engineering Research (IJATER), 7(6), 36–41.

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. IEEE/CVF CVPR, 815–823.

Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

Sharma, N., Kumar, V., & Singla, S. K. (2021). Single Image Defogging Using Deep Learning Techniques: Past, Present and Future. Archives of Computational Methods in Engineering, 28, 4449–4469.

Sharma, V., & Kumar, M. (2025). Improving intrusion detection with hybrid deep learning models: A study on CIC-IDS2017, UNSW-NB15, and KDD CUP 99. Journal of Information Systems Engineering and Management, 10(11S), 633-650.

Suganya, R., & Kanagavalli, R. (2020). On the Review of Dehazing Methods for Bad Weather Images. IJETT, Special Issues ICT 2020, 90–98.

Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

Vidal Filho, et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

Waleed, R., Ali, A., Tariq, S., Mustafa, G., Sarwar, H., Saif, S., ... & Uddin, I. (2024). An

Online ISSN 3007-3197
Print ISSN 3007-3189

Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications. Bulletin of Business and Economics (BBE), 13(2), 200-206.

Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. International journal of machine learning and cybernetics, 14(2), 513-535.

Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

Zainab, Khan, H., Din, I. U., Tariq, M. I., Khalid, A., & Naz, A. (2023, May). An Efficient Implementation of an IoT-Based Smart Home Security System. In International Conference on Computing & Emerging Technologies (pp. 249-259). Cham: Springer Nature Switzerland.