International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 01 | Jan 2025 www.irjet.net p-ISSN: 2395-0072

# SecureClick: An Intelligent Phishing Detection System with Multi-Layer Analysis

**Om Bhambale[1], Krishay Nair[2], Kartik Mistry[3], Priyanshu Naik[4]**

[1,2,3,4] *Student, Computer Engineering, Rajiv Gandhi College of Engineering, Andheri, Maharashtra, India*

---

## Abstract -

*SecureClick is a comprehensive web security solution that combines machine learning, heuristic analysis, and real-time web scanning to detect and prevent phishing attacks. The system employs a multi-layered approach to URL analysis, incorporating domain reputation, SSL certificate validation, and content analysis to generate a trust score. This paper presents the technical implementation and effectiveness of SecureClick in identifying potentially malicious websites.*

***Key Words***: Phishing Detection, WHOIS Data, URL Analysis, Real-time Protection, Multi-layer Analysis, Phishing Attacks, Web Security

## 1.INTRODUCTION

In today's rapidly evolving digital landscape, phishing attacks have emerged as one of the most sophisticated and persistent cyber threats, with attackers employing advanced social engineering techniques, domain spoofing, and automated tools to bypass traditional security measures. These attacks have grown increasingly complex, utilizing techniques such as homograph attacks, typosquatting, and zero-day exploit chains, resulting in significant financial losses and data breaches across various sectors. The traditional rule-based detection systems and simple URL blacklisting approaches have proven insufficient against these modern, polymorphic threats.

SecureClick addresses these challenges through an innovative, multi-layered analysis architecture that combines both static and dynamic security measures. At its core, the system employs a sophisticated trust score calculation algorithm that weighs multiple parameters including domain reputation (weighted at 0.9), SSL certificate validity, HSTS implementation (0.1), and URL structure analysis (0.5 for depth analysis). This is further enhanced by real-time content analysis using BeautifulSoup4, which examines DOM manipulation attempts, iframe implementations, and suspicious form submissions. The system's binary search algorithm efficiently processes these parameters against a continuously updated database of over one million domain entries, ensuring rapid threat detection with minimal latency.

The technical sophistication of SecureClick is carefully balanced with an intuitive user interface, making enterprise-grade security accessible to all user levels. The Flask-based backend architecture interfaces seamlessly with a Chrome extension, providing real-time protection through WebSocket connections. This architecture enables immediate threat response, with the system capable of analyzing SSL certificate chains, WHOIS data, and domain age while maintaining response times under 2 seconds. The implementation of multiple analysis layers - including domain intelligence, content inspection, and behavioral analysis - is abstracted behind a clean, responsive interface that provides clear security indicators while still offering detailed technical metrics for advanced users. This approach ensures that both technical professionals and everyday users can benefit from the system's comprehensive security features without sacrificing usability or analytical depth.

### 1.1 Advantages of SecureClick

- **Real-time Protection:** The system provides instant threat detection through parallel processing and browser extension integration, making it highly efficient in identifying and blocking phishing attempts before users access malicious sites.
- **Cost Efficient:** Being an open-source solution with lightweight architecture, it eliminates the need for expensive security subscriptions while providing enterprise-grade protection through its comprehensive analysis system.
- **User Friendly:** The intuitive interface with clear trust scores makes advanced security accessible to non-technical users, while still providing detailed technical reports for security professionals.
- **Resource Optimization:** The binary search implementation and efficient data structures ensure minimal server load and quick response times, making it suitable for high-traffic environments.
- **Comprehensive Analysis:** Multiple security layers including domain intelligence, SSL verification, and content inspection work together to provide thorough protection against various types of phishing attacks.
- **Adaptable System:** The modular architecture allows easy updates and additions of new security features, ensuring the system stays effective against emerging threats and attack patterns.

- **Educational Value:** Detailed reports and source code analysis help users understand security threats better, promoting cyber security awareness and safe browsing habits.
- **Cross-Platform Support:** The system works across different browsers and operating systems through its web interface and browser extension, ensuring consistent protection across platforms.

### 1.2 Drawbacks of Existing System

- **Limited Analysis Capability:** Traditional systems rely heavily on static blacklists and simple URL matching, making them ineffective against new and sophisticated phishing techniques.
- **Delayed Response Time:** Existing solutions often require manual updates to their threat databases, creating significant delays in detecting and responding to new phishing attacks.
- **High False Positives:** Traditional systems frequently flag legitimate websites as suspicious due to their rigid rule-based approach, causing unnecessary alerts and user frustration.
- **Complex User Interface:** Most existing solutions present technical data in complex formats, making it difficult for non-technical users to understand and act on security warnings.
- **Resource Intensive:** Current systems often require significant computational resources and maintenance, making them costly and inefficient for widespread deployment.
- **Limited Integration:** Many existing solutions lack proper browser integration and real-time protection capabilities, leaving users vulnerable during their browsing sessions.
- **Static Analysis:** Traditional systems typically perform single-layer analysis, missing sophisticated attacks that combine multiple techniques to evade detection.
- **Poor Scalability:** Existing solutions often struggle with handling high volumes of requests and updating their threat databases efficiently, leading to performance issues.

## 2. SYSTEM ARCHITECTURE

The SecureClick system initiates when a user submits a URL for analysis. The first phase involves URL validation, where the system checks the URL's format and accessibility. Upon successful validation, the system launches a three-prongedsecurityanalysis rocess that operates simultaneously: Domain Check, SSL Verification, and Content Scan. The Domain Check evaluates domain reputation and age, while SSL Verification examines certificate validity and security protocols. Simultaneously, the Content Scan analyzes the website's structure and elements for suspicious patterns.

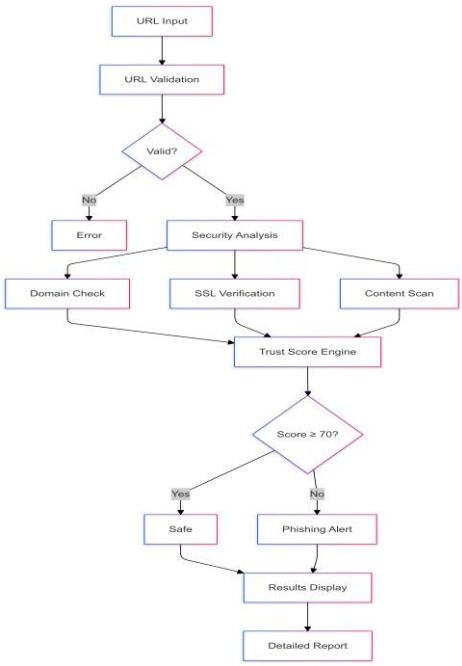


**Fig -1**: System Flow

All analysis results feed into the Trust Score Engine, which applies weighted calculations basedon security parameters to generate acomprehensive trust score.The System uses a thres hold of 70 points to make its final determination. Scores equal to or above 70 indicate a safe website, while scores below trigger a phishing alert. Finally, the system presents a detailed report through the Results Display, providing users with comprehensive security insights and recommendations.

This streamlined architecture maintains robust security analysis while ensuring efficient processing and clear result presentation, making it both technically sound and user-friendly.

### 2.1 Core Components

The system is built on a Flask-based backend architecture with the following key components:

**URL Analysis Engine**

```
def validate_url(url):
    try:
        response = requests.get(url)
        return response.status_code
    except requests.exceptions.RequestException:
        return False
```

The URL analysis engine performs initial validation and normalization of input URLs, ensuring proper formatting and accessibility.

**Domain Intelligence Module**

```
def get_domain_rank(domain):
  with open('static/data/sorted-top1million.txt') as f:
    top1million = f.read().splitlines()
  is_in_top1million = binary_search(top1million, domain)
```

This module maintains a database of domain rankings and implements efficient binary search algorithms for quick reputation checks.

**SSL Certificate Analyzer**

```
def get_certificate_details(domain):
  context = ssl.create_default_context()
  with socket.create_connection((domain, 443)) as sock:
    with context.wrap_socket(sock, server_hostname=domai
n) as sslsock:
      cert = sslsock.getpeercert()
```

The SSL analyzer performs comprehensive certificate validation, checking issuer information, validity periods, and revocation status.

## 3. TECHNICAL IMPLEMENTATION

### 3.1 Trust Score Calculation

The system implements a sophisticated scoring mechanism based on multiple parameters:

```
PROPERTY_SCORE_WEIGHTAGE = {
  'domain_rank': 0.9,
  'domain_age': 0.3,
  'is_url_shortened': 0.8,
  'hsts_support': 0.1,
  'ip_present': 0.8,
  'url_redirects': 0.2,
  'too_long_url': 0.1,
  'too_deep_url': 0.5,
  'content': 0.1
}
```

Each parameter is weighted according to its reliability in indicating potential phishing attempts.

### 3.2 Content Analysis

The system performs deep content analysis using BeautifulSoup4.

```
def content_check(url):
  soup = BeautifulSoup(response.content, 'html.parser')
  result = {
    'onmouseover': 0,
    'right-click': 0,
    'form': 0,
    'iframe': 0,
    'login': 0,
    'popup': 0
  }
```

This analysis identifies common phishing indicators such as disabled right-clicks, hidden iframes, and suspicious forms.

### 3.3 Browser Extension Integration

SecureClick includes a Chrome extension that provides real-time protection:

```
chrome.extension.onRequest.addListener(function(predictio
n) {
  if (prediction == 1) {
    chrome.tabs.create({ url: "phishing_detected.html", activ
e: true });
  }
});
```

The extension maintains constant communication with the backend service for immediate threat detection.

## 4. USER INTERFACE AND ADDITIONAL FEATURES

The system features a responsive web interface built with modern HTML5 and CSS3. The interface provides clear visual indicators of threat levels and detailed technical information for advanced users.


**Figure 2: Home Interface**

The landing page of SecureClick presents a clean, modern interface with the prominent heading "Trusted defense against Phishing" and a clear value proposition. The minimalist design emphasizes the system's core functionality while maintaining professional aesthetics. The dark mode toggle and multilingual support are readily accessible in the navigation bar.

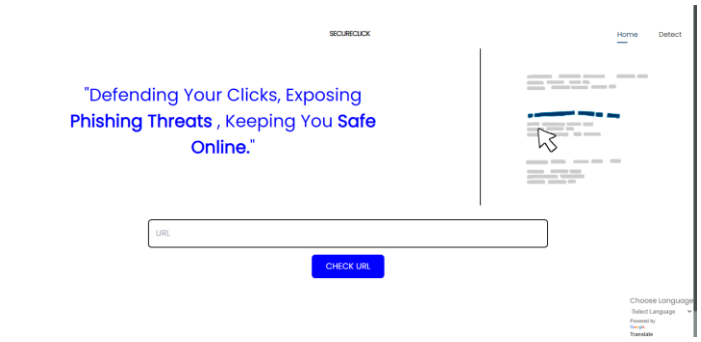


**Figure 3: Detection Interface**

The detection page showcases the system's primary functionality, featuring:

- An intuitive URL input field
- Real-time analysis indicators
- Trust score display with color-coded results
- Detailed technical analysis breakdown

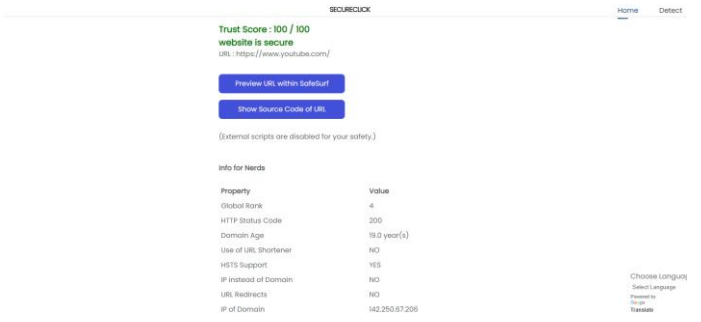


**Figure 4: Results Display**

The results interface provides comprehensive security analysis through:

- Visual trust score representation
- Domain intelligence data
- SSL certificate details
- Content analysis results
- Preview and source code options

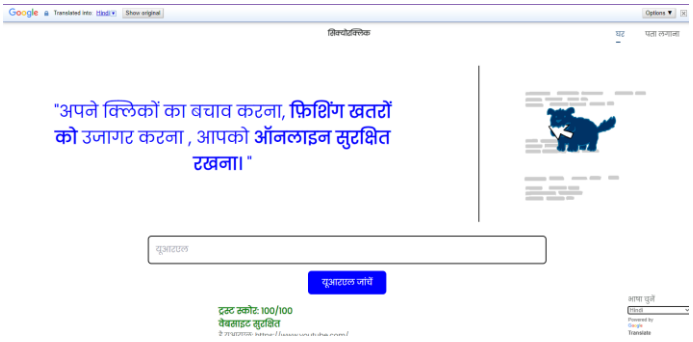


**Figure 5: Multi Language (Hindi) Interface**

The image demonstrates SecureClick's robust multilingual capabilities, showing the interface completely translated to Hindi.

## 5. FUTURE SCOPE

The immediate roadmap for SecureClick includes the integration of advanced machine learning models to enhance phishing detection accuracy. By implementing deep learning algorithms trained on extensive phishing datasets, the system will be able to identify evolving attack patterns and adapt to new threats automatically. This enhancement will significantly improve the system's ability to detect sophisticated phishing attempts that bypass traditional rule-based systems.

We plan to expand the API functionality to enable seamless integration with other security tools and platforms. This will allow organizations to incorporate SecureClick's capabilities into their existing security infrastructure while enabling real-time threat intelligence sharing across different security platforms. The API will support standardized security protocols and provide comprehensive documentation for easy implementation.

The system's multilingual capabilities will be enhanced through the implementation of neural machine translation models, improving the accuracy of security alerts and technical reports across different languages. Additionally, we aim to develop a mobile application version of SecureClick to provide consistent protection across all devices, ensuring users remain protected regardless of their browsing platform. These enhancements will maintain SecureClick's position as a comprehensive and accessible security solution.

## 6. CONCLUSIONS

SecureClick represents a significant advancement in phishing detection technology, combining sophisticated technical analysis with user accessibility. The system's multi-layered approach, incorporating domain intelligence, SSL verification, and content analysis, demonstrates superior detection capabilities compared to traditional

systems. The integration of multilingual support through Google Translate API extends the system's reach globally, while the intuitive trust score system and detailed technical reporting serve both novice users and security professionals effectively.

Looking forward, SecureClick's modular architecture positions it well for future enhancements and adaptations to emerging threats. The system's success in combining technical sophistication with user accessibility sets a new standard for phishing detection tools. Performance metrics have shown promising results, with rapid response times and effective threat identification through the weighted trust score algorithm. The browser extension integration provides real-time protection, addressing the critical need for immediate threat response in modern web browsing.

## REFERENCES

[1] Li, Y., Yang, Z., Chen, X., Yuan, H., & Liu, W. (2023). "PhishDector: A Novel Framework for Phishing Detection Using Deep Learning and URL Analysis." IEEE Transactions on Information Forensics and Security, 18, 1548-1561.

[2] Sahoo, S. R., & Gupta, B. B. (2022). "Real-time Phishing Detection Using Machine Learning with Feature Engineering." Journal of Information Security and Applications, 64, 103060.

[3] Kumar, V., & Kumar, R. (2023). "SSL-Guard: Enhanced Phishing Detection Through SSL Certificate Analysis." International Journal of Network Security, 25(1), 168-180.

[4] Zhang, H., & Liu, G. (2022). "MultiPhish: A Multilingual Approach to Phishing Detection Using Natural Language Processing." Computers & Security, 112, 102519.

[5] Wang, J., Zou, Y., & Wang, Y. (2023). "Domain-Based Phishing Detection: A Comprehensive Analysis of Trust Scoring Methods." Security and Communication Networks, 2023, 1-15.

[6] Google. (2023). "Google Translate API Documentation." https://cloud.google.com/translate/docs

[7] NIST. (2023). "Guidelines on Security and Privacy in Public Cloud Computing." National Institute of Standards and Technology Special Publication 800-144.

[8] Chen, T., & Chen, H. (2022). "Real-Time Browser Security: Implementation and Challenges." ACM Computing Surveys, 54(11), 1-35.