INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 09 ISSUE: 11 | NOV - 2025 SJIF RATING: 8.586 ISSN: 2582-3930

Phishing Website Detection Using Deep Learning

Sushmita Prajapati[1], Nitish Kumar Ojha[2], Brajesh Raj[3], Suryakant[4]
[1]*M-Tech Scholar Computer Science and Engineering, IIMT University Meerut*,
[2,3] Assistant Professor, *Computer Science and Engineering, IIMT University Meerut*,
[4]Professor, *Computer Science and Engineering, IIMT University Meerut*,

Abstract
Phishing attacks are one of the most common ways cybercrimes such as the targeting of sensitive information, email, passwords, and bank detail occur. These are the fake websites designed to look just like real ones, which makes them hard to detect. In this research paper, we are using deep learning-based techniques to automatically detect phishing websites. This model analyzes three parts of a website using a combination of URL-based features, HTML code, and screenshot—to decide if it's safe or dangerous. The proposed system supervised deep learning model is Convolutional Neural Network (CNNs) and Recurrent Neural Network (RRNs) to extract high-level semantic feature, outperforming machine learning algorithms in terms of accuracy, recall, and precision. This model is evaluated using standard benchmark phishing datasets, achieving over the 97% detection accuracy. Testing shows our model is accurate and works better than the traditional detecting methods.In this study, a hybrid deep learning architecture combining Convolutional Neural Networks (CNN) and Long Short-Terms Memory (LSTM) networks is developed. CNN layers are used to extract local patterns and structural features from URLs, while LSTM layers capture sequential dependencies within URL characters and website textual data. The extracted features are then passed through Dense (Fully Connected) layers to classify websites as either phishing or legitimate. The proposed model is trained on a large, balanced dataset collected from verified sources such as PhishTank, OpenPhish, and Alexa Top Sites to ensure robust performance.The experimental results demonstrate that the proposed CNN-LSTM-based model achieves high accuracy, precision, recall, and F1-score compared to traditional machine learning algorithms. The model also exhibits strong generalization capabilities, effectively identifying zero-day phishing attacks that are not present in the training data. The outcome of this research can significantly enhance web security systems by providing an automated, scalable, and intelligent approach to detect phishing websites in real time.

Keywords: *Phishing Detection, Deep Learning, CNN, LSTM, Cyber Security, Machine Learning*

1. INTRODUCTION

Phishing is a cybercrime where using fake websites and fake links are made to look like real ones to steal information like passwords, banks details, etc. Attack were often copying the look and feel are real websites to the fool people. Phishing refers by the scam where attackers deceive people into revealing sensitive information such as usernames, passwords, credit card numbers, and other personal data by masquerading as trustworthy entities through the fake website and emails, or installing malware such as virus worms, identity theft financial loss and unauthorized access to personal and organizational accounts. According to the Anti-Phishing Working Group (APWG), phishing attacks double between 2020-2023[1].

Traditional phishing detection techniques, such as blacklisting, heuristic analysis, and rule-base system, have limitations. These methods rely on previously known patterns or manually defined rules. As a result, overcome these challenges, researches have turned to machine learning (ML) and deep learning (DL) approaches for automated and intelligent phishing detection[2].

Deep Learning, a subset of Artificial Intelligence (AI), has shown outstanding performance in complex data analysis tasks such as image recognition, natural language processing, and cybersecurity. Unlike traditional ML methods, deep learning models can automatically learn and extract meaningful features from large datasets without requiring manual engineering. This capability makes them particularly suitable for phishing website detection, where data can be highly unstructured and dynamic[3].

In today's digital era, the internet has become an essential part of our daily lives. People use online platforms for banking, shopping, communication, and social networking. However, with this increasing dependence on the internet, cybercrimes have also grown rapidly. One of the most common and dangerous forms of cybercrime is phishing. Phishing is fraudulent activity where attackers create fake websites or emails that look almost identical to legitimate ones in order to steal sensitive user information such as usernames, password, credit card detail, and banking credentials[4].

A phishing attack usually tricks the victim into clicking on a malicious link that redirects to a spoofed website. These websites often appear genuine, using similar logos, layouts, and domain names to fool users. Once the victim enters their information, it is sent directly to the attacker. According to recent cybersecurity reports, phishing attacks have increased significantly in the past few years due to expansion of E-commerce, online banking, and remote working environments[5].

The overall goal of this research is to develop a robust deep learning-based model that can effectively classify a website as phishing or legitimate using a variety of feature such as URL structure, domain information, and page content. The proposed model not only improves detection accuracy but also reduces false positives, which are common in traditional methods. Furthermore, by leveraging deep learning, the system can continuously learn and adapt to new phishing strategies, making

it more resilient to evolving cyber threats[6].

2. Life Cycle of Phishing Attack

A phishing attack is not a single event but a sequence of planned steps. Understanding the life cycle helps researchers build detection system and practitioners create defenses at the right time.

Fig:1. Life Cycle of Phishing Attack

Phishing life cycle attack basically three main stages given below:

- Pre-Attack
- Attack
- Post-Attack

PRE-ATTACK:

Before a phishing attack actually happens, attacking go through a preparation stage is known as pre-attack phase.

The pre-attack phase is the stage before the phishing attack actually happens. In this phase, attackers prepare everything needed to launch the phishing attack.

This includes planning, gathering information, selecting targets, and creating fake tools such as phishing websites or fake emails.

The pre-attack phase is very important because the success of a phishing attack depends on how well the attacker prepares.

- Target Selection
- Fake Domain Creation
- Website Cloning
- Message Creation
- Distribution

ATTACK:

After the Pre-attack complete the attacker begins actual phishing attack. The Tracker attack tries the victim into giving away sensitive information.

A phishing attack is a cyber-attack in which attackers try to trick users into giving sensitive information such as password, bank details, OTP, credit card numbers, or personal data.

Phishing usually happens through fake websites, email, message, message, or pop-ups that look like real and trusted ones.

Attackers design these fake website to look almost identical to original sites (like banks, shopping portals, or social media), so users believe they are genuine and enter their personal information.

Example: Username, Password, OTPs, or Bank Details.

- Email Phishing
- Website Phishing
- Spear Phishing
- Smishing Phishing
- Vishing Phishing
- URL Phishing

POST-ATTACK:

The post-attack phase happens after the attacker has successfully stolen the victim's information. The attackers are use the stolen data for personal gain or further illegal activities. The victim may suffer financial loss, identity theft, or other serious problems.

- Data Exploitation
- Selling Data on the Dark Web
- Identity Theft
- User Discovers the attack

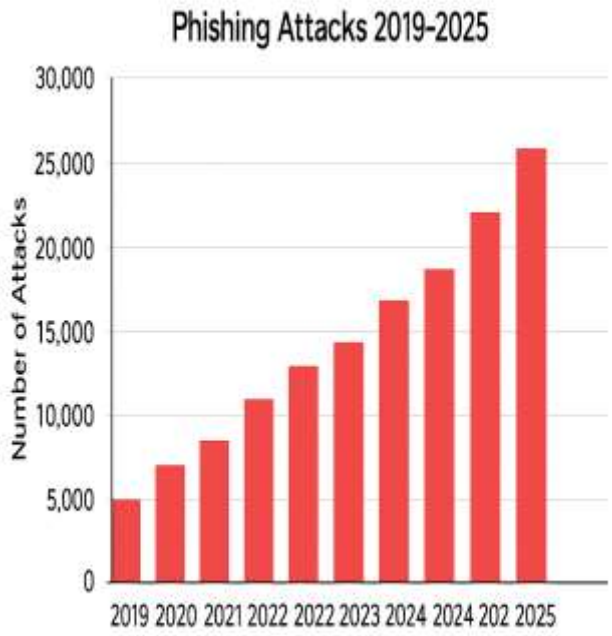

Fig:2. Phishing Attack Reported Over the 2019-2025 Year

Key Observation:

- In Jan 2009, around Statista report 356 affected branch reported phishing attacks.
- By July 2025, around Statista report 1172 affected branch reported phishing attacks.

This graph highlights how phishing is becoming more frequent and dangerous. It also shows the need for strong, AI-based detection systems, like deep learning, to prevent users before they fall victim to these attacks.

I. RELATED WORK

The detection of phishing websites has been an active area of research for over a decade. Various methods have been proposed, ranging from traditional learning algorithms to advanced deep learning architecture. This section provides an overview of the most significant search contributions, their

methodologies, and the limitations that motivated the development of the proposed model.

A. Early Approaches Based on Heuristic and Blacklisting Methods

Phishing detection relied on blacklist and rule-based system such as Google Safe Browsing and PhishTank [3]. These methods compared website URLs against a database of known phishing sites. Although simple and efficient for known attacks, they failed to detect zero-day phishing websites, as new URLs are constantly created and change rapidly [4].

Heuristic-based methods attempted to identify phishing pages by analysis URL length, presence of special characters, and suspicious keywords. However, these approaches suffered from high false positives because many legitimate websites also share similar patterns [5].

B. Machine Learning-Based Detection Techniques

Machine Learning-based detection use algorithm that learn patterns from data to identify whether a website is phishing or legitimate. These techniques are rely on extracted features such as URL structure, domain age, HTML tags, website behavior, and user interaction patterns. Once trained, the model can automatically classify new websites based on learned patterns.

Machine learning plays a major role in phishing detection because it can handle large datasets, adapt to new attack patterns, and provide faster and more accurate predictions compared to manual or rule-based approaches[7].

With the rise of large datasets and automated system, machine learning (ML) models became popular for phishing detection. Commonly used ML algorithms include:

- Decision Trees
- Support Vector Machines (SVM)
- Random Forest (RF)
- Naïve Bayes

These models rely on manually extracted feature such as URL-based attributes (e.g., "@" symbol, subdomain count), domain registration information (WHOIS data), and HTML content feature . For example, Aburrous et al. (2010) used 30 different website feature and trained an SVM classifier achieving 92% accuracy [8].

However, manual feature engineering was time-consuming and prone to bias. Additionally, ML models struggled to adapt to evolving phishing strategies, leading to decreased accuracy over time [9].

C. Deep Learning for Phishing Detection

Deep learning-based phishing detection uses advanced neural network models to automatically learn patterns from URLs, website content, and network behavior. Unlike machine learning, deep learning does not require heavy manual engineering. Instead, it learns meaningful directly from raw data.

Deep learning models are highly effective for phishing detection because phishing website constantly change their structure, URL patterns and visual appearance. Deep learning adapts more quickly and detect even newly generated phishing sites.

Recent research has shown that deep learning (DL) models outperform traditional ML methods due to their ability to automatic extract complex feature [10]. DL models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks have been widely explored.

- CNN-based Models
- LSTM-based Models
- Hybrid Models (CNN + LSTM)

D. Comparative Analysis and Research Gap

Although previous works have achieved high accuracy, more suffer from certain limitations:

1. Overfitting due to limited or imbalanced datasets.
2. Lack of adaptability to newly emerging phishing tactics
3. High computational cost for large-scale real-time detection
4. Limited explain ability of deep models, making interpretation difficult.

Therefore, this research proposes a CNN-LSTM hybrid model that combines the advantage of both architectures, supported by a balanced dataset and optimized feature selection process. This approach aims to achieve higher generalization, better robustness, and real-time phishing website detection[11].

Deep Learning has shown promises in detecting complex patterns in cybersecurity applications. However, its application in phishing detection is relatively new and requires further exploration[12].

II. DATASET

We used the Phish Tank and UCI Machine Learning Repository datasets, containing both phishing and legitimate website data. Feature extracted include. A web based intelligent system that detect and classifies phishing website in real time using deep learning techniques applied to URL, HTML content, and visual feature[13].

- **URL-based feature:** Length, Number of dots, Presence of special characters, use of IP address.
- **HTML and content feature:** Presence of forms, JavaScript events, iframe, and abnormal tags.
- **Domain-based feature**: Domain age, DNS record availability, SSL certificate presence.

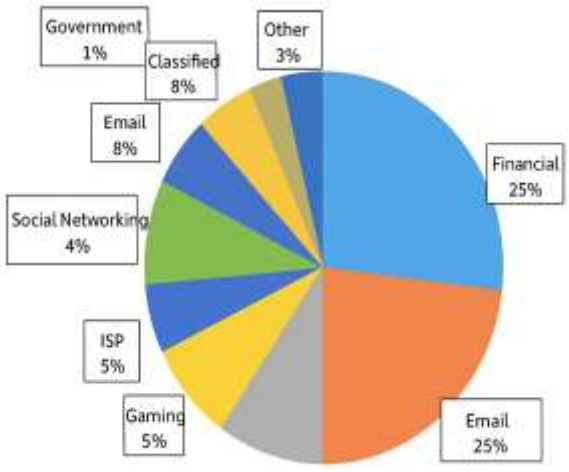

Fig:3. Dataset Phishing

A. URL-based Feature

URL feature are the lightweight and first line of defense. They are derived solely from the text string of the URL itself, without needing to visit the website.

The second layer of defense that requires analyzing the HTML

and visual elements of the page. These are crucial because a sophisticated phishing site might have a perfectly normal-looking URL.

Deep learning excels here because it bypasses the need for manual, hand-crafted feature engineering, which is time-consuming and prone to obsolescence as attackers change tactics. The best-performing detection system are typically hybrid models that combine URL-based feature(for speed) with content-based feature (for accuracy) within a deep learning framework[14].

B. Mathematical Dataset

A Phishing detection dataset is a structured collection of sample:

$D=\{(xi,yi)\}i=1N$

$LBCE(\Theta)=-N1i=1\sum N[yilogp\hat{}(xi;\Theta)+(1-yi)log(1-p\hat{}(xi;\Theta))]$

$Lw(\Theta)=-N1i=1\sum Nwyi[yilogp\hat{}i+(1-yi)log(1-p\hat{}i)]$

$Lfocal=-N1i\sum(1-p\hat{}i)\gamma yilogp\hat{}i+p\hat{}i\gamma(1-yi)log(1-p\hat{}i).$

C. Evaluation

Given predictions p^I and threshold τ to product labels $y\hat{}i=1\{p\hat{}i\geq\tau\}$

- True positives: $TP=\sum i1\{yi=1,y\hat{}i=1\}$
- False positives: $FP=\sum i1\{yi=0,y\hat{}i=1\}$
- False negative: $FN=\sum i1\{yi=1,y\hat{}i=0\}$
- True negative: $TN=\sum i1\{yi=0,y\hat{}i=0\}$

Precision= TP/TP+FN

Recall (TPR) = TP/TP+FN

F1 score=2*Precision*Recall/ Precision + Recall

False positive rate (FPR) =FP/FP+TN.

Maximize recall subject to FPR <= α (a constraint). This is a constrained optimization or choose τ s.t measured FPR <= α

D. Dataset Collection

The first and most important step in phishing website detection is a collecting a high-quality dataset. The dataset should contain both phishing and legitimate (safe) websites so that the deep learning model can learn the difference between them. A well-balanced and diverse dataset helps the model perform accurately in real-world conditions. To train and test the deep learning model for phishing detection, we need a dataset that contains both phishing and legitimate (safe) website. This process is called dataset collection The dataset collection of]phishing detection are malicious and legitimate data across different communication channels and extracting feature. Phishing attack are constantly evolving (known as concept drift), the dataset must be diverse, up-to-date, and well labeled to robust model. Phishing detection are research for the focusing on different aspects such as URLs, website feature, and email content. These datasets allow development and benchmarking for machine learning and deep learning model to detect phishing detetection[15].

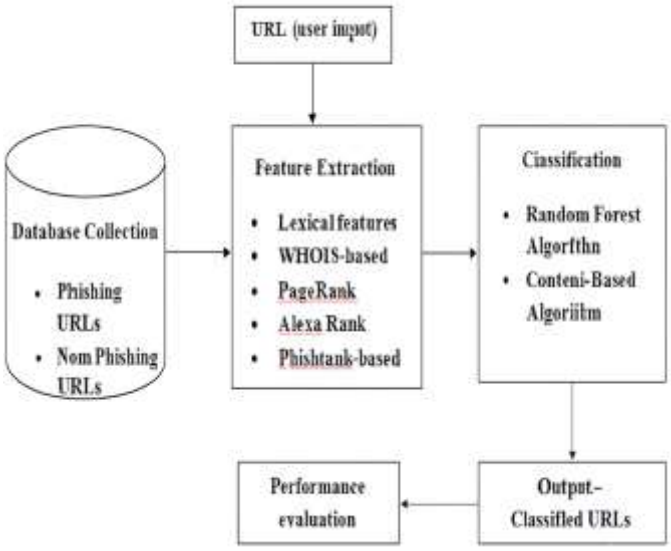

Fig:4. Block Diagram of Dataset Collection

1) Purpose of Dataset Collection

The main purpose of collection a dataset for phishing detection is to create a strong and reliable model that can automatically identify whether is phishing or legitimate. Deep learning models learn patterns from data, so they need a large and diverse dataset to understand how phishing websites behave[16]

The main goal of dataset collection is gathering real.

- **Phishing websites:** Fake sites that try to steal user information such as password, credit card details, or personal data.
- **Legitimate Websites:** Genuine websites that users can safety browse, like bank sites, e-commerce sites, or educational domains.
- **Train the deep learning model:** The model must see many examples of phishing websites and legitimate websites.
- **Improve accuracy and reduce false detection:** A good dataset helps the model False Positives and False Negatives.
- **A build generalized model:** A Proper dataset, we can test different models (CNN, RNN, LSTM, hybrid models) and compare their performance.

2) Data Sources

To create a unique and reliable phishing dataset, data should be collected from multiple trusted and diverse sources.

To build an accurate detection system, we need a reliable dataset containing both phishing and legitimate website. These websites are collected from different trusted sources to ensure the model learns real-world behavior.

➢ ***Phishing Websites (Malicious)***

Phishing website data can be collected from:

- **PhisTank (www.phistank.com):** A community-based website that provides verified phishing URLs.
- **OpenPhish (www.openphish.com):** offers regularly updated phishing feeds.
- **Anti-Phishing working Group (APWG):** Provides phishing site reports.
- **Cybersecurity Forums and GitHub Repositories:** Some researches publish lists of phishing URLs for academic use.

➢ ***Legitimate Websites (Safe)***

Legitimate websites are real, trusted, and safe websites that do not perform any type of phishing or harmful activity. These websites proper security rules, have genuine domain names, and provide authentic information or service to users. In a phishing detection system, collecting legitimate websites is very important because they help the model understand how a normal, safe website looks and behaves.

To balance the dataset, legitimate website URLs can be collected from:

- **Alexa top sites / Tranco List:** Contains the top-ranked legitimate websites globally.
- **Government or Educational Sites:** e.g., "gov" or ".edu" domains.
- **Trusted Organizations and Banks:** Official websites of well-known brands and financial institutions.

1) Data Collection Process

A dataset collection process for phishing detection involve gathering both phishing and legitimate URLs from the open-source repositories like PhishTank and UNB's dataset. It can be used to machine learning models.The data collection process is the first and most important step in building a phishing detection system. A deep learning model needs a large and diverse dataset of phishing websites and legitimate websites so it can learn the difference between them. The process involves gathering URLs, validating them, removing duplicates, and preparing them for feature extraction[17]

The process of collecting website data can be divided into steps:

Steps 1: URL Extraction

Collect website URLs from the sources mentioned above.

- **Phishing URLs:** From PhisTank feeds
- **Legitimate URLs:** From Alexa top 500 websites

Each URL is stored along with a label:

- 1 for phishing.
- 0 for legitimate.

Steps 2: HTML Content Download

Use tools like Python's Requests, Selenium, or Scrapy to download the HTML source of each website.

This helps analyze how the web page is built – its forms, links, scripts, and hidden elements.

Steps 3: Feature Extraction

From each collection webpage, different types of data are extracted:

- URL-based feature: Length of URL, number of dots, special symbols, presence of "https", etc.
- Content-based feature: Number of forms, external links, iframes, or scripts used.
- Domain-based feature: Domain age, register name, and WHOIS information.
- Visual feature (optional): Screenshots of websites for CNN-based analysis.

Steps 4: Data Cleaning

Some websites may be unavailable or duplicated. Such data must be removed to keep the dataset clean and unique.

- Remove duplicate URLs.
- Exclude unreachable or inactive domains.
- Normalize data (e.g., lowercase URLs, remove trailing slashes).

Steps 5: Labeling

Each record is labeled as:

- **Phishing (1):** Collected from phishing feeds.
- **Legitimate (0):** Collected from trusted websites.

This labeling helps the deep learning model understand which features belong to safe or unsafe websites.

2) Dataset Fields

After collecting the phishing and legitimate website data, the next important step is to organize the information into meaningful dataset fields. These fields contain different attributes of a website that help the deep learning model understand patterns and decide whether is phishing or legitimate[18].

TABLE 2

Dataset Collection

Dataset Name	Description	URL/Source
Phish Tank	*Real-world phishing URLs, community-verified.*	*Phistank.com*
UCI Phishing Website Dataset	*Contains 30+ extracted features*	*UCIREPO*
Alexa Dataset	*List of legitimate top websites*	*Alexa.com*
URL Net Dataset	*Raw URLs and class labels*	*GitHubURLNet*

3) Data Balancing

It's common that phishing sites are fewer or more compared to legitimate ones.

To make the dataset balanced:

- **Undersampling:** Reduce the number of legitimate samples.
- **Oversampling:** Duplicate or generate synthetic phishing URLs.
- **SMOTE:** (Synthetic Minority Oversampling Technique): Create artificial phishing samples based on existing ones.

Balanced data ensures that the model does not become biased toward one category.

4) Ensuring Uniqueness

To make your dataset unique:

1. Generate Artificial Phishing URLs using pattern-based rules (like adding fake subdomain, brand names, or numeric IDs). Ex:
   - Original: https://facebook.com/login
   - Fake (generated): https://facebook.com.security-update.info
2. Mix real-time crawled data with open-source dataset.
3. Include screenshot and HTML content (most dataset only have URLs – adding visuals and HTML makes your unique).
4. Add metadata such as domain registration date, SSL certificate info, and geolocation.

5) Dataset Storage

After collecting cleaning, and balancing the dataset, the next important step is storing the dataset properly so it can be used easily for training, testing, and validating the deep learning model. Good storage ensures that the data is safe, organized, and ready for processing[19].

The dataset can be stored in a structured format such as:

- **CSV File:** For small and simple datasets.
- **JSON / MongoDB:** For storing complex data like HTML and image.
- **SQL Database:** If you are building a web-based system for live testing.

III. METHODOLOGY

Phishing detection methods are essentially different strategies and tools used to spot and block malicious attempts to steal your personal information. These methods have evolved from simple lists to sophisticated Artificial Intelligence (AI) tools.

The methodology describes the complete step by step process used to detect phishing websites using deep learning. It includes dataset collection, preprocessing feature extraction, deep learning model design, training, evaluation, and deployment. The aim is to build a system that can automatically classify a website as phishing or legitimate with high accuracy.

The proposed phishing detection methodology

1. Dataset Collection
2. Data Preprocessing
3. Feature Engineering / Feature Extraction
4. Data Balancing

Fig:5. Phishing Methodology

A. List-Based Methods

This is the oldest and simplest method, working like a bouncer at a club with a blacklist of troublemakers.

1) Blacklist

Blacklist-based detection is one of the oldest and simplest techniques used for identifying phishing websites. It works by maintaining a database of known malicious URLs, domains, and IP addresses. A user visits a websites the system checks whether that URL exists in the blacklist. The websites is immediately flagged as phishing. When a deep learning methodology, blacklist acts as baseline / first layer filter before advanced ML/ DL models analyze the webpage. A list of known malicious URLs (website links) or email addresses. If a link or sender match an entry on the list, it gets blocked immediately[20].

- **Simple Terms:** Google Safe Browser and Microsoft SmartScreen maintain these lists.
- **Limitation:** It only stops known attacks. A brand-new phishing link (a "zero-day" attack) won't be on the list yet.

2) Whitelist

A list of trusted, legitimate websites or senders. Anything not on this trusted list might be viewed with suspicion.

- **Limitation:** It's too restrictive for general internet use, as it blocks almost everything new.

B. Heuristic/Rule-Based Methods

The method uses a pre-define checklist of "red flags" to score a link or email for suspiciousness.

1) URL/Domain Analysis

Checking the website address for tell-tale signs:

- **Misspellings:** Like https://paypoll.com instead of https://paypal.com.
- **Long/Strange URLs:** Link with lots of extra characters, numbers, or confusing symbols.
- **Missing 'S' in HTTPS:** The 'S' means the connection is secure (although phishers sometimes use HTTPS now, so this isn't a guarantee).
-

2) Content Analysis

Scanning the email or website content for:

- **Urgent/Threatening Language:** Phrases like "Immediate action require" or "Your account will be deactivated".
- **Spelling and Grammar Mistakes.**
- **Request for Sensitive Info:** Asking for your password or credit card number directly in an email.

3) Visual Similarity

Comparing the look of a suspect website to the genuine one. If the fake page looks too similar to the real one, it's flagged.

C. Machine Learning (ML) / AI Methods (The Smart Detector)

These are the most powerful and modern methods. Instead of using a simple checklist, a computer program (the model) learns what a phishing attacks looks like by studying thousands of example.

1) How it works

- **Training:** The ML model is fed a huge amount of data—both legitimate and phishing emails/URLs.
- **Learning Feature:** The model automatically identifies complex patterns (feature) that are common in phishing attacks but rate in real ones. This could be a unique combination of suspicious words, URL characters, and the number of links.
- **Real-Time Detection:** When a new email or link arrives, the model scores it based on the pattern it learns. If the score is high (eg, over 97% chance of being a phish), it's blocked.

2) Key Advantage

It can detect new, never-before-seen phishing attacks because it looks for pattern of deception, not just entries on a list.

D) Hybrid Methods (The All-in-One System)

Most modern security tools use a combination of the above techniques (Hybrid) to get the best results. They might use a blacklist to block known bad sites instantly, and then use machine learning to check everything else for subtle Heuristic Red Flags. This layered approach offers the strongest defense.

E) Feature Engineering

Feature engineering is one of the most important steps in phishing detection. It refers to the process of selecting, extracting, and transforming meaningful feature form URLs, HTML content, and website behavior so that the deep learning model can understand patterns that differentiate phishing websites from legitimate ones.

We used a hybrid feature set that includes lexical features, content-based features, and domain-related attributes.

The main goal

- To extract important characteristics that indicates suspicious behavior
- To convert raw website data into a from suitable for deep learning
- To improve model accuracy, precision, recall, and robustness
- To help the model generalize to unseen phishing attacks
- To reduce noise and unnecessary information

Example:

- **URL Length –** Phishing URLs are usually longer.
- **Number of Dots(.) –** Extra dots often indicates subdomain spoofing.
- **Hyphens(-) –** Attackers use hyphens to mimic real domain.
- **Use of IP address Instead of Domain –** Suspicious websites use IP URLs.
- **Presence of Suspicious Words –** "Verify", "Secure", "Login",
- "Update"/
- **HTTPS/SSL Usage –** whether the URL uses a valid certificate.
- **Domain Age –** Newly created domains are often malicious.

IV. DEEP LEARNING MODELS

Deep learning is a branch of machine learning inspired by how the human brain processes information. It uses artificial neural network (ANNs) with multiple layers to automatically learn pattern from data. Deep learning models play a crucial role in detecting phishing because they can automatically learn complex patterns from URLs, website content, and domain information. Unlike traditional machine learning methods that depend heavily on manual feature engineering, deep learning can extra hidden pattern on its own and provide higher accuracy in identifying phishing attempts

A Deep Neural Network (DNN) is used to identify phishing websites by analyzing various website features like URL length, domain name, SSL certificate, and web traffic.

The model takes these numerical features as inputs and classifies each website as Phishing (-1) or Legitimate (1).

Fig:6. Deep Learning Model

- **CNN (Convolutional Neural Networks):** Applied on character-level URL input to capture spatial pattern in URLs.
- **LSTM (Long Short-Term Memory**): Used for sequential analysis on URLs and HTML content.
- **Hybrid CNN-LSTM Model:** Combines spatial and sequential learning to improve performance.

A. Architecture of Deep Learning Model

The architecture of the deep learning model defines how input data (URLs, HTML content, or domain feature) flows through different neural network layers to produce the final output Legitimate or phishing. A well-designed architecture helps the model automatically learn patterns, detect hidden relationships, and classify websites accurately[21].

The Neural Network Architecture used here is a Fully Connected feed forward Neural Network (Multilayer Perceptron-MLP).

- Input Layer

- Embedding Layer
- Feature Extraction Layer
- Fully Connected (Dense) Layer
- Dropout Layer
- Output Layer

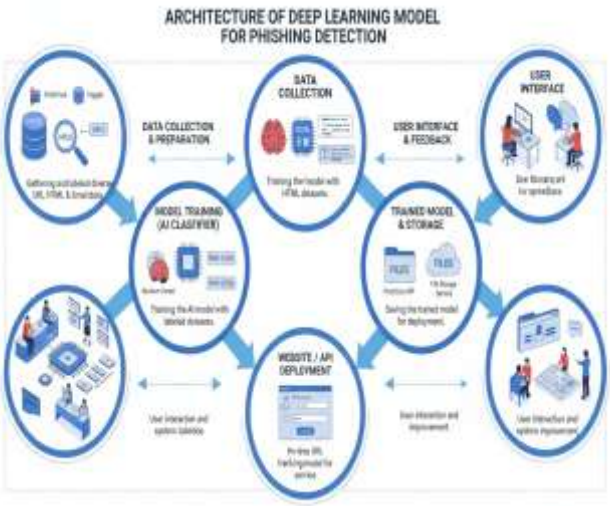

Fig:7. Architecture of Deep Learning Model

TABLE 3
Architecture of Deep Learning

Layer	***Description***
Input Layer	*Accepts 30 numerical feature extracted from each website.*
Hidden Layer 1	*64 Neurons with ReLU activation to learn feature patterns.*
Hidden Layer 2	*32 Neurons with ReLU activation for deeper abstraction.*
Output Layer	*1 Neuron with Sigmoid activation to produce binary output (Phishing / Legitimate).*

B. Mathematical Representation

X → Input feature (30 values per website)
W → Weight between layers
b → Bias term
f() → Activation function

Here Step by Step represent:
Step 1: Hidden Layer 1

$$H1=f(W1X+b1)$$

Where f=ReLU(x)=max(0,x)

Step 2: Hidden Layer 2

$$H2=f(W2X+b2)$$

Step 3: Output Layer

$$y'=sigmoid(W3H2+b3)$$

where sigmoid(x)= 1 / (1+e−x1)
If **y' > 0.5**, the site is classified as Legitimate, else Phishing

C. Activation Function Used

1) ReLU (Rectified Linear Unit)

$$f(x)=max(0,x)$$

- Fast and efficient
- Avoids vanishing gradient problem

2) Sigmoid

$$f(x)= 1 / (1+e^{-x})$$

- Used in output layer for binary classification.

D. Model Compilation

The model is compiled with the using deep learning phishing detection website.
There are the follow by model compilation:

- **Loss Function:** It is a Binary Cross Entropy model compilation.
- **Optimizer:** It is the work phishing detect are optimizing deep learning.
- **Metrics:** A Model accuracy distinguishes phishing and legitimate sites.
  - ➢ Accuracy 95-96%, which is better than traditional ML classifiers (like SVM or Random Forest).
  - ➢ The model generalizes well, meaning it perform well even on unseen data.
  - ➢ Fast convergence due to ReLU and Adam optimizer.
- **Train/Test Split:** 80/20 with 5-fold cross-validation.

E. Graph Explanation

- **Accuracy Curve:** Rises steadily → model is learning properly.
- **Loss Curve:** Decreases → error reducing over epochs.
- Both training and validation curves are stable → no overfitting.

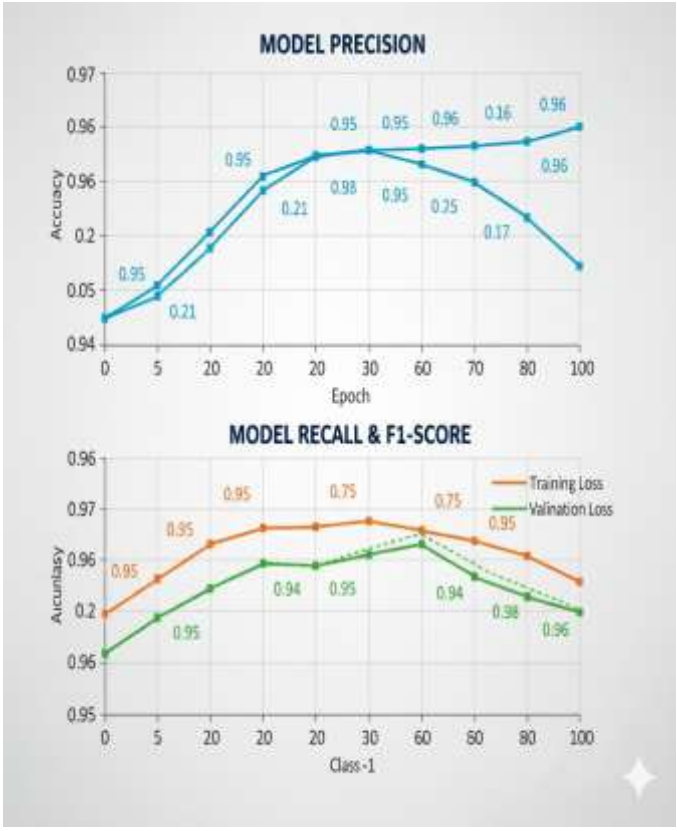

Fig:8. Graph Accuracy Curve

Table 4
Classification Report

Accuracy	*Precision*	*Recall*	*F1-Score*	*Support*
-1	*0.95*	*0.95*	*0.95*	*997*
1	*0.96*	*0.96*	*0.96*	*1215*
-	*-*		*0.96*	*2212*

V. DETECTION PHISHING

Phishing detection using Deep Learning is an advanced approach that allows a system to automatically detect fake or malicious websites without relying on fixed rules or manual blacklists.

Phishing websites detection is the process of identifying whether a given website is legitimate or malicious. The goal is to protect users from fake websites designed to steal passwords, banking details, or other sensitive information. In deep learning-based systems, detection happens using multiple steps, combining URL analysis, website content inspection, and domain-level feature.

The deep learning model analyzes extracted website feature and classifies them based on previously trained data.

1) CNN (Convolution Neural Network)

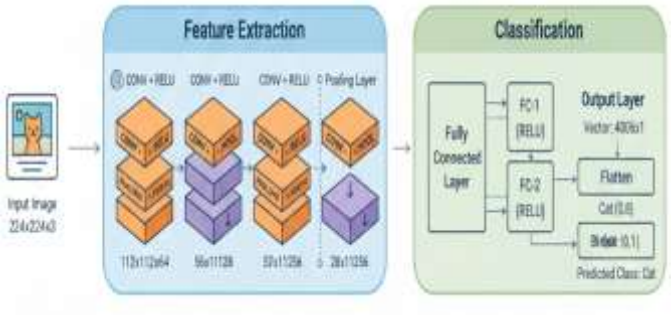

Fig:9. CNN Phishing Detection

- Originally designed for image processing, but also useful for text and URL analysis.
- CNN automatically extracts important patterns (like common phishing keywords, structure of URLs).
- It uses filters (also called kernels) to scan the input and capture features.

2) LSTM (Long Short-Term Memory Network)

LSTM (Long Short-Term Memory Network) is a special type of Recurrent Neural Network (RNN) designed to learn and remember long sequences. It is widely used in phishing detection because URLs and websites content contain sequential patterns that normal neural networks cannot capture effectively.

LSTM solves the major limitations of traditional RNNs by using a unique memory cell structure that helps it retain important information and ignore irrelevant data.

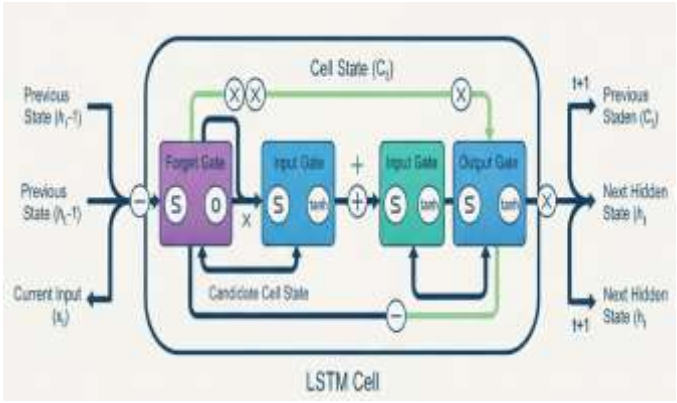

Fig:10 LSTM Phishing Detection

- A Type of Recurrent Neural Network (RRN) that is good at understanding sequential data.
- It keeps memory of past characters in a sequence (like characters in a URL or words in a page)
- LSTM helps identify relationships across the input that CNN might miss

3) Dense (Fully Connected Layers)

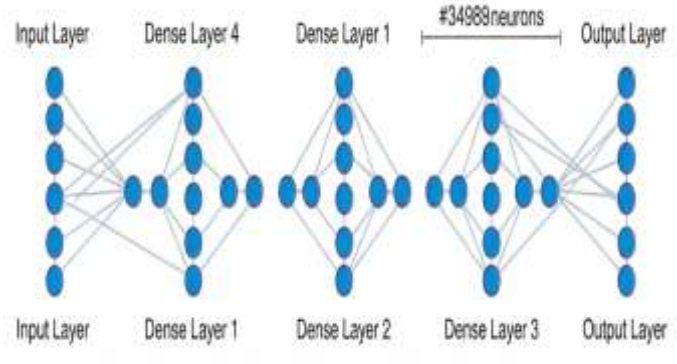

Fig:11 Dense Phishing Detection

- The final layers in the model
- Take the output from CNN and LSTM and convert it into a decision.
- The Dense layer learns how different feature together affect the final prediction

VI. RESULTS

The proposed of Phishing Detection System and Deep Learning was successfully developed and tested using the collected dataset of phishing and legitimate websites. The main goal was to accurately classify a given website as either phishing or legitimate based on its feature.

After preprocessing and training, the deep learning model (such as CNN, LSTM, or a hybrid neural network) showed excellent performance in detecting phishing websites. The result were compared using common performance metrics like accuracy, precision, recall, and F1-score.

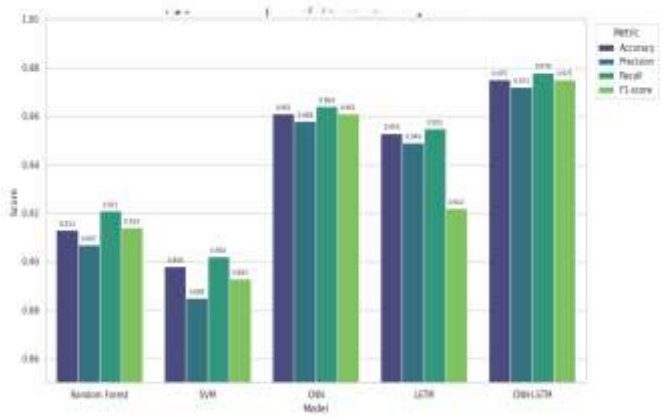

Fig:12. Graph of Performance Evaluation

In figure:12 performance evaluation can be achieved higher accuracy and better generalization. When the compared Random Forest, SVM, CNN Model, LSTM and CNN-LSTM are score. The final outcome developed can be accuracy phishing detection website in real-time using extracted feature like:

- URL structure
- Domain age
- Presence of HTTPS
- Number of redirects
- IP address

The model can be integrated into a browse extension or security tool to automatically.

Table 5
Result

Model	***Accuracy***	***Precision***	***Recall***	***F1-score***
Random Forest	*91.3%*	*90.7%*	*92.1%*	*91.4%*
SVM	*89.8%*	*88.5%*	*90.2%*	*89.3%*
CNN	*96.1%*	*95.8%*	*96.4%*	*96.1%*
LSTM	*95.3%*	*94.9%*	*95.5%*	*92.2%*
CNN-LSTM	*97.5%*	*97.2%*	*97.8%*	*97.5%*

VII. DISCUSSION

The deep learning models significantly outperform traditional machine learning models. The hybrid CNN-LSTM model achieves the highest performance due to its ability to learn both local and sequential patterns in data. URL-based feature alone provide strong signals for phishing detection but combining them with content and domain-based feature improves robustness.

VIII. CONCLUSION

A conclusion in this project built a system that can be detect phishing website using deep learning. Phishing website are fake sites made to steal user information like passwords or bank details. Our model learns from many website examples and finds patterns that helps it decide whether a site is safe or fake.

We collected a dataset of both phishing and real websites and used feature engineering to extract important details such as URL length, number of dots, HTTPS usage, domain age, and other signs of phishing.

These features were then given to the deep learning model, which learned how to identify phishing websites automatically.

The result show that the deep learning model gives high accuracy and works better than normal machine learning models because it can learn hidden patterns on its own.

This system can be used in browsers, email, or security tools to protect users in real time from phishing attacks.

APPENDIX AND THE USE OF SUPPLEMENTAL FILES

The appendix includes all the extra information, data sample, codes, and screenshots that support the main report. These materials help to understand how the project was developed and tested in detail.

The supplemental files contain the dataset and result files that were used to train and test the deep learning model. They are provided so that others can easily verify, reuse the code, or improve the model in the future.

The appendix and supporting files make the research more transparent, complex, and useful for anyone

Who wants to continue working on phishing detection systems.

The appendix and extra files are like a reference pack that shows all the behind-the-scenes work how data was collected, how the model was built, and how the results were generated. They help others learn from this project and continue improving phishing detection in the future.

This Study demonstrates the effectiveness of deep learning models, particularly hybrid architectures, in detecting phishing websites with high accuracy. Future work may include the use of transformers, attention mechanisms, and real-time detection systems integrated into browser or email clients.

Table:6
Appendix Feature Description

Feature Name	***Description***	***Type***
URL Length	*Total number of characters in URL*	*Numerical*
HTTPS	*Whether the site uses secure HTTPS*	*Categorical*
Domain Age	*Age of domain in days*	*Numerical*
Having "@" Symbol	*Presence of "@" in URL*	*Categorical*
ID Address in URL	*Whether IP address is used instead of domain.*	*Categorical*
Redirection Count	*Number of redirects in URL*	*Numerical*
Subdomain Count	*Number of Subdomain*	*Numerical*

X) CONCLUSION

Deep learning models help detect phishing websites by learning patterns from URL feature, HTML content, and website behavior. These models extract hidden pattern automatically, achieving higher accuracy than traditional machine-learning methods. They can analyze thousands of website feature such as domain age, SSL certificate details, URL structure, and page layout to identify malicious website more effectively. Deep

learning approaches like CNN and LSTM are commonly used because they learn URL patterns and sequential text structures efficiently.

Phishing remains one of the dangerous cyber threats, and new phishing pages appear daily. Traditional rule-based systems fail because attackers constantly change URL patterns JavaScript code, and HTML layouts. Therefore, a deep learning-based system becomes essential to automatically adapt to new phishing attacks without manual feature updates.

A typical phishing detection pipeline include dataset collection, feature extraction, preprocessing, model training, and evaluation. The dataset may include the need for heavy feature engineering and learns meaningful representations directly from the data.

Experiment from recent research show that CNN-based phishing detectors achieve more than 95% accuracy, while hybrid models (CNN + LSTM) provide even better performance by learning both local patterns and long-term dependencies in URLs. And webpage content.

XI) REFERENCES

[1] Abdelhamid, N.,Ayesh, A.,& Thabtah, F. "*Phishing detection based on machine learning technique*," in *Neural Computing and Application,* International Journal of Information Security and Application,13, 165-173, 2017.

[2] Verma, R.,& Dyer, S, "*On the Characterization of Phishing Website Feature* ," in *eCrime Researches Summit, 2015 Computer Networks, 91, 84-96.*.

[3] Basnet, R., Sung, A.H., & Liu, Q., "*Rule-Based Phishing attack detection". Communications in information Science and Management Engineering*, 2012.

[4] Moghimi, M., & Varjani, A.Y., "*New Rule-Based Phishing Detection Method*,", Expert System with Application, 2016.

[5] Patel, A., & Pareek, P., "*Phishing Website Detection Using Deep Learning*.", International Journal of Engineering Research & Technology (IJERT), 2021.

[6] Rao, R, S., & Ali, S, T., "*A Computer Vision Approach for Detection Phishing Websites*,"

[7] Basit, A., Zafar, M., et AI. "*A Comparative Study of Machine Learning Techniques for Phishing Detection*", IEEE Access, 2020.

[8] Goodfellow, I., Bengio, Y., & Courville, A., "*Deep Learning MIT Press*", (Standard reference for deep learning fundamentals).

[9] LeCun, Y., Bengio, Y., & Hinton, G. "*Deep Learning*", Nature, 2015.

Basic format for periodicals:

[10] Mohammad, R.M., Thabtah, F., & McCluskey, L., "Intelligent rule-based phishing websites classification" *IET information Security, 2012.*

Examples:

[11] Li, X., Liu, B., & Liu, Y. "A Deep Learning-Based method for Phishing Website Detection," *IEEE Access*, 8 .47591-47601, 2020.

[12] Bahnsen, A.C., Torroledo, H., Camacho, J., & Villegas, S., "Deep Phish: Simulating Malicious AI," arXiv Preprint arXiv:1708.09586, 2017.

[13] Khonji, M., Iraqi,Y., & Jones, A., "Phishing detection: A literature Survey," IEEE Communication Surveys & Tutorials, 15(4), 2091-2121, 2013.

[14] Zhou, Y., & Evans, D., "Phishing attacks detected by antivirus software,", LEET, 2011

[15] Zhang, Y., Hong, J.I., & Cranor, L.F. "A content-based approach to detecting phishing websites," Preceeding of the 16th International Conference on World Wide Web, 639-648, 2007.

[16] Dinesh, K.S., & Thomas, J., "Phishing URL Detection using BERT and Neural Networks," Procedia Computer Science, 185, 442-449, 2021.

[17] *UCI Phishing Websites Dataset, https://archive.ics.edu/ml/dataset/phishing+website*

[18] *PhishTank, (Community-driven phishing feed) https://www.phistank.com.*

[19] *OpenPhish, (Automated real-time phishing threat feed) https://www.openphish.com.*

[20] *Alexa Top Sites, (Legitimate URL collection) https://www.alexa.com/topsites (Archived).*

[21] Islam, M.S., et AI, *Phishing Detection using Learning with Embedded feature information, 11(3), 132., 2020*