Feature-Rich URL Shortner

Pranav Karande, Krishap S Sreenivasan, Tejas Mahajan, Utkarsh Tikkiwal

VIT, Vellore Campus, Tiruvalam Rd, Katpadi, Vellore, Tamil Nadu 632014

Abstract

URLs can get long, unattractive, and break when sent via e-mail. To shorten an Internet address, we proposed a secure URL shortening service which will take a long Web address and create a shorter address. Most of the approaches proposed for classifying malicious URLs utilize information from both social networks and URL shorting service providers. In this paper, we propose a novel approach to detect malicious short URLs by focussing on outliers in existing implementations. This is achieved by taking user feedback into account.

Keywords:
URL shortner, Spam Detection, User Feedback, Cassandra, PostgreSQL

1. Introduction

URL shortening is a technique that allows you to significantly shorten your Uniform Resource Locator (URL) and still access the desired page directly. This is achieved by using a redirect which links to the web page that has a long URL. The proposed secure URL shortening service will give the user more trust to use the service with security, availability, and confidentiality consideration. A shortened URL can be used in messaging technologies which limit the number of letters, for making it easier for one to remember it, for reducing the amount of typing if someone is manually copying the URL and can be used for permalinks So they save space and make manual entry of URL easier. Some URL shortening service providers are listed on spam block lists because their redirect services are used by websites trying to bypass spam block lists. Some URL shortening service providers have found themselves on spam blocklists, because of the use of their redirect services by sites trying to bypass those very same blocklists. Some popular websites like Twitter allow only 140-character tweet to be posted on their platform.

So given the limit on the length of the tweet URL shortener have become very popular method to share links on Twitter. A Popular URL shortening site is bit.ly which convert long URL into smaller ones. However, the technology has also attracted spammers. . They utilize the URL Shorteners to camouflage their spam links, enabling the spammers to hide the true domain of the URL. Our goal is to provide a safe URL shortening service that allows users to report malicious links that spread spam and malware in which we delete and block these shortened links and avoid the distribution of these inappropriate links which contain malware.

2. Related Work and Motivation

S.no	Title	Author(s)	Technique / Algo	Limitations / Conclusion
1	A Thesis / Project / Dissertation Report on URL SHORTENER	Kashish Saxena, Shubham Satyam Dubey	The proposed secure URL shortening service will give the user more trust to use the service with security, availability, and confidentiality consideration	Because shortened URLs are so short, they are vulnerable to brute-force scanning, meaning that attackers can guess multiple shortened URLs and read all of the working ones.
2	A URL Shortening Service Project	Rohit Sankhala, Manan Kharbanda, Ankit Yadav, Pardeep Suthar, Parampreet Kaur	The proposed URL shortening service will take the long URL link and gives a shorter link that will not break while sharing on social media platforms and also provides with the custom domain and by this we aim at user trust to use the service with availability.	1) Privacy breach 2) Dead links that is they become inaccessible after some time
3	Comparative Analysis of Malicious Detection of Short URLs from Tweets	Tareek Pattewar, Manish Wagh, Umesh Bisnariya, Lomesh Patil	Performed a comparative study of long and short Bitly URLs propagation on Twitter and found that Bitly links received orders of magnitude more clicks than an equal random set of long URLs	Many short URLs redirect the URLs to malicious content
4	Proposing a Secure URL Shortening Service by using Blackboard Architecture	Dr. Reem J. Ismail	An organization that constantly uses very long or complex URLs will often find that customers expect not to understand a URL provided to them in any electronic communication.	This short URL would be supplied by a third-party site and is used to obfuscate the true destination.

| S.no	Title	Author(s)	Technique / Algo	Limitations / Conclusion
1	You Look Suspicious!! : Leveraging Visible Attributes to Classify Malicious Short URLs on Twitter	Raj Kumar Nepali, Yong Wang	4 ML algorithms taking only visible features of tweets and user profiles as input: Naïve Bayes, random forest, support vector machine, and logistic regression and obtains an accuracy of up to 97%	1) Completely automated process, no consideration of user feedback 2) computationally intensive
2	Using URL Shorteners to Compare Phishing and Malware Attacks	Sophie Le Page, Guy-Vincent Jourdan, Gregor v. Bochmann, Jason Flood, Iosif-Viorel Onut	Uses URL shortener click analytics to compare the life cycle of phishing and malware attacks	1) phishing attacks have higher click through rate with shorter timespan 2) efforts against phishing attacks are stronger than the efforts against malware attacks
3	Measuring the Effectiveness of Twitter's URL Shortener (t.co) at Protecting Users from Phishing and Malware Attacks	Simon Bell, Peter Komisarczuk	Investigates Twitter's URL shortening service to examine the impact of filtering blacklisted URLs that are posted to the social network	1) Only about 12% of tweeted blacklisted URLs – which were not blocked at time of tweet and therefore posted to the platform – were blocked by Twitter in 2018-19. 2) Twitter's URL shortener is not particularly effective at filtering phishing and malware URLs
4	Deep Dive into Short URL based e-Crime Detection	Neha Gupta, Anupama Aggarwal, Ponnurangam Kumaraguru	This paper analyses malicious bitly links on OSM and discusses their spam detection technique which is not found efficient	A limited dataset is used from bitly.

S.no	Title	Author(s)	Technique / Algo	Limitations / Conclusion
1	A Thesis / Project / Dissertation Report on URL SHORTENER	Kashish Saxena, Shubham Satyam Dubey	The proposed secure URL shortening service will give the user more trust to use the service with security, availability, and confidentiality consideration	Because shortened URLs are so short, they are vulnerable to brute-force scanning, meaning that attackers can guess multiple shortened URLs and read all of the working ones.
2	A URL Shortening Service Project	Rohit Sankhala, Manan Kharbanda, Ankit Yadav, Pardeep Suthar, Parampreet Kaur	The proposed URL shortening service will take the long URL link and gives a shorter link that will not break while sharing on social media platforms and also provides with the custom domain and by this we aim at user trust to use the service with availability.	1) Privacy breach 2) Dead links that is they become inaccessible after some time
3	Comparative Analysis of Malicious Detection of Short URLs from Tweets	Tareek Pattewar, Manish Wagh, Umesh Bisnariya, Lomesh Patil	Performed a comparative study of long and short Bitly URLs propagation on Twitter and found that Bitly links received orders of magnitude more clicks than an equal random set of long URLs	Many short URLs redirect the URLs to malicious content
4	Proposing a Secure URL Shortening Service by using Blackboard Architecture	Dr. Reem J. Ismail	An organization that constantly uses very long or complex URLs will often find that customers expect not to understand a URL provided to them in any electronic communication.	This short URL would be supplied by a third-party site and is used to obfuscate the true destination.

43

S.no	Title	Author(s)	Technique / Algo	Limitations / Conclusion
1	Modelling Replication in NoSQL Datastores	Rasha Osman and Pietro Piazzolla	Goes into setting up replication in cassandra and running performance evaluations on the cluster	Cassandra works well with use cases with more writes and less reads.
2	Cassandra as a Big data Modeling Methodology for Distributed Database System	Dr. Kalpesh U. Gundigara Ms. Vibha H. Mehta	Goes into detail about the methodologies used to enter and retrieve data from a nosql database like cassandra	Cassandra works well in cases with that require lots of scaling
3	Security Threats of URL Shortening: A User's Perspective	Nhien-An Le-Khac and M. Tahar Kechad	This paper covers existing knowledge gap compiles a baseline assessment on the frequency of use, user confidence and user awareness when utilizing short URLs	Analysis was done on few people only (100 people).

44

3. ER Diagram
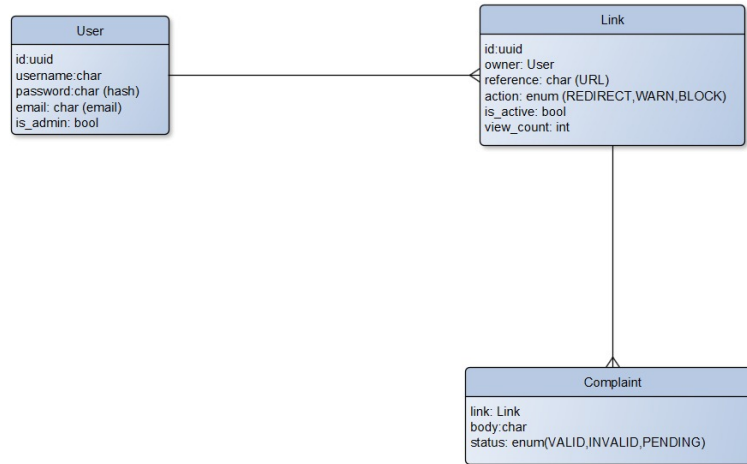
4. SQL Queries

4.1. PostgreSQL

4.1.1. User Login SQL command

SELECT users.id AS users_id, users.username AS users_username, users.email AS users_email, users.hashed_password AS users_hashed_password, users.is_active AS users_is_active, users.is_admin AS users_is_admin

4.1.2. Register User SQL command

INSERT INTO users (username, email, hashed_password, is_active, is_admin) VALUES (%(username)s, %(email)s, %(hashed_password)s, %(is_active)s, %(is_admin)s) RETURNING users.id

4.1.3. Create Complaint

INSERT INTO complaints (link_id, body, status) VALUES (%(link_id)s, %(body)s, %(status)s) RETURNING complaints.id

4.1.4. Get Complaints

SELECT complaints.id AS complaints_id, complaints.link_id AS complaints_link_id, complaints.body AS complaints_body, complaints.status AS complaints_status

4

4.2. Cassandra

4.2.1. Create a keyspace

CREATE KEYSPACE IF NOT EXISTS url_shortener WITH REPLICATION = { 'class' : 'SimpleStrategy', 'replication_factor' : '1' };

4.2.2. Create a table

CREATE TABLE IF NOT EXISTS url_shortener.urls (key text PRIMARY KEY, reference text, owner_id int, action text, is_active boolean);

4.2.3. Create link

INSERT INTO urls (key, reference, action, owner_id, is_active) VALUES (?,?,?,?,?);

4.2.4. Get link by key

SELECT * FROM urls WHERE key = ? ;

5. Conclusion

Using efficient algorithms that also consider user input, we have successfully built an efficient URL shortening service that prioritizes spam, phishing, and malware detection. We have focused on outliers in existing implementations. H. URLs that are considered safe but are actually malicious, or vice versa. The proposed secure URL shortening service allows users to use the service with more confidence, keeping security, availability and confidentiality in mind. Users can report malicious links that spread spam and malware which gets removed and blocked to prevent their spread.