International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-5, Issue-1, January-2018
DOI: 10.21276/ijirem.2018.5.1.10

# Finding Topic Experts and Inference Attacks On User Privacy Data in Twitter

**Ashwitha Rajendran**
IV Year UG Student
Department Of Computer Science And Engineering
S.A. Engineering College, Chennai -77
ashwitha14051997@gmail.com

**Ragini**
IV Year UG Student
Department Of Computer Science And Engineering
S.A. Engineering College, Chennai -77
jonishas@saec.ac.in

**Sarala**
IV Year UG Student,
Department Of Computer Science And Engineering
S.A. Engineering College, Chennai -77

**Jonisha S**
Assistant Professor,
Department Of Computer Science And Engineering
S.A. Engineering College, Chennai -77

## ABSTRACT
Twitter is one of the popular applications in social network which is used for sharing tweets among friends and other users.In this Paper, We propose an attack technique for inferring the clicks on shortened URLs in Twitter. The URL shortening services provides short alias of services from long URL for sharing tweets .Most of the experts can be found on twitter via searching through articles and blog posts, then following a link on their site to twitter. It seems to be much more effective way to find topic experts in Twitter.

**Keywords:** Expert Search, Meta Data, Public Click Analytics

## 1. INTRODUCTION
Finding experts in twitter has become hot topic among all the social networks. Expert finding is the most important problem in twitter because many experts posts valuable tweets which consists of rich information. So we are going to compute relevance between users and given queries and then rank all the Users based on the local relevance and find top-N users by ranking with highest scores. The third party applications are windows, MAC and android. Among the third party services, URL shortening services provides short alias from long URL for twitter users to share long URL tweets. For example, ***goo.lv***. Twitter allows the user to post tweets that contains only texts. If whenever users want to share complicated or restricted information, they should include URL with informationonto tweets**.**

## 2. LITERATURE SURVEY

### 2.1 Script less Timing Attacks on Web Browser Privacy
The existing Web timing attack methods are heavily dependent on executing client-side scripts to measure the time. However, many techniques have been proposed to block the executions of suspicious scripts recently. The most widespread history sniffing attack relies on inspecting the visual style difference between the visited and unvisited links.

**Technique:** Cascading Style Sheets (CSS)
A novel timing attack method to sniff users' browsing histories without executing any scripts. Our method is based on the fact that when a resource is loaded from the local cache, its rendering process should begin earlier than when it is loaded from a remote website. We leverage some Cascading Style Sheets (CSS) features to indirectly monitor the rendering of the target resource. Three practical attack vectors are developed for different attack scenarios and applied to six popular desktop and mobile browsers. The evaluation shows that our method can effectively sniff users' browsing histories with very high precision. We believe that modern browsers protected by script-blocking techniques are still likely to suffer serious privacy leakage threats.

### Disadvantages:
- Limited process of script blocking.
- Different attacks are applied in each browsing.
- High cost.

### 2.2 Collaborative Filtering with Privacy
Server-based collaborative filtering systems have been very successful in e-commerce and in direct recommendation applications. In future, they have many potential applications in ubiquitous computing settings. But today's schemes have problems such as loss of privacy, favoring retail monopolies, and with hampering diffusion of innovations.

**Technique:** Aggregate Algorithm
An alternative model in which users control all of their log data. We describe an algorithm whereby a community of users can compute a public "aggregate "of their data that does not expose individual users' data. The aggregate allows personalized recommendations to be computed by members of the community, or by outsiders. The numerical algorithm is fast, robust and accurate. Our method reduces the collaborative filtering task to an iterative calculation of the aggregate requiring only addition of

 

vectors of user data. Then we use homomorphism encryption to allow sums of encrypted vectors to be computed and decrypted without exposing individual data.

### Disadvantages:

- Individual user's data not exposé.
- Decryption without exposing individual data.
- Need addition of vector data high.

## 2.3 Timing Attacks on Web Privacy

Describe a class of attacks that can compromise the privacy of users' Web-browsing histories. The attacks allow a malicious Web site to determine whether or not the user has recently visited some other, unrelated Web page. The malicious page can determine this information by measuring the time the user's browser requires performing certain operations. Since browsers perform various forms of caching, the time required for operations depends on the user's browsing history; this paper shows that the resulting time variations convey enough information to compromise users' privacy.

**Technique:** Exploiting Web Caching

Accessing Web documents often takes a long time, so Web browsers use caching — they save copies of recently-accessed files, so that future accesses to those files can be satisfied locally, rather than requiring another time-consuming Web access. Caching is relatively effective in reducing perceived access times of Web pages.

### Disadvantages:

- Anonymous browsing tools fail to prevent them.
- Time consuming high.
- High cost

## 2.4 Finding Experts in Community-Based Question-Answering Services

In this paper, we are going to investigate that how experts can be captured and which group of experts likely provide answers to the given questions

**Techniques:** Mean Reciprocal Rank (MRR)

### Disadvantages:

- We know is who actually answered a question, but not who possesses the knowledge for that question

## 2.5 Expert Finding in a Social Network

The goal of finding experts is that identifying the person with experience of a particular given topic. In this paper, we focus on the relationships between person local information in unified approach. By estimating an initial expert score for each person using person local information, we select the person with top rank as experts and propagate it to the persons with whom he/she has relationships.

**Techniques:** Propagation Based Appro

# 3. CONCLUSION

We proposed attack technique for shortening URL. Our aim is to identify the attackers by crawling & monitoring the click analytics of shortened URL. We find topic experts by assigning similar ranking scores to the similar users and lists. Based on rank, we select top-N users for any given topic in twitter.

# REFERENCES

[1]. V. Qazvinian, E. Rosengren, D.-R.Radev, and Q.-Z. Mei, "Rumorhas it: Identifying misinformation in microblogs," in Proc. Conf. Empirical Methods Natural Language Process. 2011, pp. 1589–1599.

[2]. J.Canny,"Collaborative filtering with privacy" in Proceedings 2002 IEEE Symposium on Security and Privacy

[3]. E. W. Felten, M. A. Schneider, "Timing attacks on web privacy", Proc. 7th ACM Conf. Comput. Comm. Secur. (CCS), pp. 25-32, 2000.

[4]. A. Pal and S. Counts, "Identifying topical authorities in microblogs," in Proc. ACM Int. Conf. Web Search Data Mining, 2011, pp. 45–54.

[5]. X. Liu, W. B. Croft, and M. Koll, "Finding experts in communitybased Question-answering services," in Proc. ACM Conf. Inf. Knowl. Manag., 2005, pp. 315–316.

 