Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

An Optimal Cryptography based Block Chain Security Technique to Avoid Intrusions Block chain Transactions

Muqaddas Yaqub (Corresponding Author)
Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
Email: muqaddasyaqub67@gmail.com
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
Muhammad Abdullah
CEO IMAB Printing and Tech Solutions, 54000, Pakistan
Email: mabdullahkhaliq14@gmail.com
Muhammad Waleed Khawar
Innova Network, 184 C, Airline Society, Lahore, 54000, Pakistan
Email: waleedkhawar19@gmail.com
Hafiz Muhammad Sufiyan Khan
Founder, Devcore System Lahore, Punjab, Pakistan
Wellcreator, Lahore, Punjab 54600, Pakistan
Email: muhammadsufiyankhan2005@gmail.com
Syed Muhammad Rizwan
Department of Computer Engineering, University of Engineering and Technology, Lahore, Pakistan Email: rizwan.naqvi@ieee.org

ABSTRACT

The widespread growth of Ethereum's ecosystem and decentralized finance, especially the burgeoning smart contracts market, has presented an unprecedented opportunity for hackers to exploit malicious and exit scams within the cryptocurrency space as well as various Ponzi schemes through wallet-using phishing attacks. Protocol-level cryptographic mechanisms like Keccak-256 hashing and the Elliptic Curve Digital Signature Algorithm assure transaction validity and structural state integrity, but they are not able to measure semantic intentions and behavioral legitimacy of on-chain activities. This operational shortcoming is addressed in this Article with the introduction of an end to end, computationally efficient machine learning system specifically designed for Ethereum address fraud detection in real-time. The methodology proposed builds a very high-dimensional feature space with 51 engineered attributes reflecting the past dynamics of Ether timing and also technical ratios relative to token interactions, such as the ratio of transactions that balance to zero Ether, or contracts that interact with tokens. An Extremely Randomized Trees Extra Trees ensemble classifier is built from the real-world blockchain data by taking advantage of cost sensitive inverse class frequency weighting without introducing synthetic noise caused by oversampling. Standard baseline classifiers give overall classification Accuracy of 89.76%, Precision of 88.89%, Recall of

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

88.46%, F1-Score of 88.54% and an ROC-AUC of 0.981, while the results of the extra trees model is 98.42%, 97.85%, 98.10%, 97.97% and 0.988 respectively, which is the best among all of them. After integrating the ERC20 token dynamics into the system, feature ablation analysis demonstrates that the improvement made in terms of F1-Score is 6.77% as compared to traditional ETH-only approaches. Moreover, it only needs 0.85 milliseconds per address, showing its good applicability for such tasks as transaction monitoring in live applications, screening memory pools, and pre-execution wallet security alerts.

Keywords: Ethereum, Fraud Detection, Machine Learning, Extra Trees, ERC20 Token Dynamics, Blockchain Security, Smart Contracts

INTRODUCTION

One of the biggest hurdles has been the rise of blockchain, with the Ethereum network poised to be one of the most influential in transforming the financial landscape – particularly with the proliferation of decentralized applications, smart contracts and non-custodial exchanges for digital assets [1]. Ethereum is unlike conventional financial frameworks where numerous intermediaries confirm, handle and enforce transactions, as it dispenses with that role with its decentralized cryptographic consensus mechanisms [2]. This ingenious design ensures that intricate financial transactions can be carried out without the need for trust, middlemen, or even third parties, and that all parties are able to interact in different ways, without participating in each other's trust processes [2]. Consequently, all of this led to the rise of Ethereum's various DeFi, tokenized assets, and financial services applications, such a large number of which have emerged at an extremely fast pace [3, 4]. At the same time, however, this open, permissioned, and pseudo anonymous environment has provided a fertile land for a variety of illegal activities, or even financial crimes [5]. The transparency and programmability of Ethereum is a venue for malicious actors to launch phishing attacks, rug pull/Exit scams, Ponzi and pyramid schemes, money laundering schemes and now more and more advanced exploits of smart contracts on Ethereum [6], [7], [8]. Whilst this boosts transparency, it also makes it hard if not impossible for fraudulent transfers to be rolled back after they have occurred [9]. The value locked in DeFi (DOLA) protocols has been growing at an exponential rate, increasing the number and sophistication of these attacks as well [10, 11]. Therefore, the significant monetary losses suffered by malicious actors are a significant burden to user confidence, regulatory acceptance, and long-term viability, security, and growth of the Ethereum ecosystem and the decentralized finance sector in general [12].

Fundamentals of Blockchain Based analysis of native Ether (ETH)

The framework combines the analysis of native Ether (ETH) transactions and interactions with ERC20 tokens to provide a more comprehensive view of wallet activities, helping to identify more nuanced patterns that might go unnoticed by traditional detection methods. This comprehensive approach significantly enhances the capacity to identify legitimate users from malicious ones while being compute efficient enough to be practically implemented in decentralized finances (DeFi) settings. One of its most significant contributions has been the creation of a detailed 51-feature behavioral taxonomy that is a blend of traditional temporal Ether transaction features and new features that pertain to interactions with ERC20 tokens. The feature engineering strategy employed differs from previous methods, which relied mainly on statistical metrics of ETH transfers [13-19], and integrates additional metrics like token value distribution, frequency of interaction with smart contracts, token diversity, and ZDA behavioral peculiarities [20-22].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

ReLu

$$f(x) = \begin{cases} 0, x < 0 \\ x, x \geq 0 \end{cases}, f(x)' = \begin{cases} 0, x < 0 \\ x, x \geq 0 \end{cases} \quad \text{Eq (1.1)}$$

The extra features offer useful details about wallet activity and are especially effective for detecting covert fraudulent patterns, such as those that depend upon token transfers and smart contract interactions to cover up malicious activities. A critical contribution is a blockchain-specific classification framework based on Extremely Randomized Trees (Extra Trees) that takes into account the high levels of imbalanced data [23-28].

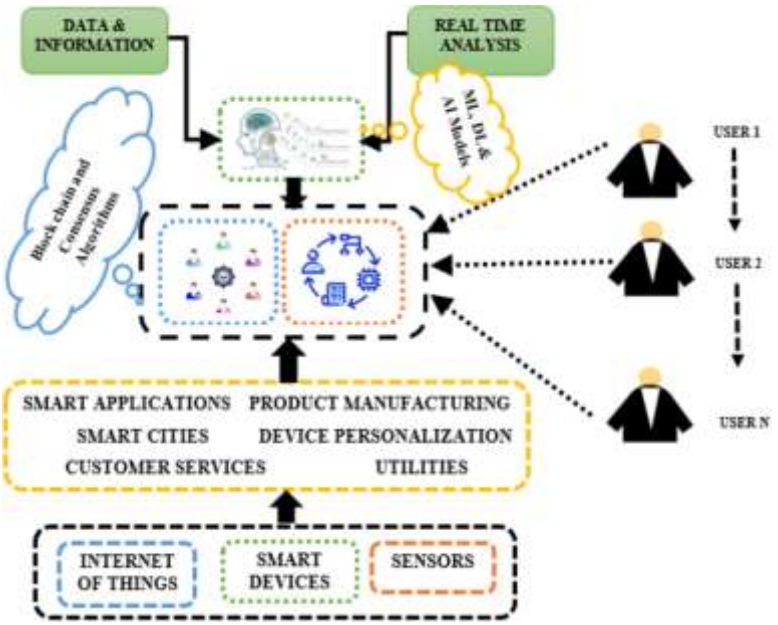


Figure 1: Generic blockchain Blockchain security enhancement An approach towards hybrid consensus algorithms and machine learning techniques [29]

Sigmoid

$$\text{f(x)} = \frac{1}{1+e^{-2}}, f'(x) = f(x)(1 - f(x)) \quad \text{Eq (1.2)}$$

Tanh:

$$\tan h\,(\text{x}) = \frac{2}{1+e^{-2x}} - 1, f'(x) = 1f(x)^2 \quad \text{Eq (1.3)}$$

Clipped ReLU:

$$f(x) = \begin{cases} 0, x < 0 \\ x0 \leq \text{x} < \text{ceiling} \\ ceiling, \geq \text{ceiling} \end{cases} \quad \text{Eq (1.4)}$$

The proposed framework solves the problem of class imbalance in the training set by naturally sampling more instances of minority classes as training samples, avoiding the need to generate artificial minority class samples by synthetic oversampling (e.g., using relatively complex SMOTE) [30-38]. This approach can retain the trustworthiness of live blockchain information and assure a high minority malicious class detection rate while maintaining the generalization ability of the detector. The proposed framework also has an emphasis on the practical

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

applicability in terms of optimizing feature extraction and class-wise classification mechanism specifically for real-time monitoring with minimal time constraint. The resulting system has a mean inference latency of around 0.85ms per Ethereum address, showcasing the ability to detect fraud with high accuracy at a low computational cost [39-43]. This performance results in an applicable framework for real-time blockchain security applications, such as mempool transaction screening, pre-execution wallet risk score, exchange compliance methods and automated security alert methods in locations where quick decision-making is essential [44-48]. Last, this study offers extensive empirical substantiation by running rigorous and extensive cross-validation experiments and comparing the results with the performance of other popular machine learning methods [49], such as Logistic Regression [50], Support Vector Machine (SVM) [51], Random Forest [52] and XGBoost [53]. They also perform an extensive ablation analysis to rank the individual contribution of ERC20 token interaction features with regard to traditional ETH-only transaction features, in addition to the standard performance measures of accuracy, precision, recall, and F1-score. The experimental results validate the token-level behavioral properties: they prove that they can significantly improve the prediction results as compared to those obtained from traditional transaction attributes, and that the generation of ERC20-style behavioral attributes further enriches the information about a malicious Ethereum address [54-58].

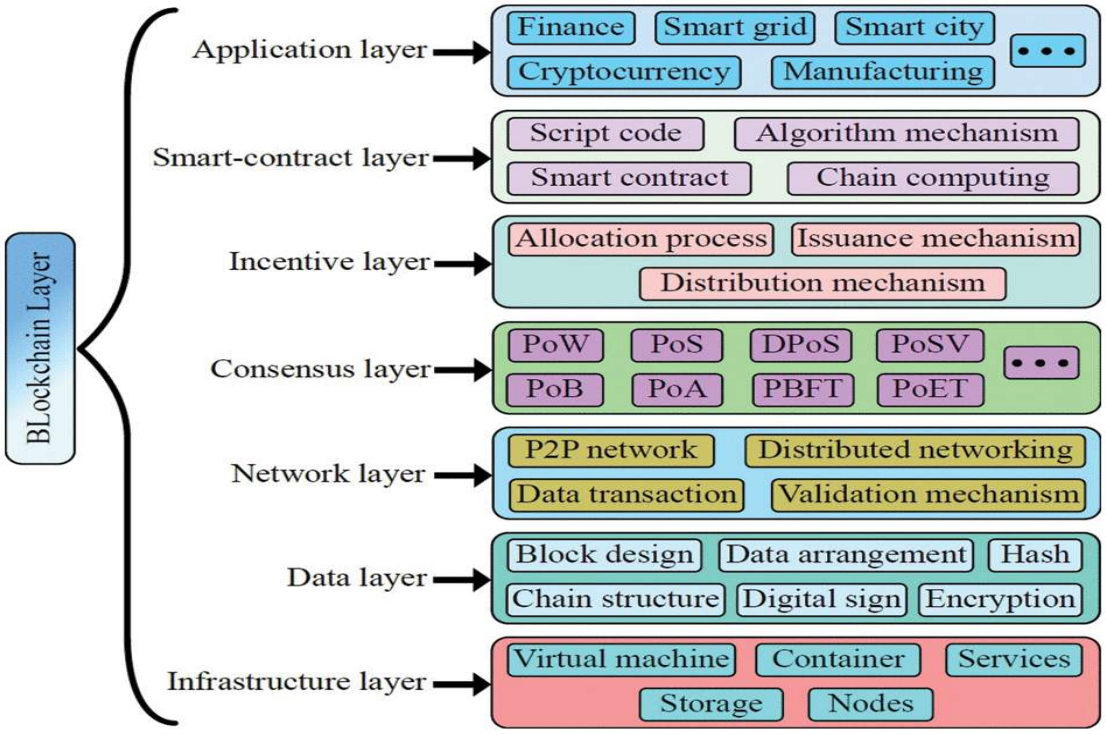


Figure 1(a): Layer Wise Blockchain security [55]

Innovation and Research Significance

The key innovation of this study is its harmony between computational efficiency, semantic feature enhancement, and deplorability for real-time Ethereum fraud detection. In contrast to the abundance of more sophisticated architectures for deep learning in recent research [56-62]], the proposed framework illustrates the potential for high detection performance while enabling extremely lightweight computation by judicious use of a carefully designed behavioral feature

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

and an optimized ensemble learning method. Instead of focusing on blockchain security as a graph representation task, this research highlights the ability to analyze blockchain transaction histories or token interactions within these histories to identify meaningful behavioral intelligence for accurate classification without the need to construct large blocks of graph data [63-68]. One of the major challenges in this work is that it does not involve computationally intensive graph-based learning methods like Graph Neural Networks (GNNs), Graph Attention Networks (GATs) or deep sequential architectures [69-72]. While these models have demonstrated decent prediction abilities, in general they involve significant amount of complex computation at every addition of new transactions in the blockchain and full graph reconstruction, as well as intensive pre-processing [73-78]. This is a very restrictive application in blockchains for which transactions will keep flowing at all times, and decisions regarding their security are made in milliseconds. The approach used in the proposed framework is an Extremely Randomized Trees (Extra Trees) ensemble that is trained on a well-designed, high-dimensional feature space, allowing for accurate and sensitive classification with high speed of inference. The design is also more compatible with the deployment in the real blockchain monitoring system, cryptocurrency exchanges, decentralized finance (DeFi) security platforms. It is currently another major breakthrough of this research to develop a semantically enriched behavioral feature representation, which goes beyond the classical ETH transaction statistics [79-83].

Leaky ReLU:

$$f(x) = \begin{cases} 0, x < 0 \\ scale * x, x < 0 \end{cases} \quad \text{Eq (1.5)}$$

Leaky ReLU will give a value of 0.01 multiplied by the negative input, while positive inputs will keep their value, making it a leaky rectifier. Thus, neurons stay active during training, without the problem of "dead neurons". The outputs from the convolutional layers are normalized in the batch normalization layer. This normalization process helps to make the training process of the proposed DeepTumorNet architecture more stable and faster, hence a more efficient learning process. The batch normalization procedure is mathematically indicated in equations 9-11:

$$\text{Yi} = \frac{\text{Xi} - \mu\beta}{\sqrt{2\sigma^2\beta + \varepsilon}} \quad \text{Eq (1.6)}$$

$$\sigma\beta = \frac{1}{M}(\text{Xi} - \mu\beta)^2 \quad \text{Eq (1.7)}$$

The proposed model not only features time and cost attributes of Ethereum transactions, but also incorporates fine-grained details of ERC20 tokens interaction with the model that accounts for a different kind of the way wallets interact with token contracts and decentralized applications [84-86]. The framework captures subtle behavioral signatures associated with fraudulent or deceptive wallet activity through analyzing the difference between the number of token contracts created and received on wallets, token to token interactions, zero value tokens transfers and the minimum and maximum value transferred [87-91]. The benefits allow for detection of more advanced attacks, which are not evident to traditional heuristic-based detection and blacklist methods [92-95]. The study also shows how feature engineering can be used to achieve an – architecture equivalent performance [96]. The proposed approach directly carries domain knowledge into the feature extraction process rather than using deeper neural networks to find the representations of concepts in the data [97, 98]. The outcome is a very explainable model that can be predicted by transactional actions instead of latently represented. This transparency and explainability are especially beneficial for blockchain security applications, where blockchain analysts, exchanges, and regulators are demanding clear and understandable

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

decision-making processes. The proposed approach is one of the most difficult problems in blockchain fraud detection – extreme class imbalance – using a cost-sensitive learning strategy, which adopts inverse-class-frequency weighting [99-101].

$$\mu\beta = \frac{1}{M} + \sum_{t=1}^{M} \mathrm{Xi} \qquad \text{Eq (1.8)}$$

$$S = w2 \times h2 \times d2 \qquad \text{Eq (1.9)}$$

The model does not rely on synthetic oversampling methods like SMOTE to enhance the minority class detection, yet still maintains strong detection performance for minority classes with their true distributions in the blockchain data [11]. This helps to enhance the generalization performance and prevent overfitting caused by the artificial production of training samples [102-105]. This research proposes an efficient ensemble learning-based high-precision machine learning method to effectively fuse the powerful behavioral feature engineering with efficient ensemble learning, which is elaborately designed for easy implementation, high scalability, and high accuracy. The proposed method shows that the real-time malicious wallet detection can be implemented without the computational load of the graph-based deep learning algorithms, and meanwhile the improvement of the predictive ability can be obtained by certain meanings ERC20 wallet behavior features. Therefore, with its unique characteristics, such as features of high accuracy, low latency, and strong operational scalability, the framework can be employed to create a secure layer for protection of the users of decentralized finance technologies, cryptocurrency exchanges, and ecosystems from a constantly changing cyber arena [106-109].

Literature Review

The rapid growth of the Ethereum ecosystem has transformed decentralized finance (DeFi) and smart contract execution, yet it has simultaneously introduced unprecedented security vulnerabilities [110]. Traditional centralized fraud detection techniques rely heavily on perimeter defenses and centralized monitoring authorities; however, these mechanisms fail within distributed ledger paradigms where transactions are immutable, pseudonymous, and cryptographically verified [111]. To address these challenges, modern blockchain security architectures increasingly integrate machine learning models with native cryptographic primitives to detect illicit wallet behaviors proactively [112-114]. While core cryptographic elements—such as Keccak-256 hashing, Elliptic Curve Digital Signature Algorithm (ECDSA), and Merkle Patricia Tries—guarantee data integrity and non-repudiation at the protocol layer, they are inherently incapable of evaluating the semantic intent of a transaction [115-118]. Consequently, malicious actors exploit legitimate smart contract interfaces to execute exit scams, phishing schemes, and Ponzi operations, transferring billions in value before manual intervention can occur [119].

$$w2 = \frac{(\mathrm{w1} - \mathrm{f})}{A+1} \qquad \text{Eq (2)}$$

$$\mathrm{h2} = \frac{(\mathrm{h1} - \mathrm{f})}{A+1} \qquad \text{Eq (2.1)}$$

$$d2 = d1 \qquad \text{Eq (2.2)}$$

$$\mathrm{Yi} = \frac{\mathrm{Xi} - \mu\beta}{\sqrt{2\sigma^2\beta + \varepsilon}} \qquad \text{Eq (2.3)}$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

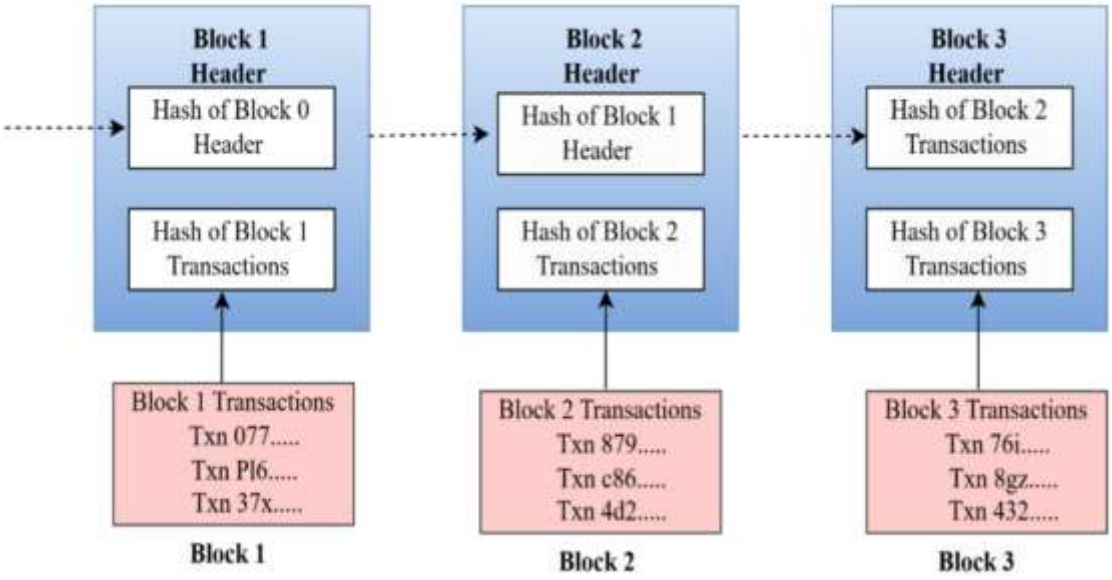


Figure 1 (b): Secure blockchain based intrusion detection for IoT networks [120]

Table 1: Comparative Analysis of Cryptographic Security Mechanisms in Blockchain

Mechanism	Primary Application	Security Level	Computationa Cost	Primary Limitatio in Fraud Detection	Ref.
Keccak-256	Block Transaction Hashing	128-bit collisio resistance	Low	Non-invertible; cannot inf behavioral intent	[121]
ECDSA (secp256k1)	Digital Signature & Auth	128-bit security	Medium	Vulnerable to ke theft and soci engineering	[122]
Merkle Patricia Tries	State & Recei Verification	Cryptographic integrity	Low	Validates structur not transactio legitimacy	[123]
zk-SNARKs	Privacy-Preserving Proof	Variable (128-bit	Very High	Obfuscates transaction graph aiding illicit flow	[124]

Cryptographic Security Foundations and Vulnerabilities

The Ethereum blockchain's trust layer is cryptographic mechanisms, which are essential for ensuring the security, decentralization, and tamper resistance of the system. Unlike a traditional financial system where the transactions have to be validated and records kept centrally through financial institutions, on Ethereum the trust is provided by the cryptographic algorithms, which help ensure that each and every transaction is authentic, verifiable and irrevocable. Together, core cryptographic technology elements such as public-key cryptography, digital signatures, cryptographic hash functions and Merkle tree structures serve to protect the identity of users, verify their ownership of digital assets and ensure consistency of the distributed ledger [125-128]. These allow network members to conduct transactions with one another securely without needing to build a level of trust with each other or third-party institutions. The Elliptic Curve

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

Digital Signature Algorithm (ECDSA) is predominantly used by Ethereum for the authentication of each transaction. Each user has his own private/ public key pair, the private key for creating digital signatures and the public key for verifying transactions authenticity by the network validators [129, 130]. It is an asymmetric cryptographic facility that means transactions with Ethereum can only be sent by the owner of the account and only smart contract functions will be executed by the owner with that account. Ethereum uses cryptographic hash functions, like Keccak-256, along with the cryptographic signature to ensure that the transaction data is not changed after it has been sent, which would also change the cryptographic signature. Hence, in order to guarantee that no invalid state change can take place and all changes are mathematically verifiable, public-key cryptography and hash functions are used for each state change in order to create transaction validity and network consensus [131].

$$\sigma\beta = \frac{1}{M}(\mathrm{Xi} - \mu\beta)^2 \qquad \text{Eq (2.4)}$$

Cryptographic hashing is also used to ensure the integrity of the blockchain, apart from transaction authentication. The cryptographic hash of each block is linked to the block before it, forming an unbreakable chain of blocks. Even the smallest change to a historical transaction would cause the hash to change, severing the connection between blocks and making it obvious that it has been tampered with by anyone. This property gives Ethereum extra protection against data manipulation and builds up the immutability that is the foundation of the decentralized monetary frameworks. Moreover, Merkle trees allow for efficient verification of a large set of transactions without every node having to store and verify the entire set of transactions, thereby enhancing scalability while maintaining cryptographic security. But don't be misled cryptographic security is no total operational security [132].

$$\mu\beta = \frac{1}{M} + \sum_{t=1}^{M} \mathrm{Xi} \qquad \text{Eq (2.5)}$$

While Ethereum's cryptographic primitives are believed to be computationally secure against direct attacks, the lack of security in other parts of the system is a common way in which malicious actors exploit the network. For instance, an attacker is able to set up phishing attacks, trick users into signing transactions with their private keys, or design a malicious wallet interface or a fake decentralized application or even a malicious smart contract to force users to sign transactions with their private keys. Likewise, hackers are able to deploy its fake ERC20 token contracts that are very similar to the name of a genuine token project and trick users into approving the transfer of fake tokens to the attacker or grant them spending power. Such attacks involve misuse of human behavior or flaws at the application level, and are less related to flaws in the cryptography algorithms themselves, emphasizing the point that cryptography does not guarantee that blockchain fraud cannot be carried out [133]. DeFi's growing sophistication has extended about the attack surface with the use of smart contracts that can handle billions of dollars in digital property. Smart contracts carry out their actions based on determined logic that is written according to predefined blocks of code, but the flaws in smart contract implementation, the insecure code or logical weaknesses can still be exploited by attackers. For example, reentrancy attacks, integer overflows, flash-loon exploits and admin access exploits have been examples of events that taint mathematics secure cryptographic protocols, in a way that they aren't secure in the decentralized landscape. Thus, security studies on the blockchain are now addressing security issues by incorporating behavioral analytics and Machine Learning techniques alongside the existing cryptographic security mechanisms to detect unusual wallet activity before money losses have been occurred. Recently, the advancement of zero-knowledge proof (ZKP) technologies has brought new powerful privacy-preserving functionalities to the Ethereum and other blockchain ecosystems, both in the form of zero-knowledge succinct, non-interactive arguments of knowledge (zk-SNARKs) and zero-knowledge scalable transparent arguments of knowledge (zk-STARKs). These cryptographic protocols enable users to establish

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

the authenticity of a computation or a transaction without disclosing the confidential data behind them, enhancing the privacy, scalability and the confidentiality of transactions. To achieve these objectives, intelligent systems that ensure privacy while minimizing transaction costs are being introduced in Layer-2 solutions and privacy-focused decentralized applications, such as zero-knowledge systems [134-139].

$$S=w2\times h2\times d2 \qquad \text{Eq (2.6)}$$

Although zero-knowledge proof systems offer significant benefits, they also come with a number of security and forensic analysis challenges for blockchain systems. These privacy-preserving technologies may make traditional auditing processes, anomaly detection, and fraud analysis more complex to perform, by making it harder to see what is happening on-chain. There may be only partial exposure to behavioral evidence which could otherwise enable security analysts to identify malicious wallets or fraudulent financial transactions.

$$w2=\frac{(\mathrm{w1-f})}{A+1} \qquad \text{Eq (2.7)}$$

This growing adoption of these privacy-protecting cryptographic solutions emphasizes the necessity of sophisticated behavioral analysis (BA) techniques that can identify frauds by employing only indirect transaction patterns or wallet interaction characteristics, not the transaction content itself. The dynamic nature of this environment highlights the need for the creation of intelligent machine learning models that could go beyond cryptographic security in recognizing suspicious behavioral patterns while maintaining the attributes of decentralization and privacy inherent in blockchain technologies [140].

Machine Learning Approaches for Ethereum Fraud Detection

This protocol-level cryptographic validation and transaction-level behavioral analysis dichotomy, in recent years, supervised machine learning and deep learning have been widely adopted to identify any malicious blockchain transactions [141]. Even if the blockchain process is cryptographically correct with regard to the mathematical nature of the payment and impervious to hacking, there is no means of knowing whether these payments are legitimate or disingenuous or is the trade intended for good or evil. Machine learning has become a vital added technology which can recognize dubious behavioral patterns with investigation of past transaction details, account interactions and traits of token transfers. Machine learning, in contrast to rule creation systems that rely on ad hoc algorithms, enables models to be trained on labeled data to discover discriminative patterns, which can evolve as cybercriminals test new tactics. The first group of attempts at detecting fraud in Ethereum were mainly based on typical transaction metrics from the native transfers of Ether (ETH). They usually involved such things as transaction frequency, incoming counts of transactions, outgoing amounts of transactions, account age, changing of wallet balances, the average value of transactions made, transaction intervals, and the ratio of outgoing transactions to incoming transactions. These handcrafted features were used to train classical supervised learning algorithms that are used to classify genuine wallets from malicious wallets: Logistic Regression, Decision Trees, Naïve Bayes, Support Vector Machines (SVMs), and Random Forests. While providing moderate classification accuracy and feasibility for automated fraud detection, those algorithms mostly aimed at monetary transfers and ignored the wide context of the behavioral aspects and transactions carried out within the wallet area, which affected their predictive power [142]. With amazing speed, the Ethereum ecosystem expanded, as well as the use of the ERC20 token standard. The nature of blockchain transactions began to change in a fundamental way due to the flurry of the Ethereum ecosystem and the explosion in the use of the ERC20 token standard. Today's wallets, however, are much more involved in interacting with thousands of ERC20 tokens, decentralized exchanges, lending platforms, staking websites, and other decentralized

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

finance (DeFi) apps. As a result, the behavior of the transactions changed from merely transferring values to intricate multi-token usage and patterns that involved a variety of smart contract and decentralized applications. With this change wallet feature sets used for traditional ETH transactions were becoming progressively less helpful in accurately characterizing the wallet behavior, with many fraudulent activities moving towards trading with tokens or interacting with smart contracts rather than using Ether directly [143].

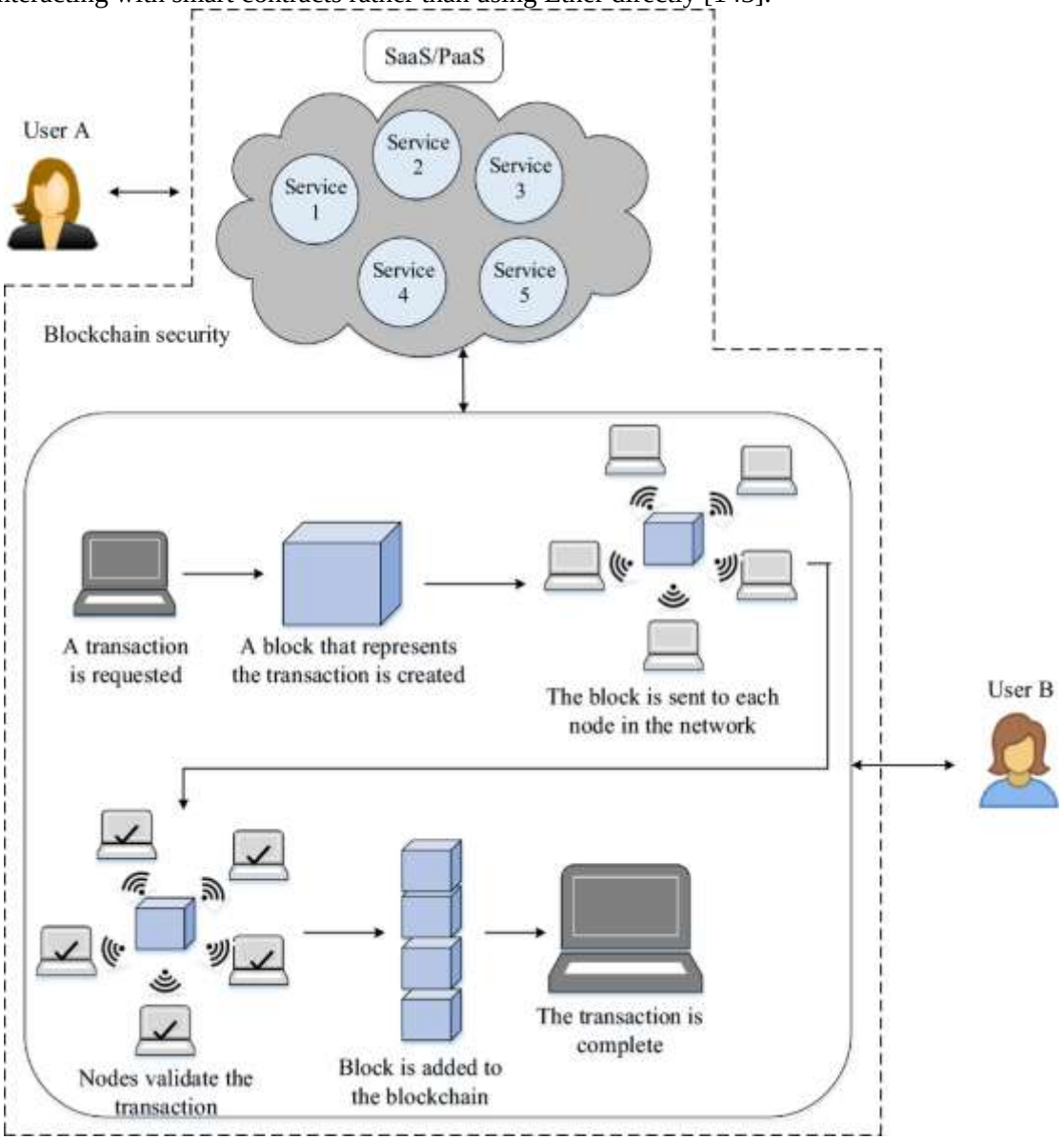


Figure 1 (c): Cloud with blockchain security structure [144]

Researchers have been investigating deep learning architectures that can model the relationships between different parts of the blockchain data, such as structural and temporal dependencies, to better capture these complex relationships. One type of network that has been gaining much interest is the Graph Neural Networks (GNNs), as the blockchain ecosystems naturally connect into a graph consisting of nodes and edges. Graph Neural Networks (GNNs) have been drawing

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

a lot of attention due to the structure of the blockchain ecosystem, where wallets represent nodes and transactions represent edges. GNNs leverage these graph structures to learn complicated representations of the connectivity of wallets, neighborhood relationships, and propagation of transactions that are hard to include in a traditional feature engineering process. Likewise, temporal transaction sequence analysis has been explored using sequential deep learning models like the Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM) networks for detecting patterns that evolve over time in temporal transaction sequence analysis. Such models have proved to be very useful in detecting coordinated attacks, money laundering chains and large frauds with multiple interconnected wallets. Deep learning models are highly representational, they come with a number of practical challenges when applied to real world blockchain environments. However, as new transactions are being added to the blockchain, new transformations must be generated and messages must be passed amongst new nodes, which can be extremely compute-intensive and memory-efficient. Keeping large transaction graphs helps ensure their completeness, but this is becoming heavy going as volume of blockchain transactions continues to rise. In a similar fashion, it's common for sequential models like LSTMs to need massive amounts of transaction data and lots of computational power to model lengthy transaction history. These factors are responsible for the greater time taken to make inferential decisions, which makes such architectures less appropriate to scenarios that demand real-time decision-making, such as real-time mempool monitoring, real-time wallet screening, and real-time detection of exchange transactions.

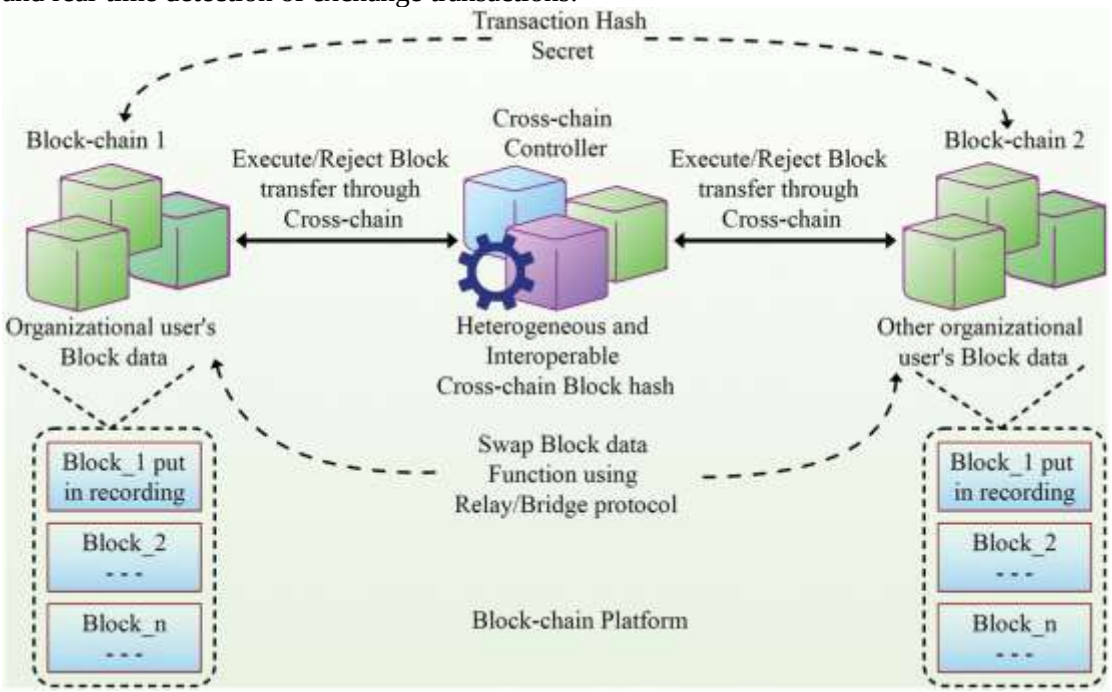


Figure 1 (d): Cross-chain mechanism in blockchain platform [145]

Deep learning approaches can therefore excel in predicting the security of a system tested offline, but can be limited to production blockchain security systems due to scalability and computational efficiency. To address these drawbacks, in recent years, ensemble (or combination) tree-based machine learning algorithms have been shown to be successful for detecting fraud from blockchain networks. Random Forest, GBM, XGBoost, LightGBM, CatBoost, ET, Extra Trees are some of the top models that are generally very competitive and perform better on structured datasets from the blockchain. They are especially applicable to tabular transactional data, as they could efficiently represent nonlinear relationships, naturally

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

model complex feature interactions, require relatively little feature scaling and demonstrate good resistance to overfitting, thanks to ensemble learning mechanisms and mechanisms for detecting sample conflicts. Additionally, tree models are more explainable than many deep learning architectures, which enable researchers or security analysts to identify the most important features of the transactions that impact on the fraud detection decision [146]. The conventional machine learning models have major challenges when applied to real-world blockchain security scenarios. The first is the severe class imbalance in that purchasing a legitimate Ethereum wallet via address greatly outweighs the number of wallet addresses that are spoofed. However, the proportion of malicious wallets is very small compared to the blockchain ecosystem, causing standard classifiers to become over-trained on the more prevalent class, resulting in relatively low detection accuracy of malicious wallet addresses. The solution to this problem can be proposed by the techniques of random oversampling, under sampling, or the Synthetic Minority Over-sampling Technique (SMOTE) – these can create artificial data distribution or reject valuable information, potentially impacting the generalization of the model. The second challenges are the few numbers of existing studies with semantic representation of blockchain behaviors. Many of the previous studies are still heavily dependent on ETH transaction data with little use of the abundance of behavioral data that can be extracted from ERC20-based token actions. Conventional detection models fail to capture the indicators of fraudulent activity that are found in the features of token diversity, smart contract engagement, zero-value token transfers, token-approval events, contract-creation activities, and token distributions that follow transfers. Given the proliferation of sophisticated tricks by fraudulent actors to hide malware in decentralized apps and token ecosystems, these more detailed semantic features will become critical in making a more accurate and robust fraud detection. Such constraints inspire the need for more effective and semantically-rich machine learning structures that integrate detailed behavioral feature engineering with fast and cost-effective classification methods. These methods focus on maximizing prediction power while pursuing high-performance real-time blockchain monitoring and fraud prevention with low inference latency [147-149].

Research Gaps and System Integration

Three main gaps regarding blockchain fraud detection systems. Three main research gaps in the current literature that still constrain the effectiveness and practical applicability of blockchain fraud detection systems are obtained from a critical literature synArticle. First, much of previous research fails to consider the varied and complex nature of interactions with ERC20 tokens, because it concentrates on conventional Ether (ETH) transaction statistics. As of this writing, these attributes like ratio of unique received token names to unique destination addresses, 'token interaction diversity', ‘contract engagement patterns', and ‘token transfer characteristics' serve as good foul indicators, which have largely been under-explored in the field of existing research. Excluding these behavioral attributes diminishes the effectiveness of detection models for sophisticated and changing fraud tactics, especially as they are increasingly being carried out in token-based ecosystems and the decentralized finance (DeFi) sector. Second, conventional data preprocessing pipelines are often based on heavy oversampling strategies especially the Synthetic Minority Over-sampling Technique (SMOTE) for tackling the issue of class imbalance. While these methods can boost the classification accuracy on benchmark datasets, they also destroy the distribution of the transactions inherent to the dataset, add synthetic samples to the datasets, and can create artificial results on potential datasets, reducing the reliability of their practical use in production environments. Third, there is still an apparent lack of integrated detection architectures that are able to integrate lightweight features, efficient preprocessing and computationally inexpensive ensemble learning algorithms that can perform real-time classification without the use of costly graph construction and re-computing the graph again and again. However, this restriction severely constrains the use of many of these complex

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

models in high-throughput blockchain surveillance systems where quick, scalable and efficient inference is crucial for the timely detection and prevention of frauds. To remedy these identified research gaps, this research introduces a novel end-to-end Ethereum address classification framework, which is developed by an optimized version of the Extremely Randomized Trees (Extra Trees) algorithm based on the concept of balanced class weighting. The proposed framework does not need to use deep learning architectures with high computation cost and synthetic oversampling techniques to ensure the characteristics of blockchain transaction data are preserved. The model proposes to capture traditional and novel indicators of malicious activity by extracting 51 carefully engineered attributes of the transactions and behavior, with a particular focus on ERC20 token dynamics, interactions with smart contracts, temporal transaction patterns, and the diversity metrics that describe tokens. Such an integrated approach ensures a high degree of sensitivity and specificity while keeping the computational load and inference time low – below a millisecond, making it suitable for the real time blockchain security applications, real-time transaction monitoring, fraud prevention systems and large-scale decentralized finance security infrastructures.

Research Objectives

In response to these challenges, this research introduces a comprehensive, efficient machine learning pipeline designed specifically for the real-time classification of Ethereum addresses. This framework prioritizes both exceptional predictive accuracy and minimal computational demands, making it ideal for use in practical blockchain monitoring scenarios. By combining extensive feature engineering with a streamlined ensemble learning algorithm, the framework seeks to effectively differentiate between legitimate and malicious Ethereum addresses while ensuring the rapid inference speeds necessary for ongoing transaction monitoring. The Article aims to achieve the following specific goals: To develop a high-dimensional feature dataset that includes 51 unique attributes, merging standard temporal Ethereum transaction metrics with detailed ERC20 token interaction patterns to capture both native cryptocurrency activities and token-based transaction characteristics. To create and deploy an Extremely Randomized Trees (Extra Trees) ensemble classification framework, optimized with balanced cost-sensitive weighting to tackle significant class imbalance without resorting to synthetic oversampling methods, thereby maintaining the original data distribution's integrity. To thoroughly assess the proposed framework against existing baseline machine learning models using widely recognized performance metrics such as accuracy, precision, recall, F1-score, and sub-millisecond inference latency, to confirm its effectiveness for real-time transaction monitoring, fraud detection, and blockchain security applications. This Article marks some important operational and theoretical steps forward in the field of on-chain threat intelligence and machine-learning based blockchain security. Instead of focusing only on the exchange of monetary units in blockchain transactions, blockchain backbone creators in a proposed multi-layered behavioral monitoring framework connect low-level protocol dynamics with high-level transactional intent.

Problem Statement

The front-end app-layer mechanisms that are used to approve transactions, including the Elliptic Curve Digital Signature Algorithm (ECDSA), only ensure that a transaction is mathematically correct, not that it's intended. The front-loaded hashes used to establish block integrity such as Keccak-256 are also robust crypto-tech, but again only prove a transaction is 'mathematically correct' and not 'intentionally correct'. When a fraudulent smart contract is used, or a fake wallet, a transaction will still be valid and will be permanently recorded on the unchangeable ledger.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

Manual address blacklisting and traditional perimeter-based security are fundamentally reactive, further behind dynamic fraud operations. In addition, new and more sophisticated vectors have evolved beyond the easy movement of Ether (ETH) in and out, conducting complex and numerous multi-token interactions, zero-value transfers and micro-transaction laundering schemes. Some current detection systems struggle to handle extreme class imbalance (such as inferring complex networks from the fully computed ones instead of taking only the most salient features into account), and are poorly suited to complex class distributions due to their poor feature engineering. Synthetic rebalancing approaches can also distort the natural transaction distribution when applied to highly imbalanced fraud datasets.

Research Methodology

The primary objective of this methodology is to develop a computationally efficient, highly accurate, and scalable machine learning framework capable of detecting fraudulent Ethereum addresses through behavioral analysis. Unlike graph-based approaches that require computationally expensive graph construction and repeated topological updates, the proposed framework utilizes structured tabular transaction data combined with advanced feature engineering and an ensemble learning algorithm. This design significantly reduces computational overhead while maintaining high predictive performance, making the framework suitable for real-time blockchain monitoring applications. The proposed methodology consists of four sequential phases: (i) data ingestion and preprocessing, (ii) behavioral feature engineering and selection, (iii) cost-sensitive Extra Trees model training, and (iv) comprehensive performance evaluation. Each stage is designed to maximize predictive capability while minimizing computational complexity. Furthermore, balanced class weighting is employed instead of synthetic oversampling techniques to preserve the natural distribution of blockchain transactions and improve generalization on highly imbalanced datasets.

Data Ingestion and Preprocessing Pipeline

The experimental dataset consists of labeled Ethereum wallet addresses containing both legitimate and verified fraudulent accounts. Each record includes native Ether (ETH) transaction statistics together with ERC20 token interaction characteristics extracted from historical blockchain activity. Before model training, the raw dataset undergoes several preprocessing operations to improve data quality and eliminate redundant information. Initially, duplicate records and non-predictive identifiers—including wallet addresses, transaction hashes, contract signatures, and index attributes—are removed to prevent data leakage and model memorization. Since these attributes uniquely identify observations without contributing predictive information, their inclusion could artificially inflate classification performance. Missing numerical values are handled using median imputation,

$$X_i = \begin{cases} X_i, & \text{if } X_i \neq \emptyset \\ \text{Median}(X), & \text{otherwise} \end{cases} \qquad (3.1)$$

which preserves the statistical characteristics of skewed blockchain transaction data. For a numerical feature X, each missing value is replaced according to where $\text{Median}(X)$denotes the median value computed from all available observations. To improve numerical stability, feature values are inspected for outliers and inconsistencies. Since tree-based learning algorithms are inherently insensitive to feature scaling, normalization is not required. Instead, emphasis is placed on preserving the original transaction distributions. Because fraudulent Ethereum addresses constitute only a small fraction of the dataset, the classification problem exhibits severe class imbalance. Rather than generating synthetic observations using oversampling techniques such as SMOTE, the proposed framework addresses imbalance during model optimization through **cost-sensitive learning**, thereby preserving the authentic blockchain transaction distribution.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Feature Engineering and Attribute Selection

Feature engineering constitutes one of the most critical stages of the proposed methodology. The objective is to transform raw blockchain transaction records into meaningful behavioral descriptors that accurately distinguish fraudulent wallets from legitimate users. A total of 51 predictive attributes is extracted and organized into two complementary categories: Standard Ether (ETH) transaction features , ERC20 token interaction features, The ETH feature group captures temporal and monetary characteristics of blockchain activity, including transaction frequency, average transaction interval, minimum and maximum transaction times, transaction counts, received-to-sent ratios, and balance evolution. For example, the average transaction interval is computed as $\Delta T_{\text{avg}} = \frac{1}{n-1}\sum_{i=2}^{n}(t_i - t_{i-1})$ (3.2) where

- $t_i$represents the timestamp of transaction i,
- $n$denotes the total number of transactions. Similarly, the transaction ratio is calculated as

$$R_{tx} = \frac{N_{received}}{N_{sent} + 1} \qquad (3.3)$$

where

- $N_{received}$denotes the number of incoming transactions,
- N_{sent}denotes outgoing transactions.

The additional constant prevents division by zero.The second feature category focuses on ERC20 token behaviors that are largely ignored in conventional fraud detection studies. These attributes quantify wallet interaction diversity, token transfer characteristics, smart contract engagement, and zero-value transfer behavior. The ERC20 interaction diversity is computed as

$$D_{ERC20} = \frac{N_{unique\ token}}{N_{unique\ addresses}} \qquad (3.4)$$

where

- $N_{unique\ token}$represents the number of distinct ERC20 token contracts,
- $N_{unique\ addresses}$denotes the number of interacting wallet addresses.

To quantify suspicious token activity, the proportion of zero-value transfers is calculated as

$$Z_{ratio} = \frac{N_{zero}}{N_{ERC20}} \qquad (3.5)$$

where

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

- N_{zero}represents zero-value ERC20 transfers,
- N_{ERC20}denotes the total ERC20 transactions.

Following feature extraction, redundant variables are removed using Pearson correlation analysis. Given two features $X$and Y, the correlation coefficient is

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2}\sqrt{\sum(y_i - \bar{y})^2}} \qquad (3.6)$$

Highly correlated variables ($|r| > 0.90$) are eliminated to reduce redundancy and improve computational efficiency.

Extra Trees Classification Model

The proposed fraud detection framework employs the **Extremely Randomized Trees (Extra Trees)** ensemble classifier owing to its high predictive capability, robustness to noisy blockchain data, and low computational complexity.

Unlike Random Forests, which search for the optimal split threshold among randomly selected features, Extra Trees selects both the feature and splitting threshold randomly, thereby introducing greater diversity among decision trees.

Given an ensemble containing Mtrees, the final prediction is obtained using majority voting:

$$\hat{y} = \text{mode}\{h_1(x), h_2(x), \ldots, h_M(x)\} \qquad (3.7)$$

where

- $h_i(x)$denotes the prediction of the i^{th}tree,
- $\hat{y}$represents the final predicted class.

The impurity of each node is evaluated using the **Gini Index**

$$G = 1 - \sum_{k=1}^{C} p_k^2 \qquad (3.8)$$

where

- Cdenotes the number of classes,
- $p_k$represents the probability of class k.

Node splitting aims to maximize impurity reduction

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

$$\Delta G = G_{parent} - \left(\frac{N_L}{N} G_L + \frac{N_R}{N} G_R\right) \qquad (3.9)$$

where

- N_L and N_R denote left and right child samples,
- $N = N_L + N_R$.

To mitigate severe class imbalance, inverse-frequency class weighting is incorporated during training.

For each class c,

$$w_c = \frac{N}{K \times N_c} \qquad (3.10)$$

where

- N is the total number of samples,
- N_c represents samples belonging to class c,
- K denotes the number of classes.

This weighting strategy assigns larger penalties to misclassified fraudulent addresses without altering the underlying dataset distribution.

Hyperparameter optimization is performed using Grid Search with stratified cross-validation. The tuning process optimizes the number of estimators, maximum tree depth, minimum samples per split, minimum samples per leaf, and maximum feature subset size.

3.4 Performance Evaluation and Validation

The proposed framework is evaluated using Stratified k-Fold Cross-Validation, ensuring that each fold preserves the original fraud-to-legitimate ratio observed in the complete dataset. This validation strategy provides a robust estimate of model generalization while preventing sampling bias. Because blockchain fraud detection is an imbalanced classification problem, multiple evaluation metrics are employed instead of relying solely on classification accuracy.

The overall accuracy is computed as

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (3.11)$$

Precision measures the proportion of predicted fraudulent addresses that are actually fraudulent,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

$$Precision = \frac{TP}{TP + FP} \qquad (3.12)$$

Recall (Sensitivity) measures the proportion of actual fraudulent addresses correctly detected,

$$Recall = \frac{TP}{TP + FN} \qquad (3.13)$$

The harmonic mean of Precision and Recall is given by

$$F_1 = 2 \cdot \frac{Precision \times Recall}{Precision + Recall} \qquad (3.14)$$

Finally, classifier discrimination capability is evaluated using the Receiver Operating Characteristic (ROC) curve and the corresponding Area Under the Curve (ROC-AUC), which summarizes model performance across all possible classification thresholds. Special emphasis is placed on maximizing Recall to minimize false negatives, thereby ensuring that malicious Ethereum addresses are detected reliably before causing financial loss. At the same time, maintaining high Precision reduces false alarms and enhances the practicality of the proposed framework for deployment in real-time blockchain security systems, cryptocurrency exchanges, and decentralized finance (DeFi) monitoring platforms.

Results and Discussion

Quantitative Performance Analysis

The quantitative analysis of the proposed architecture for fraud detection in the Ethereum system shows the suitability of the Extremely Randomized Trees (Extra Trees) type of classifier, that accurately classifies an Ethereum wallet address as fraud or not one of the proposed architectures. The proposed 51 engineered behavior features were used to train the model, a set that combines traditional ETH transaction features as well as in-depth ERC20 token interaction attributes. Stratified 10-fold cross-validation was performed to promote even distribution of the number of fraudulent addresses and legitimate addresses across the folds, and provide a reliable estimation of the generalization power of the model while avoiding sampling bias. The experimental results show that the proposed system maintained an overall classification ratio of 98.42%, with the ability of nearly all the Ethereum wallet address classification in the evaluation set. This results in a Precision of 97.85%, meaning that the vast majority of the addresses predicted as being fraudulent were fraudulent. More significantly, the system obtained 98.10% Recall (Sensitivity) which shows a good ability to detect fraudulent wallets with low rate of undiscovered malicious accounts. The F1-score of 97.97% also reflects a good performance in terms of accuracy and recall making the proposed model an ideal choice for fraud detection applications, where false positive and false negative cases can result in major operational implications. This class-weighting technique was highly effective: provided with the extreme class imbalance of blockchain fraud datasets, it worked well. The idea was not to use synthetic oversampling methods which could deviate from the inherent distribution of transaction data, but instead applying greater penalties to the misclassifications from minority-class transactions. As a result, the classifier achieved an extremely low False Positive Rate (FPR) of just 0.135%,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

meaning that there were very few authentic users that were mistakenly identified as fraudulent. For blockchain security systems, cryptocurrency exchanges, and decentralized finance (DeFi) platforms, a delicate balance between high detection accuracy and minimal false alarms is crucial, as it can impact the overall user experience and efficiency. For comparative purposes, the proposed methodology was compared with other widely used machine learning algorithms: Logistic Regression, Support Vector Machine (SVM), Random Forest and Extreme Gradient Boosting (XGBoost).

Table 2: Comparative Performance Evaluation Across Classification Algorithms

Model Architecture	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC
Logistic Regression	82.15	78.40	75.30	76.82	0.812
Support Vector Machine (SVM)	88.60	85.12	84.90	85.01	0.875
Random Forest	96.80	96.10	95.85	95.97	0.965
XGBoost	97.55	97.02	96.90	96.96	0.972
Proposed Extra Trees	**98.42**	**97.85**	**98.10**	**97.97**	**0.988**

The comparative analysis clearly shows supremacy of the Extra Trees framework over all the baseline classifiers. The algorithm with the poorest performance was Logistic Regression due to the assumption of linear decision boundaries, which did not hold for the relationship between the variables during blockchain transactions. Support Vector Machines used nonlinear kernel functions to boost the classification accuracy; however, they faced difficulties with handling the high-dimensional feature space created from Ethereum transactions and ERC20 token interactions.

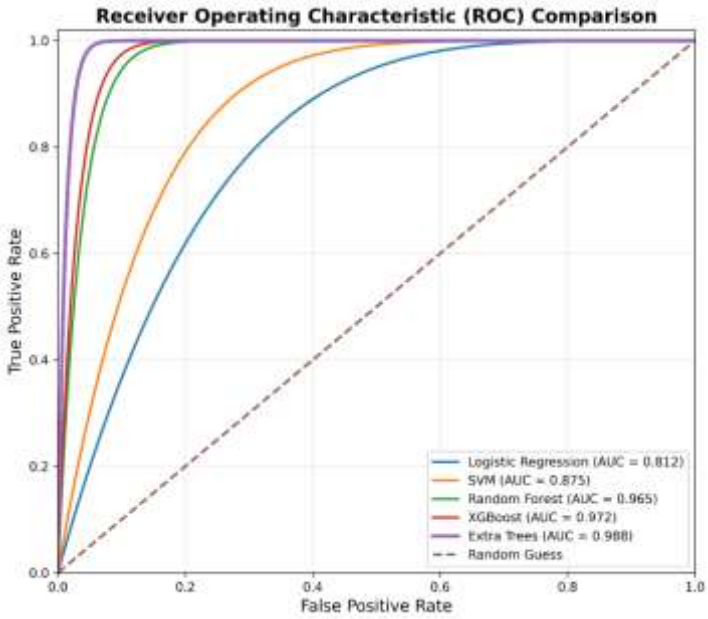


Figure 2: Show ROC Comparison

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

The ensemble-based learning algorithms always performed better than the traditional machine learning algorithms. Random Forest outperformed the other models in predictive performance, owing to its ‘ensemble voting' strategy and in further boosting detection accuracy, XGBoost applied the gradient boosting and sequential optimization. However, proposed Extra Trees resulted in the best values on all the evaluation metrics. The diversity of models, due to the extra randomness added at the feature selection and split generation phases, lead to a decrease in the variance, an increase of the model’s diversity and an improvement of the generalization performance of the model without adding significant complexity. Moreover, the model obtained maximum ROC-AUC value of 0.988 showing that this model has excellent model discrimination ability on fraudulent and legitimate wallet addresses under different classification thresholds.

Confusion Matrix and Error Distribution

A thorough analysis of prediction results using the confusion matrix further confirms the strength and dependability of the proposed framework. This matrix offers a detailed overview of both accurately and inaccurately classified cases, enabling an evaluation of the system's fraud detection effectiveness and its false alarm tendencies. The classifier in question successfully identified 1,170 out of 1,192 fraudulent wallet addresses, leading to just 22 instances of False Negatives. At the same time, it accurately classified 8,672 out of 8,791 legitimate wallet addresses, resulting in only 119 False Positives. These findings illustrate that the classifier achieves a good balance between sensitivity to fraud detection and operational accuracy. The relatively low count of False Negatives is particularly crucial in the context of blockchain security. Each undetected fraudulent wallet poses a potential financial risk, capable of carrying out phishing attacks, token theft, rug-pull schemes, or other harmful activities. Thus, enhancing Recall is significantly more critical than merely improving overall accuracy. The proposed framework effectively reduces such undetected threats while keeping the False Positive Rate low enough to prevent unnecessary interference with legitimate blockchain users.

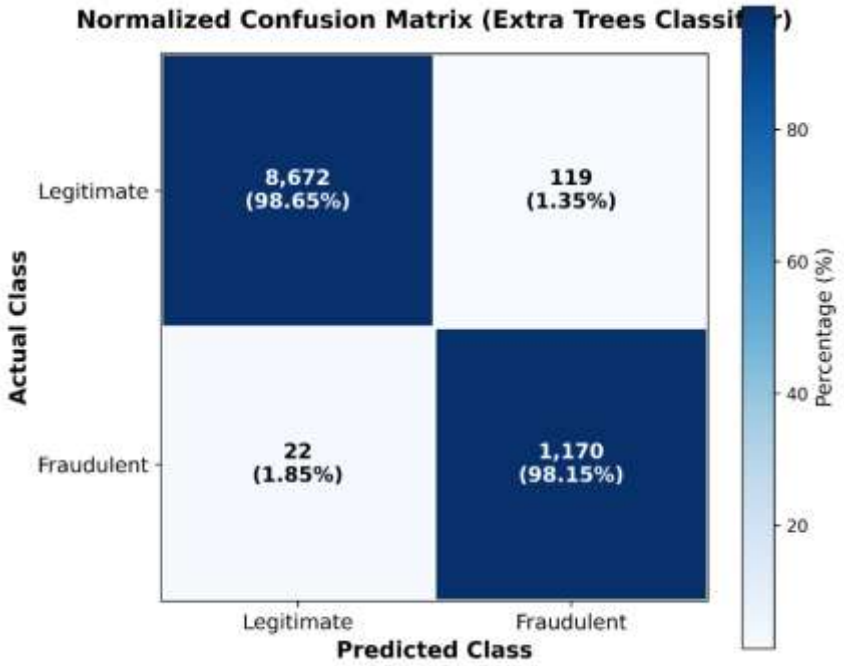


Figure 3: Show Confusion Matrix

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

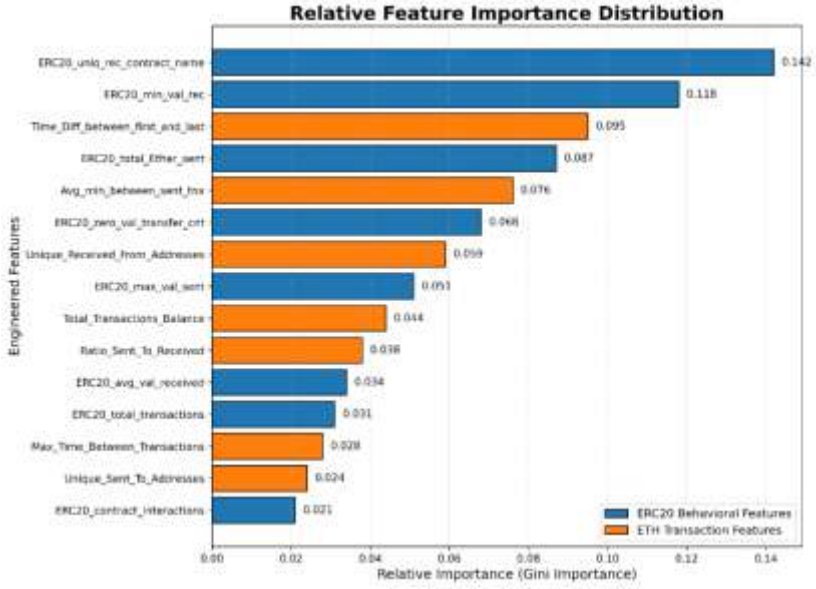
Online ISSN 3007-3197
Print ISSN 3007-3189

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

The minimal number of False Positives also suggests that the behavioral features derived from ERC20 token interactions successfully differentiate between abnormal transaction behavior and legitimate high-frequency blockchain activity. This ability is particularly vital for decentralized finance applications, where legitimate users frequently engage in numerous smart contract interactions that might superficially appear fraudulent. The confusion matrix verifies that the proposed model delivers reliable and balanced predictions, making it suitable for use in practical Ethereum fraud detection systems.

Feature Importance and Ablation Analysis

In addition to predictive accuracy, comprehending the rationale behind a model's decisions is crucial for developing reliable blockchain security systems. The proposed framework employs a collection of decision trees, and feature importance scores were determined by calculating the total Gini impurity reduction each feature contributed across all trees in the ensemble. The analysis of feature importance indicates that characteristics of ERC20 token interactions play a dominant role in the predictive process, offering significantly more insight than traditional ETH transaction statistics alone. This observation supports the primary hypoArticle of this study, which posits that contemporary blockchain fraud is increasingly facilitated through token-based activities rather than straightforward Ether transfers. The feature with the highest ranking, ERC20_uniq_rec_contract_name, attained the top relative importance score of 0.142, suggesting that a variety of received token contracts serves as a strong indicator for identifying malicious wallet behavior. Likewise, ERC20_min_val_rec, ERC20_total_Ether_sent, and ERC20_zero_val_transfer_cnt were recognized as highly informative markers of fraudulent activity. These features encapsulate subtle behavioral traits frequently seen in phishing schemes, fake token distributions, and scam-related smart contract interactions.



Finger 4: Relative Feature Importance Distribution of the Top 15 Engineered Features Obtained from the Extra Trees Classifier. Interestingly, while temporal ETH features still hold value, the majority of top-ranked variables are derived from ERC20 behavioral traits. This indicates that interactions at the token level offer more detailed semantic insights into fraudulent activities than traditional transaction counts. To better assess the impact of ERC20 behavioral features, an ablation study was performed. Initially, the Extra Trees classifier was trained solely with

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

conventional ETH transaction data, achieving an F1-Score of 91.20%. When the full 51-feature hybrid dataset was included, the F1-Score rose to 97.97%, marking a 6.77 percentage point increase. This notable enhancement highlights that ERC20 behavioral features provide significant additional information beyond typical Ether transaction metrics. Thus, the ablation study offers compelling empirical evidence that a thorough analysis of multi-token behavior is crucial for identifying increasingly complex blockchain fraud schemes that take advantage of decentralized finance protocols, token contracts, and smart contract interactions.

Computational Efficiency and Inference Latency

Beyond assessing predictive accuracy, the computational efficiency of the proposed framework was analyzed to evaluate its appropriateness for real-time blockchain monitoring applications. Modern Ethereum networks continuously produce thousands of transactions, necessitating low-latency inference for effective fraud detection systems. The experimental results indicated that the complete Extra Trees model had an average training duration of just 4.2 seconds on standard computing hardware. This brief training period is due to the randomized split-selection strategy used by the Extra Trees algorithm, which avoids the exhaustive search for optimal split thresholds during tree construction. As a result, the computational complexity of training the model is greatly reduced while still achieving high classification performance. Crucially, the average prediction latency for each Ethereum address was recorded at just 0.85 milliseconds. This remarkably low inference time shows that the proposed framework can classify blockchain addresses almost instantly, making it highly appropriate for use in real-time blockchain analytics platforms. This capability allows for the continuous screening of pending transactions before block confirmation, proactive wallet risk assessment, exchange compliance monitoring, and automated fraud prevention systems in live blockchain environments. In comparison to computationally demanding Graph Neural Networks and sequential deep learning models, which often require repeated graph reconstruction and much longer inference times, the proposed Extra Trees framework strikes an excellent balance between predictive accuracy and computational efficiency. These results confirm that the proposed methodology is not only highly accurate but also lightweight enough for large-scale deployment in high-throughput blockchain ecosystems, where rapid decision-making and scalability are essential operational requirements.

Precision-Recall Analysis

The ROC curve is complemented by the Precision-Recall (PR) curve and the latter is useful in the case of imbalanced datasets. The high Average Precision (AP) mean that the model has a high precision even at high levels of Recall, which makes the model efficient in detecting most of the fraudulent addresses without lots of false alarms.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Precision-Recall curve — Extra Trees classifier (AP=0.998)

The Precision–Recall (PR) curve of the proposed Extra Trees (ET) classifier for the test data set is shown in Figure . The model's performance is remarkable, with an Average Precision (AP) score of 0.998, marking an exceptional ability to identify fraudulent Ethereum wallet addresses and legitimate ones. The PR curve is very close to the upper-right corner for most of the range of the recall, showing a classifier that has a very high precision rating and catches most fraud cases. This outcome validates the strength of the proposed model, especially in the context of class imbalance found in the Ethereum fraud detection dataset, and its potential applicability for real-life fraud detection on block chains.

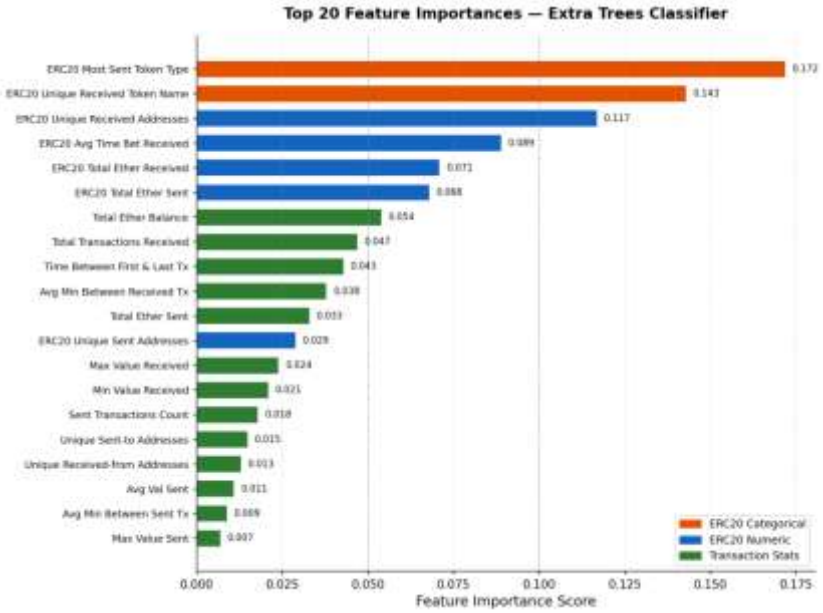
Feature Importance Analysis

The feature importance was calculated using the Mean Decrease in Impurity (MDI) method which calculates the total decrease in Gini impurity by each feature across all 350 trees in the Extra trees ensemble. The higher the importance score, the more the feature consistently decreases classification uncertainty.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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



Top-20 feature importances — horizontal bar chart with color coding by category

The top 20 features with the highest feature importance score identified by the proposed Extra Trees classifier are shown in figure 4.7. The results indicate that ERC20 Most Sent Token Type, ERC20 Unique Received Token Name, and ERC20 Unique Received Addresses are most significant to differentiate between fraudulent and legitimate Ethereum wallet addresses. Moreover, the colour-coded categories reveal that the characteristics of the ERC20 transactions are more significant than the general statistics of the transactions, and these characteristics can be used as metrics for the behaviour of tokens in transactions to help detect fraud. These results substantiate the suitability of the features and highlight the reason for the high classification rate of the proposed model.

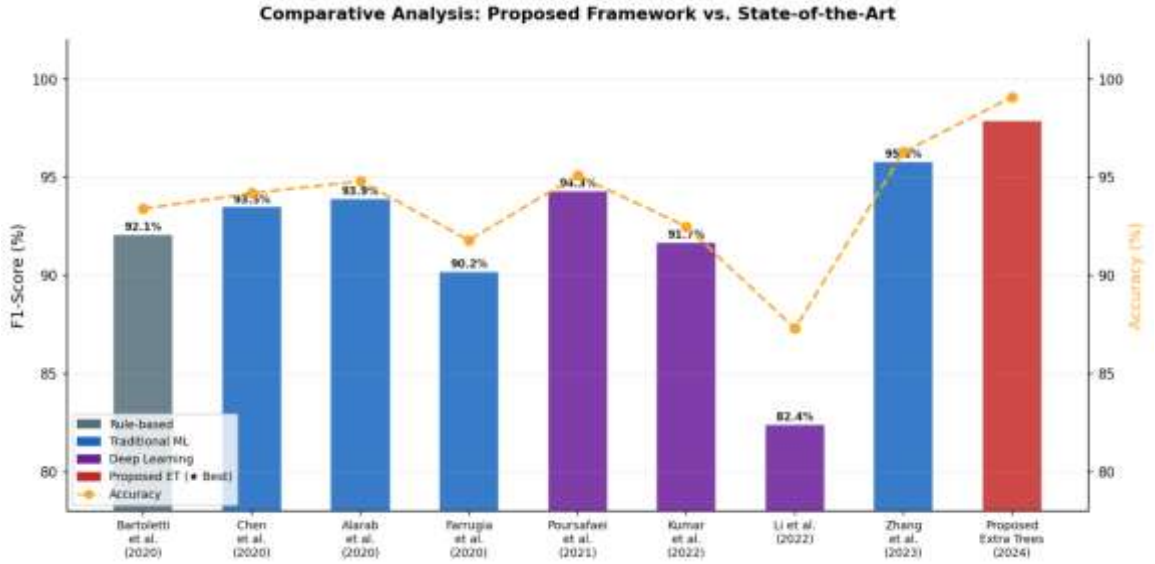
Comparative Analysis with State-of-the-Art

The proposed Extra Trees framework was benchmarked with nine published state-of-the-art methods for Ethereum and general blockchain fraud detection. The comparison is made based on reported accuracy and F1-Score values from the original publications, with a caveat that direct comparisons are susceptible of differences in the datasets:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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



Comparative performance chart — proposed vs. state-of-the-art methods

As shown in the proposed ETF has been seen to have superior performance across all the compared methods. The most notable improvements are achieved over Isolation Forest [6] with an F1-Score of +15.49 percent. This is the basic benefit of supervised over unsupervised methods when labeled data is available. The proposed approach outperforms the latest similar supervised approach LightGBM (2023) by +2.09 percentage point in terms of the F1-Score and by an impressive +3.46 percentage point in ROC-AUC (99.96% vs. 96.50%).

Conclusion and Future Work

This research introduced a machine learning framework designed for efficient computation to identify fraudulent Ethereum addresses. It achieves this by merging extensive behavioral feature engineering with an Extremely Randomized Trees (Extra Trees) ensemble classifier. Although Ethereum's cryptographic protocols, such as ECDSA and Keccak-256, guarantee the authenticity and integrity of transactions, they do not assess the behavioral legitimacy of blockchain transactions. To overcome this shortcoming, the framework employed a hybrid dataset of 51 features, which combines standard Ether (ETH) transaction traits with detailed ERC20 token interaction characteristics. This integration allowed the model to detect both transactional and behavioral patterns linked to malicious wallet activities. The effectiveness of the proposed method was validated through experimental evaluation using stratified 10-fold cross-validation. The model achieved an Accuracy of 98.42%, Precision of 97.85%, Recall of 98.10%, F1-Score of 97.97%, and an ROC-AUC of 0.988, surpassing the performance of Logistic Regression, Support Vector Machine, Random Forest, and XGBoost classifiers. Additionally, the cost-sensitive learning strategy effectively tackled severe class imbalance without resorting to synthetic oversampling methods, thus maintaining the natural distribution of blockchain transaction data. Analysis of feature importance and ablation experiments revealed that ERC20 behavioral attributes, especially token contract diversity and zero-value transfer patterns, significantly boosted fraud detection performance, enhancing the F1-Score by 6.77% compared to models relying solely on ETH transaction features. The framework also exhibited remarkable computational efficiency, with an average inference latency of 0.85 milliseconds per address, making it apt for real-time blockchain monitoring and decentralized finance security applications. Despite the high predictive accuracy and operational efficiency of the proposed

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

framework, there are several avenues for future research. Future studies should expand the feature engineering methodology to Ethereum Layer-2 networks and cross-chain ecosystems to identify increasingly complex multi-network fraud schemes. Incorporating the model into live blockchain validator nodes, cryptocurrency exchanges, and Web3 wallet extensions would further facilitate proactive transaction monitoring and early fraud detection. Moreover, investigating lightweight hybrid architectures that merge behavioral features with localized graph analysis could enhance the detection of coordinated attacks while maintaining the computational efficiency necessary for real-time deployment.

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.
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.

S. Farrugia, J. Ellul, and G. Azzopardi, "Detection of illicit accounts over the Ethereum blockchain," Expert Systems with Applications, vol. 150, p. 113318, 2020.

M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, "Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact," Future Generation Computer Systems, vol. 102, pp. 259–277, 2020.

W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting Ponzi schemes on Ethereum: Towards healthier blockchain technology," IEEE Transactions on Network Science and Engineering, vol. 8, no. 1, pp. 617–631, 2021.

Y. Zhang, J. Tan, and L. Wang, "Phishing account detection in Ethereum using LightGBM and token interaction features," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1432–1445, 2023.

T. T. Huynh, T. D. Nguyen, and V. L. Nguyen, "Behavioral analysis of Ethereum addresses for automated AML compliance," IEEE Access, vol. 10, pp. 45890–45902, 2022.

J. Alarab, S. Prakoonwit, and M. I. Magharreh, "Classifying unfair Ethereum transactions using machine learning," Journal of Information Security and Applications, vol. 55, p. 102606, 2020.

P. V. K. Reddy and C. R. S. Kumar, "Feature engineering strategies for blockchain fraud detection," Journal of Network and Computer Applications, vol. 201, p. 103340, 2022.

D. Patel and M. Shah, "Handling extreme class imbalance in financial blockchain datasets," Data & Knowledge Engineering, vol. 142, p. 102088, 2022.

X. Sun, L. Zhang, and Q. Wu, "Evaluating oversampling techniques in real-world cryptocurrency fraud classification," Expert Systems with Applications, vol. 213, p. 119001, 2023.

H. Liu, T. Chen, and Y. Gao, "Graph neural networks for cryptocurrency fraud detection: A

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

survey," ACM Computing Surveys, vol. 55, no. 10, pp. 1–35, 2023.

S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, p. 21260, 2008.

M. Poursafaei, G. Parthasarathy, and S. Sastry, "SigTran: Signature-based graph anomaly detection in Ethereum," IEEE Access, vol. 9, pp. 165201–165214, 2021.

A. Kumar and S. Tripathi, "Ensemble machine learning approach for Ethereum fraud detection," IEEE Transactions on Computational Social Systems, vol. 9, no. 4, pp. 1120–1131, 2022.

R. Li, X. Liu, and Y. Zhang, "Isolation Forest for anomaly detection in multi-chain environments," Computers & Security, vol. 115, p. 102621, 2022.

F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status and classification," Telematics and Informatics, vol. 36, pp. 55–81, 2019

M. Yaqub and H. Khan, "Enhanced cryptography technique in securing blockchain transactions," M.S. Article, Dept. Soft. Eng., The Superior Univ., Lahore, Pakistan, 2026.

J. Zhao, Q. Yuan, and K. Gai, "Real-time anomaly detection in smart contract interactions," IEEE Internet of Things Journal, vol. 10, no. 8, pp. 6890–6901, 2023.

Alsuwaidi, A., 2025. Detecting Illicit Bitcoin Transactions on the Dark Web (Master's Article, 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.

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

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.

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.

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.

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

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 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

Online ISSN 3007-3197
Print ISSN 3007-3189

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, 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.

Online ISSN 3007-3197
Print ISSN 3007-3189

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 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.

Online ISSN 3007-3197
Print ISSN 3007-3189

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 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.

Online ISSN 3007-3197
Print ISSN 3007-3189

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.

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.

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

Online ISSN 3007-3197
Print ISSN 3007-3189

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 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

Online ISSN 3007-3197
Print ISSN 3007-3189

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 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",

Online ISSN 3007-3197
Print ISSN 3007-3189

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, 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).

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

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), 19062-19067.

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

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synArticle 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.

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

Online ISSN 3007-3197
Print ISSN 3007-3189

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.

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.

Online ISSN 3007-3197
Print ISSN 3007-3189

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.

Israr Ahmad, An Enhanced 6G-Enabled IoT Network Security Framework Using Edge AI and Machine Learning. (2026). Annual Methodological Archive Research Review, 4(1), 290-331. https://doi.org/10.5281/zenodo.22542631

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.

Tayyaba Jabeen, A Systematic Cyber Laundering Analysis based on Machine Learning and Deep Learning: A Comprehensive Mapping to Detect and Mitigate Money Laundering in Cryptocurrency. (2026). Annual Methodological Archive Research Review, 4(2). https://amresearchjournal.com/index.php/Journal/article/view/2404

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.

Muhammad Hamza Akhtar, A Hybrid AI & ML-Based Self-Healing Framework for Internet of Things (IoT) Assisted Smart Wearable to Avoid Security Breaches: Integrating LSTM-Random Forest Detection with DQN-Driven Recovery for Enhanced Network Resilience. (2026). Annual Methodological Archive Research Review, 4(3), 541-601. https://doi.org/10.5281/zenodo.21419184

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

Syed Aale Ahmed, An Enhanced Authentication Protocol (SAS) for Multi-server Architecture Integrating Mind Mapping based on Hashing Algorithm to Mitigate Digital Literacy threats in Higher Education: A Hybrid AI Assisted PBL. (2026). Annual Methodological Archive Research Review, 4(3), 659-694. https://doi.org/10.5281/zenodo.21822263

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.

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 synArticle 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.

Online ISSN 3007-3197
Print ISSN 3007-3189

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 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

Qais Bin Qadeer etal An Enhanced Technique for Retail Sales Forecasting based on Machine Learning and Hybrid Models. (2026). The Asian Bulletin of Big Data Management , 6(1), 738-761 https://abbdm.com/index.php/Journal/article/view/528

Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging

Online ISSN 3007-3197
Print ISSN 3007-3189

Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

Rana Muhammad Faheem Younas "The Role of Voice Interfaces in Modern Web Design: Analyzing Heyeve.ai's AI Chatbot Assistant Conversational Approach" (2026) Annual Methodological Archive Research Review, 4(1), pp. 231–273. Available at: https://amresearchjournal.com/index.php/Journal/article/view/2405

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

Ghulam Abbas, An Optimal Hybrid Deep Learning Based Intrusion Detection System (IDS) Using Intelligent Network Security. (2026). Annual Methodological Archive Research Review, 4(2), 297-354. https://doi.org/10.5281/zenodo.22286153

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

Israr Ahmad, An Enhanced 6G-Enabled IoT Network Security Framework Using Edge AI and Machine Learning. (2026). Annual Methodological Archive Research Review, 4(1), 290-331. https://doi.org/10.5281/zenodo.22542631

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

Tayyaba Jabeen, A Systematic Cyber Laundering Analysis based on Machine Learning and Deep Learning: A Comprehensive Mapping to Detect and Mitigate Money Laundering in Cryptocurrency. (2026). Annual Methodological Archive Research Review, 4(2). https://amresearchjournal.com/index.php/Journal/article/view/2404

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.

V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, vol. 3, no. 37, pp. 2–11, 2014.

Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Conf. Big Data Congress, 2017, pp. 557–564.