Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Detect Malicious URL Based on the Multi Social Media Application

Mrs P Anuja[1], Madhan Kumar S[2]

[1]Assistant Professor, [2]Bsc Computer Science

[1,2]School of Sciences and Allied Health Science, Jeppiaar University, Tamil Nadu, Chennai - 600119

Abstract:

Due to the fast development of social media sites, web links are being exchanged at a high rate among the users. As much as these platforms offer a convenient process of communicating and in exchanging information, they equally make attackers to avail avenues of spreading malicious URLs. These malicious links can send the users to phishing sites, viruses, or other deceitful applications that cause critical privacy and security threats. The problem of malicious URLs in the social media environment has therefore become a major cyber security issue.

This research paper provides a framework that will be employed in identifying the presence of malicious URLs that have been shared with the help of several social media applications. Such system can examine various textual attributes of the web pages including the redirection behavior, Iframe usage and suspicious link structures of the web pages to establish malicious and legitimate web URLs. The methods of classification, i. e. Hidden Markov Model and correlation-based analysis are used in improving the accuracy of detection. The system has administrative monitors and user interaction modules that facilitate the detection of suspicious URLs and blocking them before they can cause impact on the users.

The suggested strategy may be a decent method of categorizing URLs and securing the social media environment, just as it has been experimentally discovered. The system aids in enforcing online communication between the users as they will not be exposed to malicious links and are less prone to cyber-attacks within the social network sites.

Keywords: Malicious URL Detection, Social Media security, Web Application security, Hidden Markov Model, Cyber security, URL Classification, Online threat detection.

I. INTRODUCTION

The modern online world has become one of the most frequented means of communication that is utilized via the social media. The social networks such as facebook, twitter, and whatsapp allow the users to share information, pictures, videos and web links in real time with a very large number of users. Although such platforms facilitate the communication process and the sharing of information is easy, they still provide the attackers with the opportunity to disseminate malicious information through URLs in the posts, messages, or comments. When users make such links they are redirected to phishing websites, malware download pages or other fraudulent applications which commit privacy and security breach to the user.

The bad URL is the address of the web site, which opens a harmful or fraudulent web page that is located to steal personal information, viruses and unverified capabilities. The social network and online communication have grown extremely rapidly such that the malicious links have disseminated and the users are struggling to distinguish between the credible and malicious URLs. This is why the problem of identifying malicious URLs is a research problem that has become relevant in the context of cybersecurity [1].The traditional security system is a mostly blacklist-based system of identifying the suspicious web content, in which the list of the malicious web addresses is stored in the databases and blocked every time any of the users attempts to open them. Security services such as Google safe browsing involve a huge

database so as to warn a user on unsafe websites. However, blacklist methods are very weak because they do not find new malicious URLs that are not yet reported or detained in the database. In order to avoid these detection mechanisms, the attackers are inclined to modify the format of the URLs and consequently the traditional security measures are turned out to be ineffective [2].

To help overcome these shortcomings, researchers have offered alternative machine learning strategies in order to detect malicious URLs. These techniques look into such aspects of URL as domain, lexical, page, and hyperlink patterns. By training machine learning algorithms on labelled datasets, they can be trained to be able to distinguish between malicious and benign URLs successfully. By investigating the learning-based approaches, J. Ma and his associates discovered that the learning-based means had the capacity to increase the detection accuracy significantly as compared to the conventional blacklist approaches [3].

In addition to the URL-based analysis, other scholars have included the malicious web page detection via script and webpage behavior analysis. Indicatively, M. Cova and his colleagues looked at the drive-by-download attacks and how malicious JavaScripts automatically download malicious programs on the system of the user without the owner being aware of it [4]. Similarly, a ruthless web scan by N. Provos showed that in many cases, hackers use muted iframe elements and redirection schemes to distribute malware using hijacked pages [5].

Although these developments took place, some of the existing malicious URL detection systems had been developed to operate in the legacy desktop web environment. The mobile web applications and social media sites often differ in the patterns of user interaction and layouts of the webpages as well as the structure of the webpages. Therefore, the conventional detection processes may not be useful within these environments. As a result of increasing popularity of mobile computing and the usage of the social networking apps, there is the need to develop those detection systems that are specifically oriented to the multi social media applications.

Throughout this paper, the author presents a recommendable system of identifying malicious URLs that are posted with the assistance of various social media applications. The proposed solution will explore the characteristics of webpages and the URL which can be taken to identify suspicious links and put them under either malicious or benign. The system will likely increase the security of the social media platforms and identify them more effectively with the help of such types of classification as Hidden Markov Model and correlation-based analysis. The specified system allows removing the access to hazardous web pages and makes the internet space of communication safer.

II. RELATED WORK

Online threat detection by detecting suspicious URLs and protecting users has become a valuable research field in the field of cybersecurity. Various research works have put forward various methods of detecting rogue sites and averting cyber attacks. It was one of the first fields where it was researched on the topic of trust and reputation systems that measure the reliability of users and services on the Internet. A survey of trust and reputation systems in online service settings provided by A. Josang, R. Ismail and C. Boyd, has shown that the trust evaluation can enhance security in the distributed systems [1].

Phishing detection is another noteworthy method of malicious websites detection. S. A phishing attack detection framework based on suspicious URL pattern analysis and web page properties analysis was suggested by Garera, N. Provos, M. Chew, and A. D. Rubin. In their work, they have shown that malicious websites can be detected through the analysis of structural properties of URLs [2].

Malicious URL detection has also been done extensively using machine learning techniques. J. Ma, L. K. Saul, S. Savage, and G. M. Voelker suggested a learning-based mechanism, which determines lexical properties of URLs to classify between malicious and benign websites. In their study, they were able to prove that machine learning models can be more accurate when detecting malicious users than conventional blacklist [3].

Likewise, M. Cova, C. Kruegel, and G. Vigna have researched on the topic of drive-by download attacks and malicious JavaScript code embedded in compromised web pages. Their contribution was dedicated to

the analysis of the web page content, the detection of suspicious scripts that can be automatically implemented on devices of users to install malware [4].

Large scale study of malicious web infrastructure has also been studied. N. Provos and his colleagues explored the evil web pages through attacks that were based on the use of iframe which redirected users to the malicious sites. Their research indicated the way in which attackers use concealed iframe components to execute web-based attacks [5].

Besides content-based analysis, reputation-based systems have also been suggested by a number of researchers to determine the trustworthiness in online environments. PeerTrust model that was proposed by L. Xiong and L. Liu is based on the feedback of the user interactions, which are used to compute trust scores of the online community participants [7]. Reputation systems can be used to recognize malicious agents based on the behavior and feedback pattern of the users.

Reputation systems are however susceptible to a number of attacks including the Sybil attacks and the collusion attacks. R. Douceur proposed a technique of the Sybil attack, a type of attack that involves a rogue user establishing numerous fake identities in order to control the system [8]. To counteract the challenge, S. Kamvar and his associates came up with an algorithm called EigenTrust which computes worldwide trust scores through transitive trust connections in distributed networks [9].

The impact of dishonest feedback on reputation systems has been explored further. C. The research by Dellarocas on the distortion of values of trust in an online system by false ratings and misleading feedback can be viewed as significant since the essay is about the significance of managing reputations in a reliable way [10]. More trust evaluation was achieved through Bayesian trust models which were presented by Y. Wang and J. Vassileva as it dealt with uncertainty of user feedback [11].

Trust management has emerged as a significant process of guaranteeing system security in the context of cloud computing and distributed systems. S. Pearson notes that cloud environments should be based on trust and that users have to trust service providers to keep their data safe and securely processed [12]. Later research by Q. He and colleagues suggested trust management models that deploy reputation systems to cloud services in order to make them more secure [13].

Detection of collusion attack in reputation systems has also been covered in other studies. J. Huang and his associates suggested the ways of identifying concerted malicious activity through rating similarity and interaction patterns among users [14]. Moreover, a study conducted by M. Li and other authors suggested the use of secure and trust-based data sharing infrastructure in the cloud, integrating trust assessment and data protection systems [15].

Despite numerous methods suggested to address the malicious URL detection and trust management, there are still a number of challenges. Most of the available solutions are centered around standard web environments and fail to recognize the spread of malicious links among the social media. Consequently, effective detection systems are required that can be used to detect malicious URLs posted on a variety of social media apps. The suggested system will overcome this difficulty by integrating URL feature analysis and classification methodologies to enhance the detection of malicious links in the social media settings.

III. PROPOSED SYSTEM MODEL

A. System Overview

1) General Description

The proposed system can provide a secure system of detecting malicious URLs that are shared in different social media platforms.

Marked as malicious web links that are likely to result in phishing websites, downloading malware, or suspicious online services are what the system is targeting.

Checking the features of URLs and webpage behaviour unlike the traditional blacklist detection model the proposed model checks on malicious links that are not known before.

By applying the machine learning and classifications techniques as well as a feature examination, the system can distinguish legitimate or possibly malicious URLs.

The system is under the control of a central administrative unit to ensure that there is an efficiency to check suspicious activity and adequate detection of harmful URLs.

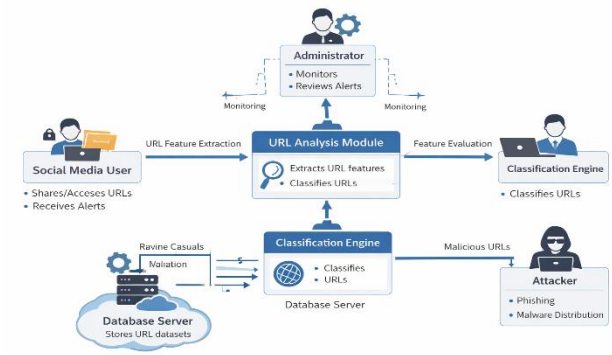

Fig. 1. General Architecture of the Suggested Malicious URL Detection System.

2) Intended Uses of the Proposed System.

- To detect malicious URLs which are being broadcasted by the social media.
- To investigate webpage features and URLs structure in order to find the threats.
- To prevent access of users to dangerous web sites.
- To make the security awareness and protect users against cyber attacks.
- To possess an effective and automated malicious URL detecting.

B. System Architecture

1) Major System Entities

i. Social Media User (End User)

- Logs in and registers with the system.
- Clicks or browses on the site.
- Pop-ups on suspected URLs.

ii. URL Analysis Module

- Fishes out various properties in the URL given.
- There exist structural properties, which are examined such as domain name, length of path, and special characters.
- Identifies the malicious URLs with the suspicious patterns.

iii. Classification Engine

- Makes use of machine learning in the categorization of URLs.
- Displays a distinction of a legitimate and malicious URL.
- Training sets increase the accuracy of detection.

iv. Administrator

- Observes the activity and detection of the systems.
- Scans suspect URLs and authenticates the threat information.
- Setting of system settings and updates rules.

v. Database Server

- Registering of user information is done in the stores.
- Has bad and good URLs lists.
- Activity and detection output of logs are recorded.

C. Threat Model

1) Considered Attacks

Phishing Attack

- Hackers have invented fake websites that steal crucial information such as password and money.
- The malicious URLs will redirect the customer to counterfeit sites imitating the authentic sites.
- Reproduction: Attack Malware.
- The hackers take advantage of the names of URLs that automatically download malicious programs.
- South: The files can destroy the systems of the users or steal their sensitive data.

URL Obfuscation Attack

- Alterations of URLs are made by attackers using special characters, encoding or misleading domain names.
- Such tricks make bad URLs appear to be true to the users.

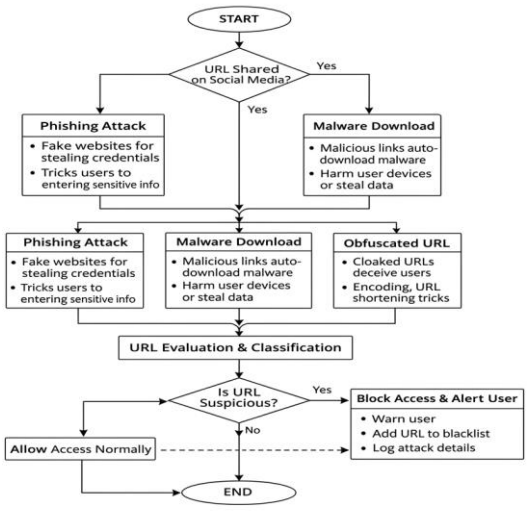

Fig. 2. Example of Threat Model to Malicious URL Attacks

Security Goals

- So as to detect the suspicious web addresses even prior to the user clicking.
- So as to protect the users against phishing and malware.
- In order to improve security and reliability of communication on social media.
- URL Feature Evaluation Model.
  - URL Analysis Parameters
- Lexical Features (LF)
  - Researches the text structure of the URL.
  - This is URL length, special characters and domain properties number.
- Host-Based Features (HF)
  - Checks registration of domains and hosting.
  - Determines suspicious new or registered domains.
- Webpage Content Features (CF)
- Webpage analysis i.e. analysis of iframes, scripts and redirection patterns.
- Determines malicious content in the webpages.

2) Equation of URL Classification.

Total bad score of a URL =:

$$MS = \alpha \times LF + \beta \times HF + \gamma \times CF \quad (1)$$

Where:

- α, β, γ are weighting parameters
- $\alpha + \beta + \gamma = 1$

3) Decision Rule

A URL will be malicious as follows:

$$MS \geq T\_url \quad (2)$$

Where

Turl is the wicked gateway which is preprogrammed.

D. System Workflow

1) Registration and Authentication of the user.
- Registration information is given by the user.
- Credential check is done in the system.
- An account is created safely to the user.

2) URL Submission and Features Extraction.
- A URL is sent by the user to analyse.
- These are systems which are extracted and they extract URL features.
- Suspect characteristics are ascertained.

3) URL Classification Flow
- Features received are sent to the classification engine.
- The malicious score is measured in the system.
- URL is classified as a malicious or legitimate one.

4) Alert and Reporting Flow
- The system informs the user in case a malicious URL is detected.
- The malicious database is fed with the URL.
- The administrator takes into account the threat report.

E. Role of Administrator in the Monitoring of the Systems.

1) Monitoring Activities
- Checks the emergence of detection and suspicious URLs.
- Identifies new malicious links of patterns.
- Maintains security records in the system.

2) Enforcement Actions
- Blocks identified questionable URLs.
- Updates detection datasets.
- Prepares security and system performance-based reports.

IV. MALICIOUS URL DETECTION ALGORITHM

A. URL Initialization

1) URL Input and Preprocessing
- In case a user shares or passes a URL in the system, it is first picked by the detection module.
- Preprocessing is done to normalize the URL structure by the system.
- Preprocessing eliminates the redundant characters and drives out the base domain information.

2) URL Normalization

i. The normalized URL may take the form:

U = Normalize(URL) (3)

ii. Normalization is used to process the URLs in the same format to be analyzed.

B. Feature Extraction Model

1) URL Feature Components

i. Lexical Features (LF)

- Taken directly off the text of the URLs.
- Encompasses URL length, special characters and questionable keywords.

ii. Host-Based Features (HF)

- Based on details of domain registration.
- Has domain age, DNS data and IP address reputation.

iii. Content-Based Features (CF)

- Taken out of webpage format.
- Also contains the use of iframe, JavaScript action behavior, and redirection pattern behavior.

C. Computation of Malicious Score.

Assuming that the sum total of transactions is P and that no policy-maker has unlimited power, the malicious score is calculated below:

i. The weighted feature model is used to calculate the malicious score of an URL:

$MS = \alpha \times LF + \beta \times HF + \gamma \times CF$ (4)

ii. Where:

Where 1, 2, 3 are weighting parameters.

- $\alpha + \beta + \gamma = 1$

1) Score Interpretation

- Furthermore, MS value near 0 implies a valid URL.
- MS close to 1 implies a very suspicious or malicious URL.

D. URL Classification Decision.

1) Threshold-Based Detection

i. A URL is considered to be malicious in case:

$MS \geq T\_url$ (5)

ii. Where Turl is the threshold of malicious detection.

2) Detection Outcome

- In case the URL is valid, it is permitted to access.
- In case of a malicious URL, the system blocks the access and gives an alert to the user.

E. URL Detection Algorithm (Pseudocode Account)

Algorithms: Malicious URL Detection.

- Input:URL
- PerformURL normalization
- Extract lexical features (LF)
- Host-based features (HF) extraction.
- Simple content-based features (CF) extraction.
- Compute malicious score MS

If $MS \geq T\_url$ then

i. Mark URL as malicious

ii. Block URL access

iii. Alert user and log event

Else
iv. Allow access to the URL

- Analysis result of store URL to database.
- End

F. Detective Performance Graphically.

G.

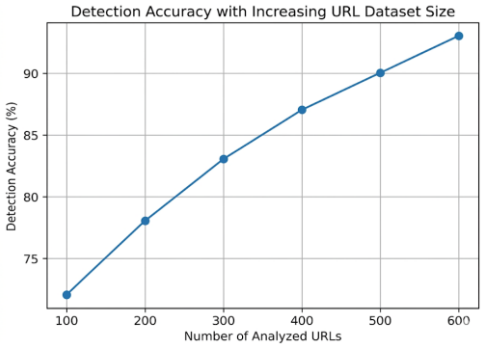

Fig. 3. Accuracy of Detection Size of URL Database.

The first table (Detection Accuracy vs Number of URLs) indicates that the detection accuracy continues to rise with the increase in the number of URLs.

- X-axis: The number of analyzed URLs.
- Y-axis: Detection accuracy

The more training URLs one has, the higher the detection accuracy.

1) Wicked Score Dissemination.

- X-axis: URL samples
- Y-axis: Malicious score
- Valid URLs have low scores.

Score is greater in malicious URLs.

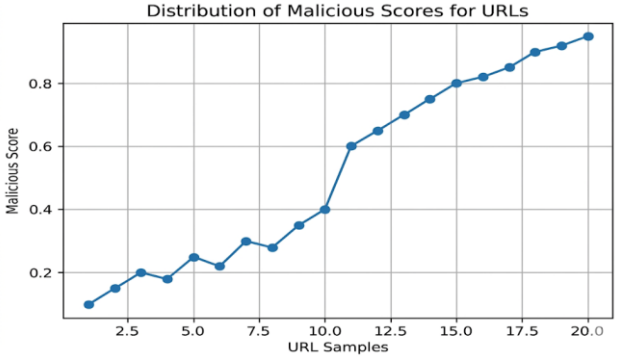

Fig. 4. The Malicious scores of URLs are distributed.

2) Detection Rate Threshold Value.

- X-axis: Threshold value
- Y-axis: Detection rate

False positives are minimized by higher thresholds.
Lower thresholds are useful in enhancing sensitivity in detection.

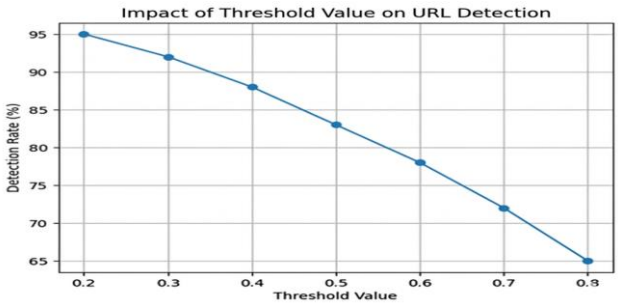

Fig. 5. Effects of Threshold Value on URL Detection.

V. MALICIOUS URL ATTACK DETECTION MECHANISMS

Bad URLs may be shared fast within the social media environments, and may be of high level of security risks to the social media users. The attackers are in a position to easily use deceptive techniques to transmit malicious links that might lead to phishing sites, downloaded malware or dishonest contents. The real system proposed of the malicious URL detection is a system that encompasses different detection systems to identify and prevent the attacks. Such systems scan URL attributes, webpage patterns, as well as user behavior patterns to come up with a flawless threat detection.

Table 1 Detection plan and Malicious URL Attack Variants.

Type of attack	Explanation of attack	Detection Strategy
Phishing Attack	Fraud Web sites to steal user credentials	Analysis of URLs and verification of domain names.
Malware Distribution	This is URLs that download malicious software automatically	Webpage content and script analysis.
URL Obfuscation	Malicious URLs are concealed by means of URL encoding or shortening.	
URL redirection Attack	Web addresses redirect to malware sites	Redirection chain monitoring

A. Phishing URL Detection

Phishing: These attacks target users to steal their sensitive information such as log-in accounts or other financial information. The proposed system detects the phishing URL during a number of verification.
Domain Verification: The system tests whether the domain name is similar to the well-known legitimate web sites.
URL Pattern Analysis: The patterns that are suspicious such as the excessive use of sub domains or misleading keywords are obtained.

B. Malware URL Detection

Fraudulent sites are capable of automatically downloading bad programs on the computers of the users. The system picks up such threats by examining the activity of the webpages.
The JavaScripts or embedded scripts that are considered suspicious are those with possible malware applications.

File Download Monitoring: The automatic file downloading activities which are related to unknown sources are detected and blocked.

C. URL Obfuscation Detection

The hackers normally camouflage the rogue URLs so that they can appear genuine.
URL Decoding: the URLs are coded and then decoded and evaluated on the suspicious patterns.
Shortened Url Expansion: The system will expand shortened URLs and display its destination before categorization.

D. Chain Analysis Redirection.

In some cases, malicious web addresses redirect the users after sifting through several intermediate pages to the real malicious web site.
Redirection Tracking: The system maintains a record of all the redirection so as to identify problem areas.
Destination Check: URL is blocked in the event that the end destination domain is malicious.

E. Adaptive Monitoring and Alert Mechanism.

Real-time Notifications: A system logs the user in real-time, in case a suspicious URL has been detected.
Database Update: Detected malicious URL is written in the t/he database to prevent future access.
Administrative Monitoring: The administrator browses the suspicious URLs and adjusts rules of detection.
Such detection systems enhance efficiency of the malicious URL detection system and they can be deployed to prevent cyber attacks within the social media contexts. By combining feature analysis, classification algorithms, and behavioral monitoring, the system is able to provide an exceptionally effective protection against phishing, malware distribution, and any other attacks on malicious URL.

VI. CONCLUSION AND FUTURE WORK

The given article presents a bad URL detector application, which is designed to make the multi social media applications more secure. With the online communication platforms evolving at a high pace, the malicious links have also become a major threat to the users since they are capable of establishing phishing attacks, malware, and other forms of cyber threats. The proposed system operates on the principle of URL format analysis, webpage features and behavioral patterns with the purpose to properly classify URLs as being both legitimate and malicious.
The system integrates the feature extraction techniques, with the classification algorithms which detect the suspicious links, which are posted in the social media sites. Host based and content based features can also be studied by the system and therefore the malicious URLs can be detected before the user logs on to the detrimental web pages. Monitoring and alert are also present in the detection system where the user is alerted that the link can be regarded as dangerous. Based on experimental research, the proposed model improves the precision of detection, yet harms the opportunities of phishing and malware attacks in the context of social media.
The malicious URL detection system will be scaled and enhanced to the next level in the next part of work.

The following are the proposed directions in the research:

- Connection to the Real-Time Social Media Platforms: The system can be further extended to feature direct connection with such applications used in the social networks, and messaging to monitor shared URLs in real-time.
- Machine Learning and Deep Learning Models: Advanced machine learning models such as deep neural networks can be employed so as to increase the accuracy and flexibility of the malicious URL detection.

• Real-Time Threat Intelligence Integration: Threat feeds and world databases of security information would be useful to add to the system in order to detect malicious URLs that have happened recently.

User Awareness and Security Notifications: Future systems will have a better user notification system and security awareness systems that will help the user to realize that suspicious links are there and avoid clicking them.
Overall, the proposed system of the malicious URL detector is a solution that can bring the improved cybersecurity to the social media space. The system can be applied in secure online communication and guarding of the users against the new web-based threats through a mixture of automated detection and active monitoring.

REFERENCES:

[1] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.
[2] S. Garera, N. Provos, M. Chew, and A. D. Rubin, "A framework for detection and measurement of phishing attacks," in *Proceedings of the ACM Workshop on Rapid Malcode*, 2007, pp. 1–8.
[3] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: Learning to detect malicious web sites from suspicious URLs," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2009, pp. 1245–1254.
[4] M. Cova, C. Kruegel, and G. Vigna, "Detection and analysis of drive-by-download attacks and malicious JavaScript code," in *Proceedings of the International World Wide Web Conference*, 2010, pp. 281–290.
[5] N. Provos, P. Mavrommatis, M. Rajab, and F. Monrose, "All your iFRAMEs point to us," in *USENIX Security Symposium*, 2008.
[6] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and evaluation of a real-time URL spam filtering service," in *IEEE Symposium on Security and Privacy*, 2011.
[7] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843–857, 2004.
[8] R. Douceur, "The Sybil attack," in *International Workshop on Peer-to-Peer Systems*, 2002.
[9] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in peer-to-peer networks," in *International World Wide Web Conference*, 2003.
[10] C. Dellarocas, "The digitization of word-of-mouth: Promise and challenges of online feedback mechanisms," *Management Science*, vol. 49, no. 10, pp. 1407–1424, 2003.
[11] Y. Wang and J. Vassileva, "Bayesian network-based trust model in peer-to-peer networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 9, pp. 1247–1259, 2007.
[12] S. Pearson, "Taking account of privacy when designing cloud computing services," in *IEEE Cloud Computing Conference*, 2009.
[13] Q. He, J. Yan, and H. Jin, "Trust management in cloud computing," *IEEE Transactions on Cloud Computing*, 2014.
[14] J. Huang, S. Wang, and X. Zhang, "Detecting collusion attacks in online reputation systems," *Journal of Computer Security*, 2011.