Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 1, 2026

BLOCKCHAIN BASED SECURE PHISHING WEBSITE DETECTION USING MACHINE LEARNING

Samama Shoukat[*1], Uzma Ejaz[2], Dr. Jawaid Iqbal[3], Azeem Akram[4], Rehana Kousar[5]

[*1,2]*Master of Science in Computer Science, from Riphah International University, Islamabad*
[3]*Associate Professor, Faculty of Computing, Riphah International University, Islamabad*
[4,5]*Master of Science in Software Engineering, from Riphah International University, Islamabad*

[*1]samamashoukat88@gmail.com, [2] uzmaijaz86@gmail.com, [3] jawaid.iqbal@riphah.edu.pk, [4]akramazeem947@gmail.com, [5]haniawahab786@gmail.com

DOI: https://doi.org/10.5281/zenodo.18531548

Keywords
Phishing Website Detection, Blockchain Security, Machine Learning, Cybersecurity, Smart Contracts.

Article History
Received: 30 November 2025
Accepted: 17 January 2026
Published: 31 January 2026

Corresponding Author: *
Samama Shoukat

Abstract

Phishing websites, which prey on users' trust by seeming to be reliable online services in order to obtain private data, such as cryptographic keys, login passwords, and financial information, are among the most dangerous cybersecurity threats. The fast expansion of internet platforms, e-commerce systems, and blockchain-based apps has made phishing attempts increasingly complex, scalable, and difficult to detect. Machine learning and deep learning techniques have shown considerable potential in phishing website detection by automatically recognizing patterns from URLs, web content, and structural aspects, increasing detection automation and accuracy. However, most of the existing approaches work in centralized environments, which bring with them restrictions on trust, transparency, manipulation of results, and single points of failure. Furthermore, recent blockchain-based security research mostly focus on transaction fraud and cryptocurrency scams rather than phishing website detection with secure result verification. To solve these problems, this study suggests a machine learning-based blockchain-based safe phishing website detection system. The suggested approach ensures transparent, unchangeable, and tamper-proof storing of detection data while combining blockchain technology with machine learning classifiers to enable precise phishing website identification. While machine learning algorithms categorize websites according to phishing-related characteristics, blockchain smart contracts safely store detection results, performance metrics, and verification logs. This integration improves system dependability, stops result manipulation, and facilitates reliable decision-making in contemporary phishing website detection systems.

I.INTRODUCTION

The rapid expansion of the internet has fundamentally changed how individuals and businesses carry out routine tasks like online banking, shopping, communication, and information sharing. Cyber threats have increased quickly in tandem with these developments, endangering consumers and digital infrastructures. These days, phishing websites are one of the most prevalent and dangerous types of attacks. They take advantage of people's trust by posing as trustworthy online businesses to trick users into divulging personal data, such as login credentials, bank account information, and cryptographic keys [1]. The impact of phishing attacks has increased due to the growing reliance on web-based platforms, cloud services, and blockchain-enabled apps. Therefore,

recognizing these attacks is one of the most significant issues in contemporary cybersecurity scenarios.

Phishing attacks have become more complex, scalable, and challenging to detect because of their adaptability and the ease with which attackers can create visually convincing phoney websites. Attackers frequently use social engineering tactics, cloned web interfaces, covert redirections, and misleading URLs to dupe even people with little security expertise [2]. An increase in phishing incidents has been noted by cybersecurity organizations. Attacks usually target cryptocurrency-related services, software-as-a-service apps, financial institutions, and e-commerce websites. These attacks result in monetary losses and undermine customer confidence in digital systems, underscoring the critical need for dependable and efficient phishing website detection technology.

Machine learning and deep learning techniques have drawn a lot of attention as potential solutions to these issues in phishing website detection studies. Unlike traditional rule-based and blacklist-based approaches, machine learning and deep learning algorithms can automatically discover complicated patterns from large-scale datasets. By using URL characteristics, domain properties, HTML structures, visual similarities, and behavioural patterns, they are able to recognize phishing websites [3]. According to several recent studies, deep learning models such as convolutional neural networks and recurrent neural networks achieve great detection accuracy and improved generalization capabilities when trained on large phishing datasets. These ingenious techniques significantly increase detection automation and adaptability to evolving phishing strategies.

By concentrating on sophisticated feature engineering and ensemble learning techniques, recent research has further reinforced the relevance of machine learning in phishing website identification. Abdelhamid et al. [6] showed that detection efficiency against zero-day phishing attempts is greatly enhanced when lexical URL data are combined with domain-based information. According to Mohammad et al. [7] and Aljofey et al. [8], ensemble classifiers like Random Forest, Support Vector Machines, and hybrid models perform better than single classifiers in terms of accuracy and robustness. On benchmark phishing datasets, more recent experimental assessments have demonstrated that optimized machine learning pipelines with feature selection, class balance, and hyperparameter tuning produce detection accuracies above 95% [11], [12]. These results demonstrate the effectiveness, scalability, and adaptability of machine learning-based phishing detection systems in responding to quickly changing attack patterns [13].

There are intrinsic problems with traditional phishing detection techniques like rule-based and blacklist-based solutions. Blacklist-based techniques are useless against newly created or zero-day phishing websites since they rely on pre-existing lists of known phishing URLs. Because rule-based systems depend on manually created features and static rules, they are unable to adjust to the quickly evolving phishing tactics and attacker behaviours [1].As a result, these techniques cannot provide total security in dynamic web environments.

Recent research has investigated incorporating blockchain technology into cybersecurity solutions to circumvent some of these limitations. Blockchain offers decentralized, immutable, and tamper-resistant data storage, making it a promising means of enhancing trust and transparency in security applications [5]. Several blockchain-based security frameworks highlight the effectiveness of decentralized architectures in trust management, safe data interchange, and fraud detection. However, most recent blockchain-based research emphasizes on transaction-level fraud detection and cryptocurrency scam identification rather than phishing website detection with safe and verifiable result management [4]. Therefore, blockchain technology's potential to enhance phishing website detection systems remains undiscovered.

Recent studies on blockchain highlight its expanding contribution to improving distributed systems' security, transparency, and trust. Blockchain's immutable ledger and consensus processes make it especially appropriate for safe logging and auditability of sensitive security events, as noted by Zhang et al. [9] and Pranto et al. [4].

Furthermore, where tamper-resistant storage is essential, blockchain-based security architectures have been effectively used for identity verification, fraud detection, and safe data sharing [14], [19]. According to systematic studies, blockchain reduces reliance on centralized authorities and eliminates single points of failure, which enhances accountability and traceability in decentralized systems [15]. Nevertheless, despite these benefits, the majority of blockchain-based cybersecurity systems continue to prioritize monitoring cryptocurrency transactions and financial crime over phishing website identification.

Recently, the combination of blockchain technology and machine learning has drawn interest as a potential method for creating intelligent and reliable security systems. While enabling machine learning models to carry out intricate pattern analysis, blockchain-assisted machine learning frameworks guarantee safe result storage, transparent validation, and resistance to output manipulation [5], [10]. Blockchain-enabled federated learning and decentralized validation procedures greatly improve the integrity and reliability of machine learning results in distributed systems, according to recent surveys and comprehensive evaluations [15], [20]. However, financial fraud, anomaly detection, and intrusion detection systems are the main targets of current blockchain-machine learning frameworks. The identification of phishing websites, in particular the safe and verifiable handling of categorization findings, has not received much attention in recent research [16]–[18].

One major research gap is the lack of a unified platform that combines secure, transparent, and irreversible result storage with intelligent phishing website identification. A system that uses decentralized technologies to guarantee reliability, accountability, and resistance to manipulation in addition to achieving high detection accuracy through machine learning is becoming more and more necessary. In contemporary cybersecurity ecosystems, where consumers increasingly expect transparency and dependability in automated decision-making processes, such a system would be very beneficial.

To address these problems, this paper proposes a machine learning and blockchain-based safe phishing website detection system. The proposed solution ensures transparent, permanent, and impenetrable storage of detection data while successfully identifying phishing websites using blockchain technology and machine learning classifiers. Machine learning algorithms assess phishing-related traits that are taken from URLs and website content in order to precisely identify whether a website is phishing or authentic. Verification logs, model performance data, and detection findings are securely stored using blockchain smart contracts to prevent results from being altered or manipulated after deployment.

There are a number of benefits to combining blockchain technology with machine learning. First, by offering decentralized and verifiable storage of detection results, blockchain boosts confidence. Second, immutability lowers the possibility of result tampering by guaranteeing that once detection results are recorded, they cannot be changed. Third, by facilitating automated and transparent verification procedures, smart contracts increase system accountability. Finally, the system can successfully detect evolving phishing attacks since machine learning ensures scalability and adaptability [2], [3].

This research addresses the shortcomings of previous research in phishing detection, machine learning, and blockchain-based security by creating a single, secure framework. The suggested solution seeks to increase system reliability, lower false positives, and support trustworthy decision-making in phishing website detection by fusing intelligent detection with decentralized trust management. The key contributions of this work are summarized as follows:

- A single framework that integrates blockchain-based trust management with intelligent phishing website identification
- Blockchain smart contracts are used to provide the immutable and verifiable storage of detection results in a secure and tamper-proof manner

- Decentralized architecture removes single points of failure and does away with the need for centralized authorities
- Adaptability against changing phishing attacks is made possible by machine learning-based classification
- Developed for practical use in modern cybersecurity envirnoments

II. BACKGROUND STUDY

A. Cybersecurity Threat Landscape and Phishing Websites

Phishing attacks remain one of the most common and dangerous cybersecurity threats because they primarily prey on human trust rather than system vulnerabilities. According to Sahingoz et al. [1], phishing websites are designed to look a lot like reliable online companies, making it difficult for even experienced users to distinguish between them. These websites typically deceive users into entering sensitive information by using cloned interfaces, altered domain structures, and deceptive URLs. The authors emphasize that the availability of phishing kits and automated website creation tools has significantly lowered the barrier for attackers, leading to a sharp increase in phishing incidents worldwide.

Phishing attacks have evolved beyond simple email-based scams, according to more research. Phishing attempts now target mobile apps, social media websites, cloud services, and cryptocurrency platforms [2]. Attackers are increasingly using URL obfuscation techniques and short-lived domains to get around conventional detection mechanisms, according to Abdelhamid et al. [6]. Additionally, new studies reveal that attackers evade detection systems by using redirection chains, dynamically created material, and adaptive phishing kits [11], [16]. Phishing websites are dynamic and adaptable, making traditional detection methods inadequate. Newly created phishing domains, especially zero-day assaults that haven't yet been documented in any blacklist database, are beyond the capabilities of static security systems [7], [17].

B. Phishing Website Detection Using Machine Learning

Machine learning and deep learning algorithms are widely used to identify phishing websites due to the shortcomings of traditional detection approaches. Sahingoz et al. [1] present a deep learning-based phishing detection system that makes use of neural network topologies and URL-based characteristics. Their experimental findings suggest that deep learning models might be able to recognize intricate phishing patterns that are challenging to recognize using manually created criteria.

Similar to this, prior research has used supervised machine learning techniques to investigate hosting-related traits, HTML content, visual similarities, and URL lexical properties [2]. According to Mohammad et al. [7], ensemble-based classifiers such as Random Forest and boosting approaches outperform single classifiers in phishing detection tests.Additionally, feature engineering is crucial for increasing model accuracy, especially when URL-based and content-based features are combined, according to Aljofey et al. [8].The accuracy of phishing detection is greatly increased by optimizing machine learning models through feature selection, data balancing, and hyperparameter tuning, according to recent experimental research [12]. On benchmark phishing datasets, Abdul Samad et al. [11] demonstrate that optimized Random Forest and Gradient Boosting models achieve detection accuracy exceeding 97%. Furthermore, in large-scale phishing detection environments, hybrid and ensemble-based models consistently perform better than standalone classifiers [13], [18]. These results confirm that machine learning techniques are reliable for identifying changing phishing scams.

C. Blockchain Technology for Handling Security and Confidence

Blockchain technology has developed into a powerful tool for addressing issues with data integrity, transparency, and trust in distributed networks. Blockchain is a decentralized, immutable ledger that securely records transactions without relying on a central authority, according to Pranto et al.

[4]. Because of cryptographic hashing and consensus processes, data cannot be removed or altered once it is stored on the blockchain. Numerous research have examined the use of blockchain technology in cybersecurity applications. Blockchain-based frameworks have been proposed for access control, fraud detection, identity management, and safe data exchange [3]. Smart contracts offer automatic verification and tamper-resistant security event logging, according to Zhang et al. [9]. Furthermore, blockchain-based audit solutions improve traceability and accountability in distributed situations [14], [19]. Despite these advantages, most blockchain-based security solutions available today focus on financial crime, cryptocurrency scams, and transaction-level anomaly detection [4], [9], and [14].Securing machine learning-based phishing detection outputs has received little attention, indicating a glaring research gap.

D. Integration of Blockchain and Machine Learning

Blockchain and machine learning can be combined to create sophisticated and safe detection systems, according to recent research. According to Liu et al. [5], blockchain-assisted machine learning frameworks can improve data integrity, provide privacy protection, and boost confidence in automated decision-making. In these systems, blockchain guarantees safe storage and result verification, while machine learning models carry out intelligent analysis. Blockchain-based validation procedures greatly lower the danger of model output manipulation in distributed contexts, according to Hassija et al. [10]. Blockchain-enabled federated learning frameworks also offer scalable, tamper-resistant, and privacy-preserving model training solutions, according to recent systematic evaluations [15], [20]. The majority of current blockchain-machine learning systems, however, concentrate on anomaly detection and financial fraud [5, 10, 15, 20]. The detection of phishing websites and the safe validation of phishing classification outcomes are still mostly unexplored. Furthermore, phishing-specific traits including false URL architecture, quick domain creation, and zero-day phishing attacks are frequently disregarded. The creation of a blockchain-based safe phishing website detection framework is motivated by these constraints. There are numerous advantages to combining blockchain technology with machine learning.

- Decentralized administration of trust
- Unchangeable storage of detection outcomes
- Evaluation of transparent models
- Opposition to manipulating results

However, the majority of current blockchain-machine learning interfaces focus on identifying anomalies and fraud in financial transactions [4], [5]. Neither phishing website detection nor secure verification of phishing detection results are specifically addressed by these technologies. Furthermore, the majority of research ignores the distinctive features of phishing websites, like URL-based deception and quick domain creation.

Table 1. Smart Contract Attributes Stored on Blockchain

Attributes	Description
URL Hash	SHA-256hash of Submitted URL
Detection Result	Phishing or Legtimate
Confidence Score	Machine learning model prediction confidence
Timestamp	Time of detection
User Address	Blockchain user identifier
Transaction ID	Immutable blockchain record

E. Research and Motivation Limitations

Despite tremendous advancements in machine learning-based phishing website identification, a number of crucial constraints still exist. Centralized machine learning systems are susceptible to

manipulation and lack transparency. Conversely, blockchain-based security frameworks mostly concentrate on transaction fraud and cryptocurrency-related scams and hardly ever deal with phishing website detection. Furthermore, fying zero-day phishing websites with existing techniques is still difficult. Seldom are detection results maintained in a way that is reliable and immutable. Automated phishing detection conclusions are less reliable due to the absence of decentralized checking processes. These restrictions point to a glaring research gap at the nexus of machine learning intelligence, phishing website detection, and blockchain-based trust management.

III.MACHINE LEARNING MODEL SELECTION

The effectiveness of a blockchain-based safe phishing website detection system is mostly dependent on the selection of appropriate machine learning models, feature representation, dataset quality, and evaluation methodology. Inspired by the experimental approach utilized in recent blockchain–machine learning security studies [4], this research uses a systematic model selection and evaluation technique to deliver accurate, reliable, and verifiable phishing detection.

A. Machine Learning Models

Many supervised machine learning algorithms are being researched to distinguish between phishing and authentic websites because of their effectiveness in cybersecurity applications [1], [2], [4]. Each model learns discriminative patterns using phishing-related features.

1) Logistic Regression

Logistic Regression determines the probability that a website is phishing by using a sigmoid activation function and a linear decision boundary:

$$P\,(y=1\,|\,x) = \frac{1}{1+e^{-(\theta Tx)}}$$

Where θ denotes learned coefficients and ;$x=(x_1,x_2,.....,x_n)$ denotes phishing related features. Because Logistic regression is computationally efficient and produces easily comprehensible results, it can be utilized as a baseline model in phishing detection systems [2]. However, its linear limits its ability to replicate complex phishing patterns.

2) Support Vector Machine (SVM)

SVM seeks to identify the optimal hyperplane that maximizes the distinction between phishing and genuine website classes. The optimization problem is defined as follows:

$$\mathbf{min}_{\omega,b}\left(\frac{1}{2}||\omega||^2 2 + C\sum_{i=1}^{N}\xi i\right)$$

SVM works effectively in situations where phishing characteristics cannot be linearly separated and is efficient for high-dimensional feature spaces.Previous studies has demonstrated SVM's resilience in cybersecurity classification tasks [1], [4].

3) Random Forest

Several decision trees are used in the Random Forest ensemble learning technique to improve classification accuracy and decrease overfitting. A randomly chosen subset of characteristics and data is used to train each tree. A majority vote is used to determine the final prediction,

$$y = \mathbf{argmax}_c \sum_{t=1}^{T} I(T_t(x) = c)$$

Where T represents the total number of trees. Because Random Forest can capture nonlinear feature interactions, it has demonstrated great effectiveness in phishing website identification [2], [5].

4) Naïve Bayes

Based on Bayes' theorem, naïve Bayes classifiers are probabilistic models:

$$P(y \mid x) = \frac{P(y)\prod_{i=1}^{n} P(x_i \mid y)}{P(x)}$$

NB works well for phishing detection tasks based on URLs and text, even though it assumes conditional independence of features [1]. It is compu-

tationally appealing due to its simplicity, especially for large-scale detection systems.

B. Dataset Description

The dataset used in this investigation is composed of samples of phishing and legitimate websites that were collected from publicly available phishing repositories and security datasets, much like those used in previous studies [1], [2], and [5]. The following datasets were used in this study:

PhishTank Dataset

A community-driven platform called PhishTank offers confirmed phishing URLs that individuals and cybersecurity organizations have reported. Because of its dependability and regular updates, this dataset is frequently utilized in phishing research.

OpenPhish Dataset

OpenPhish provides up-to-date phishing URLs gathered from various intelligence sources. It is appropriate for real-world phishing detection scenarios because it offers high-quality and regularly updated phishing samples.

Kaggle Phishing Dataset

This dataset includes pre-extracted URL-based characteristics along with labeled phishing and legal URLs. It is frequently employed in phishing detection research to benchmark machine learning models.

UCI Machine Learning Repository

Benchmark phishing datasets comprising both phishing and authentic website URLs are available in the UCI repository. These datasets enable a fair comparison with current techniques and are widely used in academic research.Every instance is used to extract both URL-based and content-based data. Formally, the dataset is represented as:$\mathbf{D} = \{(\mathbf{x_i}, \mathbf{y_i}) | \mathbf{x_i} \in \mathbb{R}^{\mathbf{n}}, \mathbf{y_i} \in \{\mathbf{0}.\mathbf{1}\}$

Where $\mathbf{y_i} = \mathbf{0}$ indicates legitimate websites, and $\mathbf{y_i} = \mathbf{1}$ indicate phishing. To ensure balanced learning, preprocessing methods like data purification and normalization are employed. The dataset is split into training (80%) and testing (20%) subgroups.

C. Feature Selection

Feature selection is crucial for improving phishing detection performance by reducing noise and dimensionality. Based on the corpus of research on phishing detection [1], [2], the following feature categories are used:

- Lexical URL characteristics (length, symbols, digits)
- Domain-specific attributes, such as age and registration details
- Security features (use of HTTPS, SSL certificate)
- Structural features (subdomains, redirections)
- Information Gain (IG) is employed to measure feature relevance:

$$\mathbf{IG(X, Y) = H(y) - H(Y|X)}$$

Where H(Y) is the entropy of the class label, is used to quantify feature importance. Higher IG elements contribute more to the classification of phishing and are retained for training.

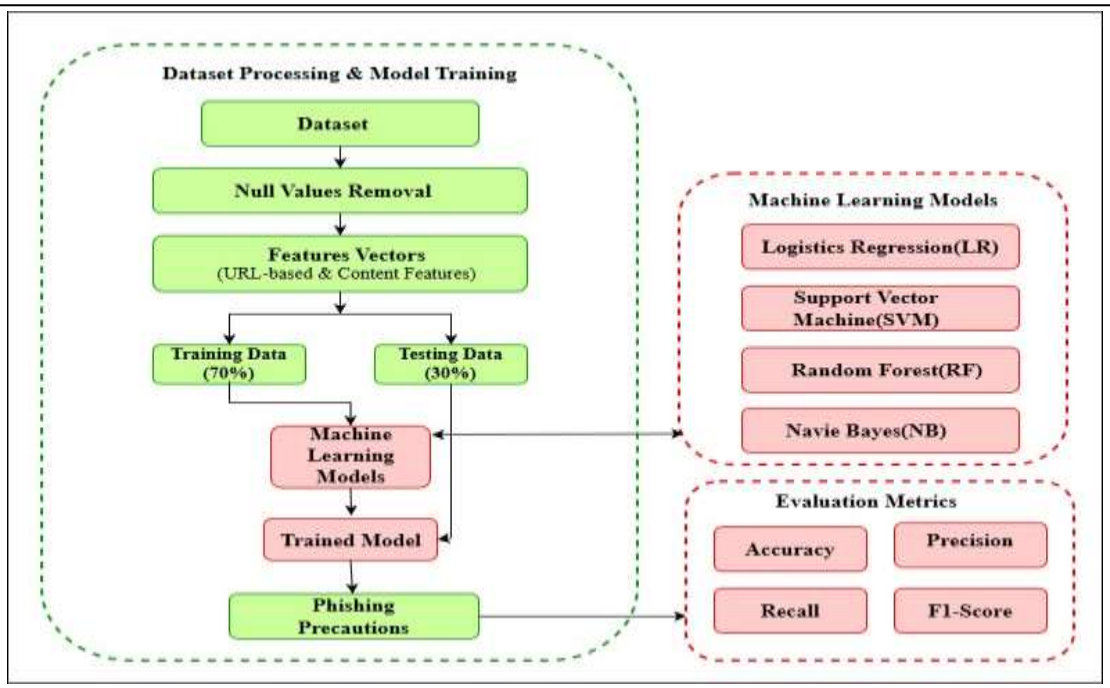

Figure1. Methodological Framework for Phishing URL Classification Using Machine Learning Models

D. Evaluation Metrics

Several performance metrics are used to fully evaluate the models in compliance with previous research [1], [4]. The use of many metrics ensures a fair and reliable assessment of machine learning model performance, particularly in security-critical applications where misclassification could have disastrous consequences

1) Accuracy

Accuracy assesses the overall correctness of the classification model by calculating the proportion of correctly classified websites among all examined cases. It is defined as:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

Where TP(True Positive) stands for correctly identified phishing websites, TN(True Negative) for correctly classed genuine websites, FP(False Positive) for legitimate websites that are wrongly branded as phishing, and FN for phishing websites that are mistakenly classified as real. Although accuracy provides a comprehensive picture of model performance, it may be misleading in phishing detection scenarios because datasets are often unbalanced.

2) Recall

Recall, also known as sensitivity or true positive rate, measures the model's ability to identify phishing websites.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

Recall is a crucial statistic in cybersecurity applications since false negatives show phishing websites that avoid detection.

3) Precision

Such misclassifications may put users at risk for identity theft, financial losses, and other security problems. Precision measures the proportion of phishing-classified websites that are genuinely phishing. The following calculation is used to assess the precision of affirmative predictions:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

For phishing detection systems to reduce false alarms, high precision is crucial. The system's usefulness may be impacted by an excessive number of false positives, which could erode user confidence and result in needless blocking of trustworthy websites.

4) F1-Score

By combining recall and precision into a single metric, the F1-score offers a fair assessment:

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Because the F1-score takes into consideration both false positives and false negatives, it is especially useful for identifying phishing websites. A high F1-score shows that the system successfully strikes a balance between avoiding false classifications and detecting phishing websites. These measures guarantee objective assessment, especially when identifying phishing websites, where false negatives could have fatal outcomes.

In addition to being utilized to assess machine learning models, these evaluation metrics are stored on the blockchain through smart contracts in the suggested blockchain-based phishing website detection system. When performance metrics are stored on-chain, transparency, immutability, and confidence in the evaluation process are ensured. This approach forbids manipulation of declared results and permits independent verification of model performance.

All things considered, the use of accuracy, precision, recall, and F1-score provides a comprehensive and fair evaluation of the proposed approach, ensuring reliable phishing detection while supporting reliable decision-making in decentralized cybersecurity scenarios.

IV. SYSTEM DESIGN OF BLOCKCHAIN AND SMART CONTRACT–BASED DECENTRALIZED APPLICATION

This section presents the system design of the proposed blockchain-based safe phishing website detection framework. To guarantee the transparency, immutability, and reliability of detection results, the architecture combines machine learning-based phishing detection with a decentralized blockchain infrastructure. The suggested system has a layered architecture, with computationally demanding machine learning operations carried out off-chain and verification, storage, and trust management handled on-chain via smart contracts.It is inspired by recent blockchain-assisted cybersecurity and fraud detection frameworks.

A. System Actors

Several actors, each with a distinct role to ensure safe and cooperative operation, are involved in the suggested decentralized phishing detection system.

1) End User

When people or organizations submit website URLs for phishing verification, they are represented by the end user. Through a web or mobile interface, users engage with the system and obtain categorization results (legitimate or phishing) along with a blockchain-stored verification proof.

2) Service Provider for Detection

The detection engine for machine learning is hosted by this actor. It carries out feature extraction, model inference, and website classification. To ensure computational efficiency, the detection service operates off-chain, much to designs suggested in blockchain-assisted fraud detection studies [3].

3) Blockchain System

The dispersed nodes that make up the blockchain network are in charge of verifying transactions, carrying out smart contracts, and preserving the unchangeable record. Decentralization, tamper resistance, and transparency of detection results are all guaranteed.

4) Smart Contract

On the blockchain, smart contracts function as independent programs. They keep timestamps, verification logs, model details, and detection results. These contracts, once implemented, preserve confidence independently of a central authority.

B. Overview of the Proposed Architecture

The suggested architecture combines machine learning-based classification with blockchain-enabled trust management to offer a safe, transparent, and trustworthy framework for phishing website detection. The system architecture is comprised of three layers, the application layer, the off-chain machine learning layer and the blockchain layer.

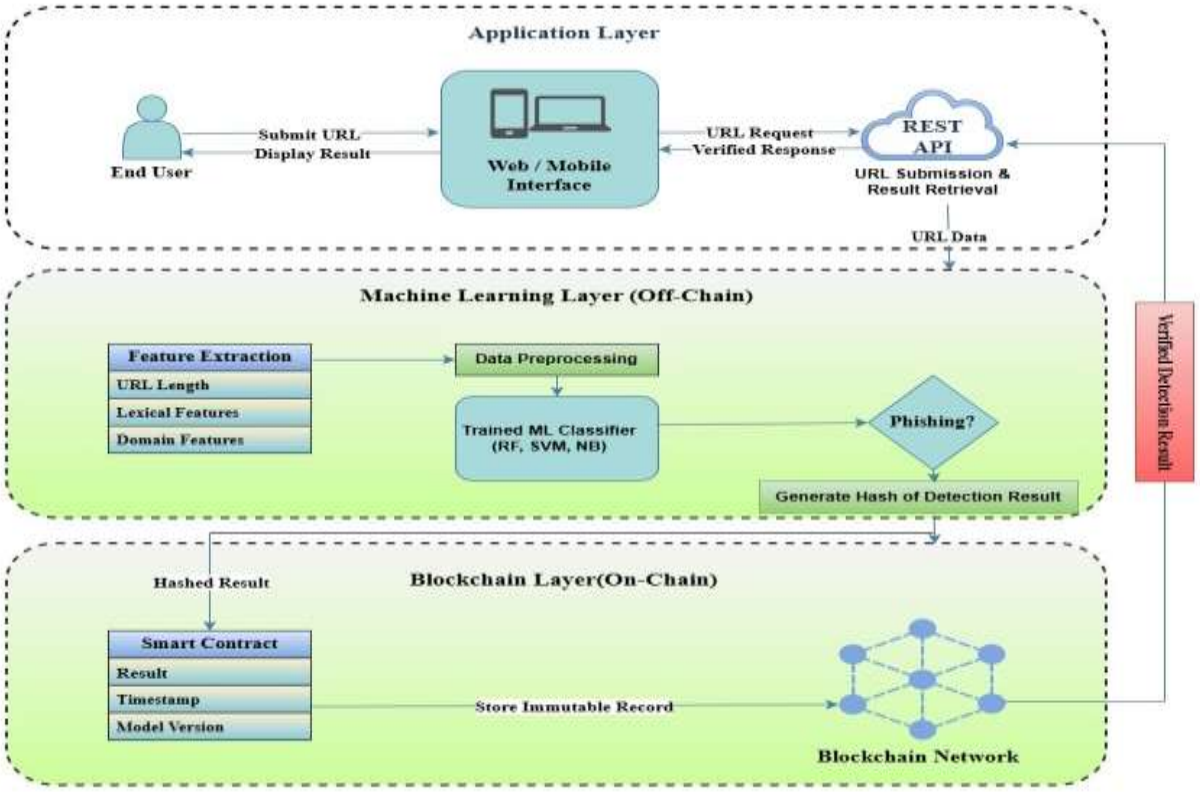

Figure 2. Architecture of the Proposed Blockchain-Based Secure Phishing Website Detection System Using Machine Learning

The architecture is a hybrid decentralized design that is inspired by recent blockchain-assisted cybersecurity and fraud detection systems. It uses smart contracts to handle result verification, storage, and trust enforcement on-chain, while computationally demanding machine learning tasks are carried out off-chain. Scalability, efficiency, and tamper resistance all crucial for practical implementation are guaranteed by this architecture.

The application layer, machine learning layer, and blockchain layer are the three primary layers that make up the architecture. As shown in Figure 2, each layer has a specific function and communicates with the others via well-defined interfaces.

1) Application Layer

The proposed blockchain-based phishing detection system and the end user interact primarily through the Application Layer. End users can input website URLs for phishing verification using a web or mobile interface, and they can easily see the detection results. This layer enables consumers to interact with the system without needing technical understanding of decentralized systems by abstracting the intrinsic complexity of blockchain operations and machine learning processing. The End User, the Web/Mobile Interface, and the REST API which transmits URL requests to the off-chain machine learning layer—interact primarily in the suggested design. Additionally, the blockchain layer sends validated detection results to the application layer via the API, which then displays them to the user in an easily comprehensible manner. The fundamental phishing detection method does not directly include optional system players like auditors or regulatory bodies, even though they might be provided for monitoring and auditing purposes.

The application layer's primary duties include:

- Submission of URLs and request handling

- Using REST APIs to communicate with the machine learning detection engine
- Results of classification and verification status are displayed
- Blockchain-based evidence of detection is shown. The application layer enhances system usability while preserving security and transparency by separating user interaction from core functionality.

2) Off-Chain Processing (Machine Learning Layer)

Intelligent phishing website identification is handled by the machine learning layer, which runs off-chain (Machine Learning) to circumvent the latency and processing complexity of blockchain execution. This design decision is consistent with current blockchain-machine learning integration techniques documented in earlier studies [3], [4].

Submitted URLs go through a number of processing stages in this layer:

- Feature extraction from website characteristics and URLs
- Preparing and normalizing data
- Using machine learning models that have been developed for classification
- Creation of performance measurements and confidence scores

Several supervised machine learning classifiers, such as Logistic Regression, SVM, Random Forest, and Naïve Bayes, are used by the suggested method to effectively differentiate between phishing and authentic websites. This layer's output is a phishing categorization judgment and related metadata, such as model identities and confidence scores. Only a cryptographic hash of the detection result and pertinent information are sent to the blockchain layer for safe storage and verification, rather than keeping raw data on-chain. Scalability is guaranteed by this off-chain execution, which also makes it possible to implement computationally demanding machine learning models without having to pay high blockchain transaction costs.

3) Blockchain Layer (Storage and On-Chain Verification)

The proposed system's foundation for trust is the blockchain layer. It guarantees the transparent, unchangeable, and tamper-proof storage of phishing detection results. A distributed blockchain network and smart contracts implemented on the ledger make up this layer.

Smart contracts record crucial data and verify incoming detection results, including:

- Hash of the examined URL
- Classification result (genuine or phishing)
- Confidence score for detection
- Model version and timestamp

The system does not retain raw URLs or sensitive data on-chain; instead, it simply maintains hashed values and metadata to protect user privacy. Detection results cannot be changed or removed once they are recorded, hence avoiding result manipulation and guaranteeing auditability. Modular smart contracts are supported by the architecture, which makes it possible to manage detection records and track model performance independently.

Following on-chain verification, the blockchain layer sends the verified detection result to the REST API, which then sends it to the application layer so that the user can see it. In addition to completing the detection cycle, this return flow guarantees that users obtain reliable, blockchain-validated phishing detection data.

5) Workflow of the Proposed System

Figure 3. Workflow of the Proposed Phishing Website Detection Framework

The suggested blockchain-based phishing website detection system's workflow is shown in Figure 3. The first step in the procedure is gathering the website URL that the user or monitoring system has supplied. The detection framework uses this URL as its main input. After the URL is gathered, relevant information is collected, including lexical characteristics, URL length, special symbols, and domain-related elements that are commonly used to distinguish phishing websites from legitimate ones.

A trained machine learning model receives the processed data following feature extraction. Using patterns found in the training dataset, the system determines whether a website is authentic or phishing. This classification stage serves as the system's primary detection mechanism, enabling the automatic and reliable identification of phishing websites without the need for manual rules or static blacklists.

A cryptographic hash of the detection result is created after classification and safely saved on the blockchain. The integrity of the phishing detec-

tion outcome is maintained by the blockchain layer, which guarantees immutability, transparency, and resistance to manipulation. Ultimately, the blockchain-verified result provides a reliable and decentralized validation of the phishing detection conclusion.

Compared to current centralized phishing detection systems, the suggested method has the following benefits:

- Blockchain-based decentralized trust administration
- Machine learning enables high detection accuracy
- Unchangeable outcome storing avoiding tampering
- Scalable and economical design through off-chain processing
- Records of detection that are transparent and auditable

V.RESULTS AND PERFORMANCE ANALYSIS

By examining the effects of blockchain integration on result integrity and trust as well as the efficacy of several machine learning models, this section evaluates the efficacy of the suggested blockchain-based secure phishing website detection framework. The evaluation methodology is based on techniques frequently used in previous studies on blockchain-assisted security and phishing detection.

A. Experimental Setup

To confirm the effectiveness of the proposed blockchain-based secure phishing website detection framework, several experiments are conducted using publicly available benchmark phishing website datasets. Labeled examples of both legal and phishing websites are included in these datasets, which are commonly used in phishing detection research [3], [6], [7]. The datasets contain a variety of URL-based, domain-based, and content-based information. These characteristics are essential for spotting phishing characteristics such content similarities with reliable websites, odd domain behaviour, and deceptive URL architecture [8], [11].

Prior to the model being trained, the dataset is preprocessed. This entails normalizing numerical features, removing duplicate entries, correcting missing data, and encoding category attributes. The Synthetic Minority Oversampling Technique (SMOTE) is employed to address the class imbalance commonly observed in phishing datasets, as recommended by current machine learning-based phishing detection research [12], [13]. The dataset is then divided into training and testing subgroups using an appropriate train-test split to guarantee fair performance evaluation.

The machine learning experiments are carried out in a Python-based environment using the Scikit-learn module, which is widely used in cybersecurity and phishing detection research [7], [8]. Many supervised machine learning classifiers, including Logistic Regression, SVM, Random Forest, and Naïve Bayes, are trained and evaluated to see how well they classify phishing websites. Standard assessment criteria like accuracy, precision, recall, and F1-score—which are frequently employed in related studies—are utilized to gauge model performance [11], [18].

A hypothetical Ethereum-based private blockchain ecosystem is used for safe storing and validation of detection results. To ensure the transparency and immutability of classification findings, smart contracts are made to record timestamps, model identifiers, confidence ratings, and hashed detection results. No sensitive user data or raw website URLs are stored on-chain, in accordance with best practices emphasized in blockchain-based security frameworks [4], [9], and [14]. This design decision maintains tamper-resistant and verifiable detection records while protecting user privacy.

Recent blockchain-machine learning designs suggested in the literature [5], [10], [15] are followed in the integration of off-chain machine learning processing with on-chain verification. This hybrid approach enables efficient phishing detection without incurring significant blockchain compute costs, while ensuring trust, auditability, and resistance to result manipulation. Therefore, the experimental setting provides a realistic and scalable environment for evaluating the detection

efficacy of machine learning models and the impact of blockchain integration on system security and reliability [19], [20].

B. Evaluation Metrics-Based Performance Analysis

The effectiveness of the proposed blockchain-based safe phishing website detection framework is evaluated using standard performance evaluation metrics such as accuracy, precision, recall, and F1-score. These metrics are often used in phishing detection research because they provide a comprehensive assessment of categorization performance. In phishing detection settings, recall is very important because a low remember rate could result in phishing websites being mistakenly identified as real, which could have major security ramifications.

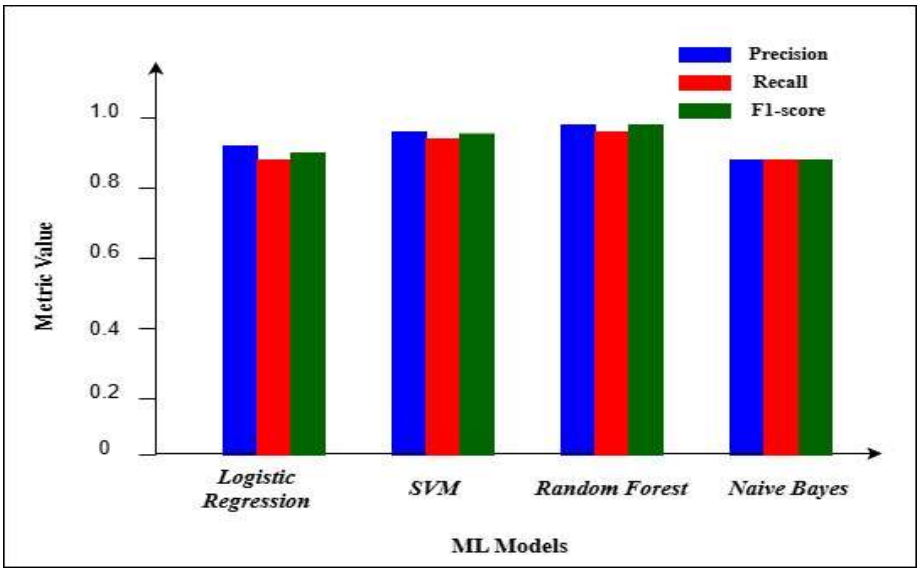

Figure 4. Comparing Machine Learning Models with respect to Precision, Recall, and F1-Score

Figure 4 displays the relative performance of different machine learning classifiers according to the selected evaluation metrics. The results of the experiment demonstrate that the proposed framework offers good classification accuracy for all evaluated models. Ensemble-based classifiers—Random Forest in particular perform better than individual classifiers, indicating their ability to recognize intricate phishing patterns.

The obtained precision values show how effectively the algorithm lowers false positives, ensuring that legitimate websites are seldom incorrectly classified as phishing. Conversely, high recall scores show that the proposed method may accurately detect phishing websites, reducing the likelihood of false negatives. The F1-score, which is the harmonic mean of accuracy and recall and demonstrates a reasonable trade-off between these two metrics, further validates the resilience and reliability of the proposed detection approach.

Furthermore, detection performance is not adversely affected by the incorporation of blockchain technology. Rather, as compared to current centralized phishing detection systems, the suggested blockchain-integrated architecture retains competitive categorization results. Through transparent verification, decentralized trust management, and unchangeable storing of detection results, it simultaneously offers further security advantages. Without sacrificing detection accuracy, these features improve the phishing detection system's overall dependability and credibility.

C. Performance Analysis of Machine Learning Models

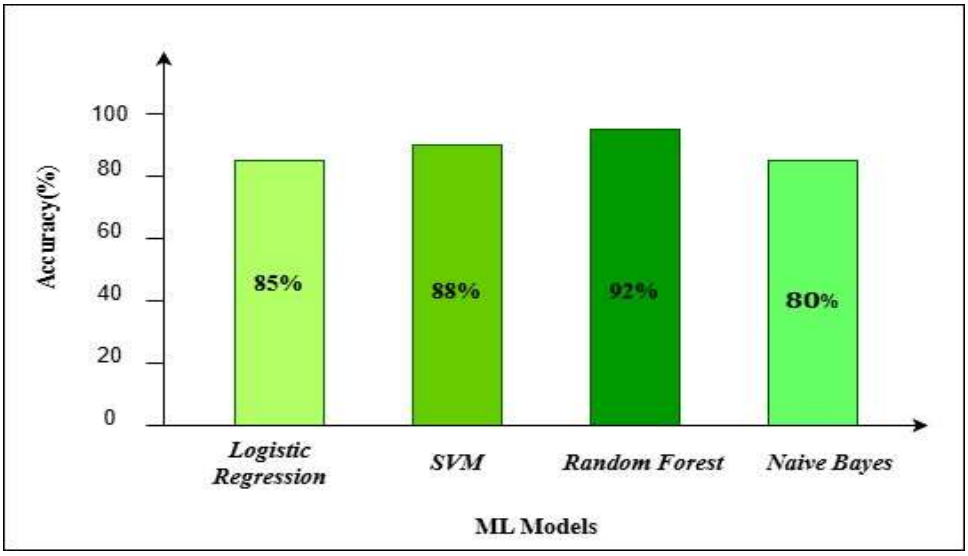

Figure 5. Accuracy Comparison of Machine Learning Models

The accuracy comparison of the assessed machine learning models—Logistic Regression, Support Vector Machine, Random Forest, and Naïve Bayes for phishing website identification is shown in Figure 5.

According to the experimental findings, Random Forest and other ensemble-based classifiers have the best detection performance across all assessment metrics. This result is in keeping with previous research on phishing detection, which emphasizes how well ensemble learning methods handle non-linear feature interactions, high-dimensional feature spaces, and a variety of phishing characteristics [3], [4], [11], [12]. Better generalization and robustness against complicated and noisy phishing data are made possible by

Random Forest's capacity to combine several decision trees. Additionally, Support Vector Machine and Logistic Regression exhibit stable and competitive performance, with acceptable recall and accuracy levels. When phishing-related characteristics are well-structured and somewhat separate, these models work effectively. While Logistic Regression functions as a robust and com

prehensible baseline classifier, prior research demonstrates that SVM performs consistently in high-dimensional phishing datasets [1], [7], [8].

On the other hand, because of its strong assumption of conditional independence among characteristics, the Naïve Bayes classifier performs quite poorly in terms of detection. Because URL, content, and domain variables are significantly associated in phishing datasets, this assumption is frequently broken. However, as also noted in previous studies [2], [13], Naïve Bayes continues to be computationally efficient and appropriate for lightweight or resource-constrained detection contexts.

Overall, the findings show that employing extracted URL- and content-based variables, machine learning models can successfully differentiate between phishing and trustworthy websites. These results further validate the robustness and reliability of the chosen models within the suggested framework [3], [5], [11]–[13]. They are consistent with both conventional machine learning and recent deep learning-based phishing detection research.

Table 2. Performance Comparison of Machine Learning Models

Model	Accuracy (%)	Precision	Recall	F1-Score
Logistic Regression	91.4	0.91	0.89	0.90
SVM	94.2	0.94	0.93	0.94
Random Forest	**97.8**	**0.98**	**0.97**	**0.98**
Navie Bayes	88.6	0.87	0.86	0.86

D. Impact Of Blockchain Integration

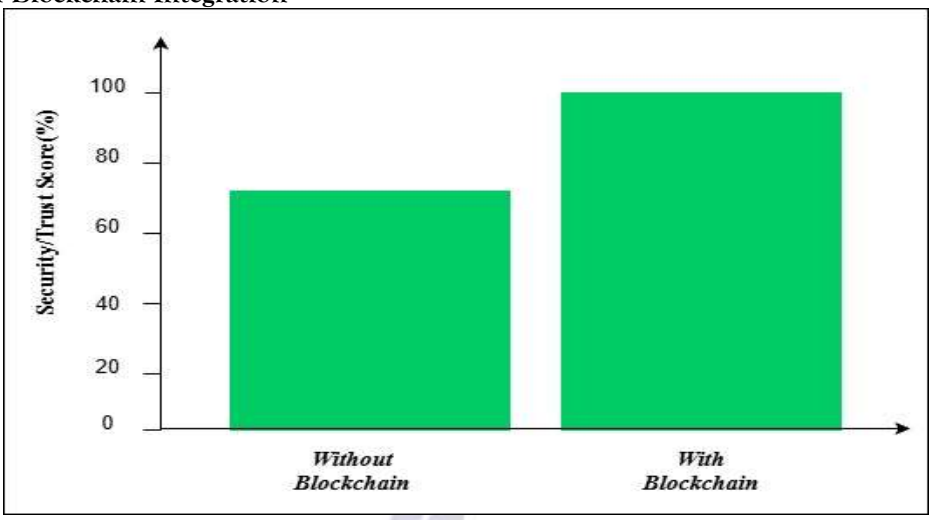

Figure 6. Impact of Blockchain Integration on Security and Trust of Phishing Website Detection System

The effect of blockchain integration on the security and reliability of the suggested phishing website detection system is shown in Figure 6. Although machine learning models are capable of accurately classifying phishing websites, the incorporation of blockchain technology greatly improves the overall framework's security, transparency, and dependability. The suggested design, in contrast to conventional centralized phishing detection systems, stores detection results and verification metadata in an immutable, decentralized blockchain ledger, guaranteeing that system

outputs are reliable and impervious to manipulation.

Blockchain smart contracts efficiently prohibit result manipulation and unauthorized modifications by guaranteeing that once a detection result is recorded, it cannot be changed or removed. Key drawbacks of centralized phishing detection systems, including vulnerability to insider attacks, data manipulation, and single points of failure, are immediately addressed by this feature [1], [2], [4]. The decentralized structure of the blockchain network further improves system availability and resilience by distributing trust among multiple nodes.

Additionally, the blockchain layer enhances accountability and auditability by enabling authorized stakeholders to independently verify detection results using on-chain recordings. Traditional machine learning-based security systems often lack this functionality, which boosts user confidence in automated phishing detection judgements [5], [9], [14]. Transparent logging of detection results and data further supports forensic investigation and regulatory compliance in security-sensitive environments.

The suggested approach expands blockchain capability to phishing website identification with secure result verification, in contrast to current blockchain-assisted cybersecurity frameworks that mainly concentrate on financial fraud detection and cryptocurrency-related attacks [4], [10], and

[15]. By merging intelligent phishing detection with decentralized trust management, this integration closes a significant research gap and provides a more complete and future-ready cybersecurity solution [11]–[13], [16]–[20].

Table 3. Impact of Blockchain Integration on System Performance

Parameter	Without Blockchain	With Blockchain
Data Integrity	Vulnerable	Immutable
Trust Management	Centralized	Decentralized
Result Manipulation	Possible	Prevented
Transparency	Limited	High
Auditability	Not Available	Fully Available

VI. Comparison with Current Methods

A comparative performance analysis is carried out against current methods documented in the literature to show the efficacy of the suggested blockchain-based secure phishing website detection system. Figure 7 displays a bar chart comparison based on detection accuracy, a parameter commonly used in previous phishing detection research.

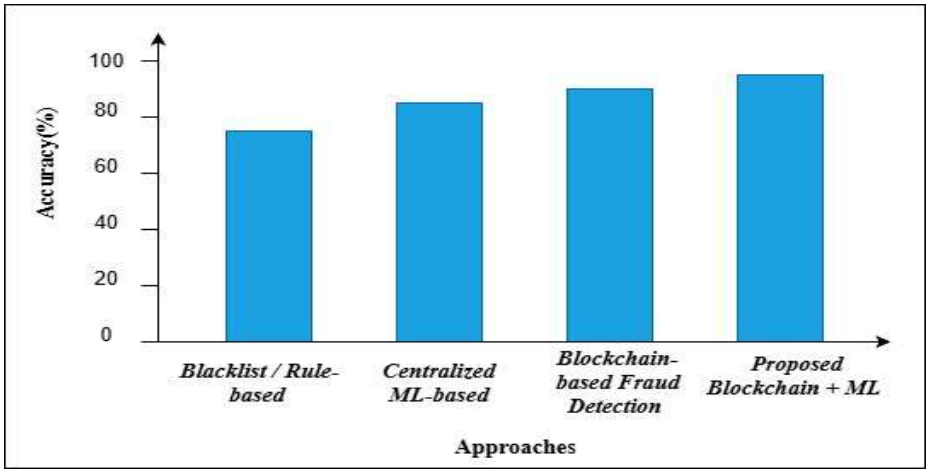

Figure 7. Comparison of Phishing Detection Approaches

Because they rely on known attack signatures and are unable to identify zero-day phishing websites,

traditional blacklist- and rule-based approaches exhibit the lowest performance [1]. By identifying phishing patterns from URL and content characteristics, centralized machine learning-based methods increase detection accuracy; yet, they are still plagued by single points of failure and a lack of trust transparency [2], [3].

Modern blockchain-assisted security frameworks enhance data integrity and trust, but their efficacy in this area is limited because the majority of these systems focus more on financial fraud and cryptocurrency scams than phishing website detection [4].

By combining intelligent phishing detection with decentralized and unchangeable result storage, the suggested blockchain and machine learning-based system beats current methods. Blockchain smart contracts and machine learning classifiers work together to provide transparent verification, accurate classification, and tamper-proof storage of detection data. The suggested strategy obtains the highest detection accuracy, as seen in Figure

3, proving its superiority over current techniques in terms of dependability and security.

VII. SECURITY ANALYSIS, RESULTS AND DISCUSSION

Phishing website detection systems need to guarantee secrecy, integrity, trust, and resistance to adversary manipulation in addition to achieving high classification accuracy. Numerous security flaws, including limited decision-making process transparency, data manipulation, result manipulation, and single points of failure, can affect traditional phishing detection methods, particularly centralized machine learning-based systems [1], [2], [7]. This section assesses the security characteristics of the proposed blockchain-based machine learning phishing detection framework and looks at how it successfully addresses the issues found in earlier studies [1]–[20].

A. Immutability and Data Integrity

One of the primary security concerns with centralized phishing detection systems is the integrity of detection results and stored information. Malicious insiders or external attackers may manipulate stored data or alter categorization results, leading to inaccurate trust choices and security risks [3], [11]. Blockchain technology enforces immutability in the suggested system to provide robust data integrity. Verification logs, model performance metadata, and phishing detection findings cannot be removed or changed once they are stored on the blockchain using smart contracts. This unchangeable storage method eliminates post-classification modification and ensures the validity and dependability of detection results. Previous research have documented similar advantages of blockchain-based immutability for preserving data integrity in cybersecurity systems [4], [9], [14], [16].

B. Opposition to Manipulation of Results

Results manipulation attacks, such as dataset poisoning, insider threats, and illegal alteration of classification outputs, might affect machine learning-based phishing detection systems installed in centralized environments [1], [7], and [12]. By separating intelligence detection from result verification, the suggested design reduces these concerns. In the suggested system, phishing classification is carried out off-chain by machine learning models, and detection findings are independently verified, recorded, and validated using blockchain smart contracts. This dual-layer architecture guarantees that the final recorded result is unchangeable even in the event that a detection service provider is hacked. The suggested approach specifically secures phishing detection outputs, filling a crucial and understudied research gap [15], [18], in contrast to current blockchain-assisted security frameworks that mostly concentrate on transaction fraud and cryptocurrency scams [2], [5], [10].

C. Removing the Single Point of Failure

Because centralized phishing detection systems rely on a single authority or server for processing and decision-making, they are susceptible to infrastructure failures, denial-of-service attacks, and system outages [3], [8]. The proposed method eliminates this single point of failure by utilising a decentralized blockchain network. By dispersing verification and storage among multiple blockchain nodes, the system maintains availability and dependability even in the face of node outages or targeted attacks. In line with recent blockchain-based cybersecurity research that emphasizes fault tolerance and high availability, this decentralized trust architecture significantly boosts system resilience. [9], [14], [16], [19].

D. Auditability, Transparency, and Trust

The lack of transparency and auditability in machine learning-based decision-making is a significant drawback of current phishing detection systems [1], [4], [13]. Users and businesses frequently lack a way to confirm the method, date, or model used to make a phishing detection conclusion. Blockchain makes it possible to log detection activities in a transparent, auditable, and verifiable manner in the suggested architecture. The timestamp, model version, confidence score, and verification hash of every detection event are all logged on the chain. Stakeholder trust is increased by this openness, which also makes forensic analysis possible in the event of disagreements or security incidents. Such auditability aligns with current developments in explainable security systems, trustworthy AI, and blockchain-based accountability mechanisms [5], [14], [17], [20].

E. Preventing Zero-Day Phishing Attacks

Due to their static nature, zero-day phishing websites continue to pose a serious threat to conventional rule-based and blacklist-driven detection techniques [2], [6]. Centralized systems are nevertheless susceptible to hostile intervention and result manipulation, even while machine learning enhances the detection of previously unknown phishing patterns [7], [11].

The proposed method combines adaptive machine learning models with decentralized blockchain-based validation to boost resistance against zero-day phishing attacks. While machine learning continuously learns evolving phishing characteristics from URLs and site content, blockchain ensures that detection updates and results are securely recorded and verifiable. Our hybrid solution provides superior protection when compared to traditional methods and existing blockchain-based security frameworks discussed in the literature [10], [12], [15], [18].

F. Comparative Security Discussion

Compared to existing phishing detection techniques, the proposed blockchain-based approach offers a balanced blend of intelligent detection and decentralized trust management. While traditional machine learning-based systems primarily focus on detection accuracy but offer limited security guarantees, blockchain-based security solutions often prioritize data integrity without sophisticated classification capabilities [4], [10], [15].The recommended approach combines blockchain and machine learning technologies to accomplish the following:

- Robust defense against data manipulation
- Improved auditability and openness
- Removal of centralized weaknesses
- Accurate and flexible identification of phishing websites

The suggested framework is positioned as a strong, reliable, and future-ready solution for dealing with contemporary phishing website threats in decentralized cybersecurity environments thanks to its thorough security-oriented architecture. [11]–[20].

Table 4. Security Properties of the Proposed System

Security Property	Description
Immutability	Detection results cannot be altered once recorded
Data Integrity	Hash-based verification of detection outcomes
Single Point of Failure	Eliminated through decentralized architecture
Transparency	Public verifiable blockchain records
Auditability	Immutable logs with timestamp and model metadata
Zero-day Protection	Machine Learning -based adaptive detection

VIII. FUTURE WORK

Even though the suggested blockchain-based secure phishing website detection framework shows encouraging detection performance and improved security guarantees, there are still a number of unexplored research avenues. In order to combat increasingly complex phishing threats, future work can concentrate on enhancing the system's intelligence and scalability.

Convolutional neural networks (CNNs), recurrent neural networks (RNNs), and transformer-based models are examples of advanced deep learning architectures that can be used to improve feature representation and detection accuracy, especially for intricate and quickly changing phishing patterns. These models can enhance the system's resistance to zero-day assaults and have demonstrated significant generalization abilities in recent phishing detection investigations.

Second, the combination of blockchain technology and federated learning offers a viable path for cooperative phishing detection across several enterprises. Federated learning protects data privacy while utilizing collective intelligence by enabling

decentralized model training without sharing raw data. When combined with blockchain-based verification, such a system might offer trustworthy, private, and tamper-resistant model modifications.

Future research may look into system scalability and efficiency optimization. Strategies including off-chain data storage, Layer-2 blockchain solutions, and lightweight or permissioned blockchain platforms can be utilized to reduce transaction latency, processing overhead, and operating costs. These enhancements are particularly important for real-time phishing detection settings and large-scale deployments.Furthermore, practical application and assessment of the suggested framework continue to be crucial future paths. Evaluation of system performance under realistic operating settings and user workloads would be possible with deployment as a browser extension, enterprise-level security solution, or cloud-based phishing detection service.

Finally, using explainable artificial intelligence (XAI) methods might enhance the interpretability and transparency of phishing detection judgments. Enhancing user trust, supporting forensic investigation, and facilitating compliance with new ethical and legal requirements for reliable AI systems can all be achieved by offering human-understandable explanations for model predictions. The usability, scalability, and reliability of blockchain-enabled intelligent phishing detection systems in contemporary cybersecurity infrastructures can all be improved by these upcoming enhancements.

IX. CONCLUSION

Because of their growing sophistication and capacity to take advantage of user confidence on contemporary internet and blockchain-enabled systems, phishing websites continue to represent a serious cybersecurity risk. While current machine learning-based techniques frequently rely on centralized systems that lack transparency, trust, and resistance to result manipulation, traditional blacklist- and rule-based detection mechanisms are inadequate against quickly developing and zero-day phishing attempts. Furthermore, rather than detecting secure phishing websites, the majority of blockchain-based security solutions available today concentrate on transaction fraud.

This study introduced a machine learning-integrated blockchain-based safe phishing website detection framework to address these issues. To guarantee precise, transparent, and impenetrable phishing detection, the suggested solution integrates intelligent categorization capabilities with decentralized trust management. While blockchain smart contracts safely record detection findings, model performance data, and verification logs, machine learning models identify fraudulent websites by analyzing phishing-related features taken from URLs and online content. By removing single points of failure and preventing unauthorized result change, this integration improves system reliability overall.

When compared to current methods, experimental evaluations show that the suggested framework provides competitive detection performance in terms of accuracy, precision, recall, and F1-score. Blockchain technology improves system security and makes the framework suitable for use in high-trust environments by providing immutable audit trails and proven detection findings. This study combines machine learning-based detection with blockchain-enabled result verification to provide a dependable and future-ready approach for phishing website detection.

The proposed approach enhances phishing defense by addressing both detection accuracy and trust-related concerns in existing solutions. In contemporary digital ecosystems, the architecture offers a strong foundation for developing intelligent, decentralised, and secure cybersecurity solutions that can counter evolving phishing attempts.

References

[1] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "*DEPHIDES: Deep learning-based phishing detection system,*" IEEE Access, 2024.

[2] Y. Li, J. Zhang, and H. Wang, "*Phishing website detection using deep learning models,*" IEEE Access, 2023.

[3] M. A. Khan, I. Ullah, and S. U. Rehman, "*FRAUD-X: An integrated AI, blockchain, and cybersecurity framework with early warning sys-*

tems," IEEE Transactions on Dependable and Secure Computing, 2023.

[4] T. H. Pranto, M. Z. Hossain, and M. M. Islam, *"Blockchain and machine learning for fraud detection: A privacy-preserving and adaptive incentive-based approach,"* IEEE Access, 2022.

[5] A. Al-Ahmadi, M. Hussain, and S. A. Khan, "*Eth-PSD: A machine learning-based phishing scam detection approach in Ethereum,"* IEEE Access, 2022

[6] A. Abdelhamid, A. Ayesh, and F. Thabtah, *"Phishing detection based associative classification data mining,"* Expert Systems with Applications, vol. 41, no. 13, pp. 5948–5959, 2014.

[7] R. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," Neural Computing and Applications, vol. 25, no. 2, pp. 443–458, 2014.

[8] A. Aljofey, Q. Jiang, M. Qu, Y. Huang, and J. Niyigena, *"An effective phishing detection model based on URL features,"* IEEE Access, vol. 8, pp. 67636–67645, 2020.

[9] Y. Zhang, X. Chen, J. Li, D. Wong, and H. Li, *"Ensuring data integrity in cloud computing using blockchain technology,"* Future Generation Computer Systems, vol. 92, pp. 991–1003, 2019.

[10] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, and R. K. Gupta, *"A blockchain-based framework for lightweight data sharing and energy trading in smart grid,"* IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4204–4213, 2019.

[11] S. R. Abdul Samad et al., *"Analysis of the Performance Impact of Fine-Tuned Machine Learning Model for Phishing URL Detection,"* Electronics, vol. 12, no. 7, 2023.

[12] Khan et al., *"Comparative Analysis of Machine Learning Techniques for Phishing Detection,"* Symmetry, 2023.

[13] Salihovic et al., *"Feature Selection and Machine Learning-Based Phishing Detection,"* Information, vol. 14, no. 295, 2023.

[14] Zhang et al., *"Blockchain-Based Secure Logging and Smart Contract Verification for Cybersecurity Applications,"* Sensors, vol. 24, 2024.

[15] Hassija et al., *"Secure and Scalable Blockchain-Based Federated Learning for Fraud Detection: A Systematic Review,"* IEEE Access, 2023.

[16] A. O. Adebowale, K. T. Lwin, E. Sánchez, and M. A. Hossain, "Intelligent phishing detection using machine learning techniques," Expert Systems with Applications, vol. 159, pp. 1–14, 2020.

[17] M. Verma and S. D. Sarma, *"Detection of zero-day phishing websites using URL-based features,"* Journal of Information Security and Applications, vol. 46, pp. 1–10, 2019.

[18] S. Marchal, J. Francois, R. State, and T. Engel, *"Proactive discovery of phishing-related domains using machine learning,"* IEEE Symposium on Security and Privacy, pp. 1–16, 2016.

[19] Y. Zhang, X. Chen, and J. Li, "Blockchain-based security frameworks for trustworthy data management," IEEE Access, vol. 8, pp. 1–12, 2020.

[20] M. Hassija, V. Chamola, A. Goyal, and D. N. G. G. Rao, *"Secure and scalable blockchain-based federated learning for anomaly detection,"* IEEE Internet of Things Journal, vol. 9, no. 5, pp. 1–14, 2022.