ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Inference Attack on Users Browsing History with Friend Recommendation System in Twitter

Swati Kamble, Dhanashree Phalke

Department of Computer Engineering, D Y Patil College of Engineering, Pune, Maharashtra, India

ABSTRACT: Twitter is the web based implementation assumptive repeat pieces of online lengthy scope casual explanation and micro blogging. Users talk with one another by distributing content based posts. Because Twitter limits the length of messages, there are many Twitter users using URL abbreviation services, such as bit.ly and goo.gl, to section lenthy web addresses with friends. Twitter users mostly use URL abbrivated services to deliver shortage of a lengthy URL for sharing it via tweets and public click analytics of shortened URLs. The public clicks analysis of abbreviated URLs. The analysis of public clicks is supplied in addition to defend the privacy of each user. Privacy is one major challenge of todays rapid digitalization of the human life. The users interact with net, make a digital occurrence that may contradict ones requirements for online privacy. Nevertheless the reality that certain URL clicking techniques have been developed for reducing the amount of private information made publicly available, it is still possible to reconstruct users preferences and interests and use this inference information for offering push advertisement. We propose practical attack techniques that indicate who clicks on abbreviated Twitter URLs using the addition of public information: Twitter metadata and public clicks analysis. Unlike traditional browsing history theft attacks, our attacks require only publicly available data provided by Twitter and URL shortening services. Index Terms Inference Attack, Novel Attack Techniques, privacy leak, Twitter, URL shortening service.

KEYWORDS: Inference Attack, Novel Attack Techniques, privacy leak, Twitter, URL shortening service.

I. INTRODUCTION

In the very important online service to change information or messages (tweets), in all over world 140 million users have created accounts on twitter and the most important thing isthat 340 million messages or information are sent daily onTwitter. A URL abbreviation service gives a short false nameto long URLs. This is valuable administration for Twitters whoshare expanded URLs through tweets (140-character tweetscontaining just messages) [12]. The well known URL providesservices, for example, bit.ly and goo.gl, additionally give anexamination of open snaps of abbreviated URLs that consistof many clicks, countries, browsers and visitor references [13].The URL abbreviation services give a joined form to securethe protection of the visitor of the attackers. We distinguisheda simple inference attack that can estimate individual visitorsfrom the aggregate analysis of public clicks using publicmetadata provided by Twitter. First, let's examine the metadataof the application and the client's route because they canbe correlated with those of the public clicks analysis. Forinstance, if a user, Merry updates their messages throughthe proper Twitter application for iPhone client, "Twitter foriPhone" will be included in the wellspring of the relatingmetadata. In addition, she can reveal on her profile page thatshe lives in the US (United States) or activate the locationservice of a Twitter client application to automatically fill inthe location field in the metadata. Utilizing this data, we canverify that Merry is an iPhone client who lives in the US(United States). Next, we perform the simple inference attackon behalf of Merry's boyfriend, Bob, as follows. Bob firstpublishes a tweet with a URL abbreviated by goo.gl. On theoff chance that Merry taps on the abbreviated URL, goo.glregisters "country": "USA", "Platform": "iPhone", "referent":"twitter.com", "browser": "Mobile" in the click analysis ofthe abbreviated URL [12]. Otherwise, goo.gl does not recordany information. Next, Bob retrieves the click scan of theabbreviated URL to find out the chance that Merry taps itsURL. If the click analysis is not modified or if your changesdo not include information in USA, iPhone and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

twitter.com,deduces that Merry does not click on its URL. If not, Merryis should tap on your URL. Attackers must cheat or involvetarget users or their networks to obtain browsing history, whichrelies upon the force hypothesis. On the contrary, anyone canaccess the Twitter information and the public can tap on theinvestigation of the shortening of the URL services so thatpassive monitoring is sufficient for the execution of attack.The proposed new attack methods to infer to surmise whethera particular client captured on particular abbreviated URLson Twitter. The attacks are in light of the mix of accessiblepublicizing data: tap on the URL metadata shortening analysisand Twitter services. The objective of the attacks is to knowin which URL the target users have clicked.

II. LITERATURE SURVEY

Z. Cheng, J. Caverlee, and K. Lee, presented you arewhere you tweet: a content-based approach to geo-locatingtwitter users. The authors propose and assess a probabilisticstructure to gauge the position at the city level of a Twitterclient construct only about the substance of the client'stweets, even without other geospatial signs. By expandingthe colossal human identification capacities of Twitter andits related microblogging administrations with area datagot from content, this structure can beat the deficiency ofgeo-empowered functionalities in these administrations andempower new area based data administrations and territorialnotices, et cetera. Three of the primary highlights of theproposed access are: (I) its dependence exclusively on thesubstance of the tweets, which implies that client IP data,private access data or outside learning bases are not required;(ii) an arrangement part for the programmed ID of words intweets with a solid nearby geo-extension; and (iii) a latexbasedneighborhood leveling model to refine the estimationof a client's position. The framework gauges k conceivablepositions for every client in diving request of certainty [1].

E. W. Felten and M. A. Schneider, presents timing attackson web privacy. The authors depict a class of assaults that can bargain the protection of clients' web perusing histories. The assaults enable a malignant site to decide if the client went by another disconnected page. The vindictive page can decide this data by estimating the time when the client's program requires certain activities to be performed. Since programs perform different types of storing, the time required for tasks relies upon the client's perusing history; this record demonstrates that the subsequent varieties in time transmit data that is adequate to bargain the security of clients. This technique for assault likewise permits different sorts of data gathering by sites, for instance, a more intrusive type of Web "treats". The culprits of the depicted assaults can be finished without the casualty's information and a large portion of the "mysterious perusing" devices can't stay away from them [2].

C. Jackson, A. Bortz, D. Boneh, and J. C. Mitchell, proposed protecting browser state from web privacy attacks. Through an assortment of means, including different techniques for program storing and shading assessment of a went by hyperlink, the condition of the customer side program can be abused to track clients against their desires. This observing is conceivable on the grounds that the constant condition of the program on the customer side isn't effectively separated by the site in the present programs. This report tends to this issue by refining the general thought of a "same starting point" strategy and by executing two program augmentations that apply this arrangement to the program's store and the connections went by. The authors likewise break down various degrees of collaboration between destinations to track clients and demonstrate that regardless of whether the long haul program state is legitimately isolated, it is as yet feasible for locales to utilize present day web capacities to bob clients between destinations. Furthermore, interfaces imperceptibly in numerous areas following its guests. The assaults to the helpful protection are an inescapable outcome of all the industrious condition of the guide that influences the conduct of the pilot and the deactivation or successive lapse of this state is the novel shape to acquire genuine security of the coludidas parts [3].

A. Janc and L. Olejnik, presented web browser history find as a real world privacy threat. The authors break down the effect of CSS-based story discovery and show the attainability of viable assaults with negligible assets.They investigate the handling of the web program andthe perceptibility of the substance stacked by standard conventions and with a few HTTP reaction codes. They build up a calculation for the productive examination of substantial arrangements of connections and assess their execution in current programs. Contrasted with existing techniques, this approach is up to

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

6 times quicker and can identify up to 30,000 associations went by every second. The authors display another web application that can viably identify client perusing histories and investigate genuine outcomes acquired from 271,576 Internet clients [4].

J. Lindamood, R.Heatherly,M. Kantarcioglu, and B. Thuraisingham, presents Inferring private information using social network data. Online locality communities, for example, social Media, are progressively utilized by numerous clients. These systems enable individuals to post insights
about themselves and interface with their companions. A limit of the data uncovered inside these systems is private and it is conceivable that organizations can utilize learning calculations in distributed information to foresee undisclosed private data. In this article, the writers investigate how to dispatch inferential assaults utilizing information distributed on interpersonal organizations to anticipate private data not uncovered in individuals. At that point, investigate the adequacy of conceivable sanitization systems that can be utilized to battle such derivation assaults in varity of location [5].

A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel, proposed you are who you know: assuming user profiles in digital networks. In paper, make the inquiry: given thequalities for a piece of the clients in an online interpersonal organization, would we be able to surmise the properties of the rest of the clients? At the last day, can the qualities of the clients, joined with the chart of the informal organization, be utilized to anticipate the traits of another client in the system? To answer this inquiry, the authors gather itemized information from two interpersonal organizations and endeavor to induce the traits of the client profile. They additionally find that clients with normal ascribes will probably be companions and regularly frame thick groups and propose a strategy to construe client properties that is enlivened by past ways to deal with recognize groups on informal organizations [6].

A. Narayanan and V. Shmatikov, presents de-anonymizing social networks. The authors display a structure to dissect protection and obscurity in informal communities and build up another reidentification calculation that focuses to mysterious interpersonal organization designs. To show their viability in certifiable systems, demonstrate that 33 percentage of clients with Twitter accounts, a well known microblogging administration, and Flickr, an online photograph sharing
website, can be re-distinguished on the unknown Twitter realistic with just a mistake rate of 12 percentage. This anonymization calculation is constructing exclusively system topology, does not offer the production of a substantial number of ”sybil” imaginary hubs, is vigorous for clamor and every single existing guard and furthermore works when they cover between the objective system and the system of the foe the assistant data is little [7].

J. Song, S. Lee, and J. Kim, presents i know the shortened urls you clicked on twitter: inference attack using public click analytics and twitter metadata. In this paper, the authors propose a commonsense assault procedure that can find who taps on what condensed URL on Twitter. Not at all like conventional program history taking assaults, has this assault technique just required openly accessible data gave by the URL and Twitter contraction administrations. The aftereffects
of the assessment demonstrate that this assault strategy cantrade off the security of Twitter clients with extraordinary exactness [8].

G. Wondracek, T. Holz, E. Kirda, and C. Kruegel, proposed a practical attack to de-anonymize social network users. This paper exhibits another anonymization assault that exploits data about gathering individuals accessible on interpersonal interaction destinations. All the more particularly, the authors demonstrate that the data about having a place with a gathering of clients are adequate to extraordinarily distinguish this individual or, in any event, to altogether lessen the arrangement of conceivable hopefuls. That is, rather than observing a client’s program as with treats, it is conceivable to track a man. To decide the participation of a client’s gathering, the framework stay on the known assaults of history taking from the web program. In this manner, each time a client of an informal organization visits a malignant site, this site can start our anonymization assault and know the character of its guests. The ramifications of this assault are different, since they require little exertion and can possibly impact a large number of informal community clients [9].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

E. Zheleva and L. Getoor, presents on user profiles. In this work, the authors indicate how a rival can exploit an online interpersonal organization with a mix of open and private client profiles to anticipate the private characteristics of clients. They allocate this issue to an issue of social arrangement and propose down to earth models that utilization data about association and gathering participation (which are regularly not covered up) to deduce touchy traits. The key novel is that, notwithstanding fellowship joins, gatherings can be transporters of significant data. They additionally demonstrate that in a few surely understood interpersonal interaction destinations, they can recover client data from private profiles effortlessly and precisely [10].

J. A. Calandrino, A. Kilzer, A. Narayanan, E. W. Felten, and V. Shmatikov,Authors create calculations that take a direct measure of helper data about a customer and deduct client exchanges from impermanent changes in people in general consequences of a proposal framework. These inferential assaults are latent and can be performed by any Internet client [11].

J. He, W. W. Chu, and Z. V. Liu, proposed networks. Since security information surmised through social connections, the protection issue turns0 progressively troublesome as online informal communication administrations turn prominent. Utilizing a Bayesian system way to deal with demonstrate the causal connections between individuals in interpersonal organizations, the authors think about the effect of the past likelihood, the impact compel and the transparency of the organization to the accuracy of the derivation in a genuine informal community on the web [12].

A. Narayanan and V. Shmatikov, presents a new class of statistical attacks of anonymization against high-dimensional microdata, such as individual preferences, recommendations, transaction records, etc. These methods are strong to change the information and endure a few blunders in the fundamental learning of the rival. We apply our anonymization philosophy
to the Netflix Prize informational collection, which contains unknown assessments of 500,000 Netflix supporters, the world's biggest online motion picture rental administration. The authors demonstrate that a rival who knows just a smidgen of a solitary endorser can undoubtedly recognize this currentsupporter's record in the informational collection. Utilizingthe Internet film database as a wellspring of essential learning, they have effectively recognized the records of known Netflix clients, finding their clear possibly touchy data [13].

III. SYSTEM ARCHITECTURE

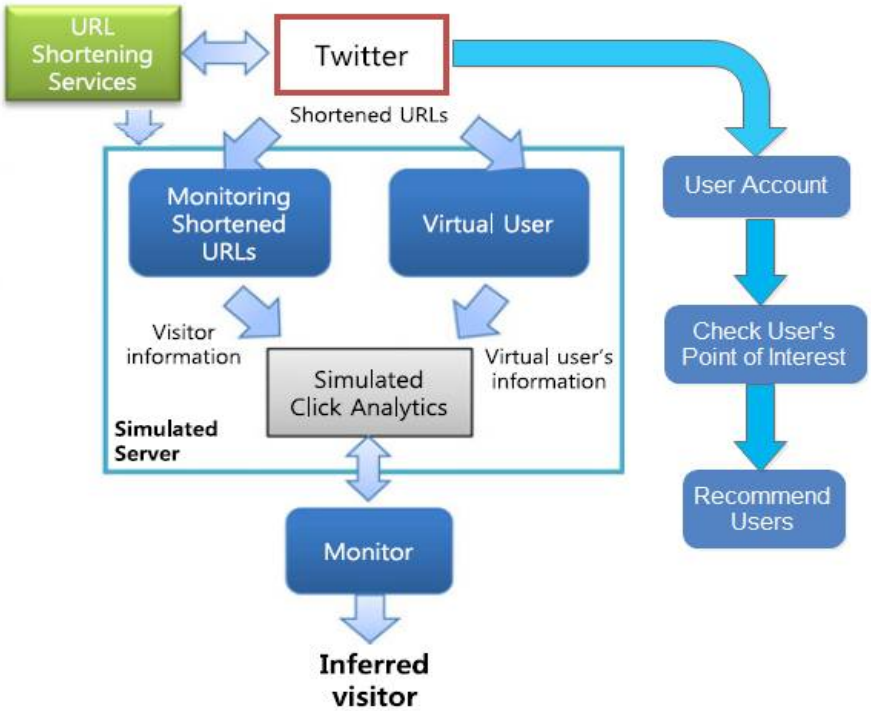

Figure 1: System Architecture

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

The inference attack attempts to detect a user who simultaneously uses the connected services by matching the superimposed information with the user's information. In our system, we use virtual users instead of Twitter clients in reality. The attack system tries to separate the condensed URLs clicked by the virtual clients of the trim URLs that real Twitter users click on. The processes involved attack system
are the following:

1) The monitoring module in the simulated server periodically monitors the analysis of the clicks of abbreviated URLs published by some Twitter users.

2) The monitor module extracts the actual visitor information from the click analysis changes and records it in the simulated click analysis.

3) The virtual user module in the simulated server stochastically adds the information about a virtual client to the analysis of the mimicked clicks to simulate the click of the virtual client.

4) The inference system periodically verifies changes in the analysis of simulated clicks and extracts information from a new user.

5) The inference framework looks at the data about the new client and the data about the virtual client.They coordinate, we surmise that the virtual client taps on the abbreviated URL.

We think about two inference attack outlines: Attack I: Inferring Visited cut down URLs by Target clients Attack II: Inferring Visitors of Shortened URLs

Attack I: Inferring Visited Shortened URLs by Target Users In attack I, our attack system identifies if an objective client taps on abbreviated URLs published by their followers. The result of this attack is an trim of URLs that the uninvolved client can tap on.

Attack II: Inferring Visitors of Shortened URLs In Attack II, our attack system identifies who tap on
the condensed URLs uploaded by a destination client. First we find a Twitter client who periodically updates the shortened bit.ly or goo.gl URLs and identifies the candidates who click on the trim URLs updated by the target user. Our system can get active twitter users interest from the system and according to that System recommends other twitter users to current user.

Modules:

1) Profiling Module Profiling module obtains the information of the target user from the target users profile
and timeline.

2) Monitoring Module The monitoring module extracts the shortened URLs from the tweets posted by the followings of the target user and monitors the changes in the click analytics of the shortened URLs. To create a Twitter user (monitoring user) who follows all the followings of the target user in order to access all tweets that the target user may view.

3) Matching Module The matching module compares the information about the new visitor with the information about the target user when the monitoring module notices the changes in the click analytics. If the matching module infers that the new visitor is the target user, it includes the corresponding shortened URL in a candidate URL set.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

IV. ALGORITHM

To advice algorithms to handle our inference attack in general situations. Initial specify customer also data. Let U be user information free by the major service. Let D be a data file liberated by the third party duty. To protect the users privacy, third party services provide the online data set D in aggregate form which consist of attributes a, values v and count of them c. Let AU be an assign set of U and AD be an assign set of D. We define U, D and their attribute sets as follows:

A_U = {a | a is an attribute of U}
A_D = {a | a is an attribute of D}
U = {(a : v) | a ϵA_U ,v is an value of a,
C is the counter of a tuple (a : v) at time t}
D = {(a : v, C(t)) | a ϵA_D ,v is an value of a,
C is the counter of a tuple (a : v) at time t}

Algorithm 1.Inference attack for a target user
Input: $A_C = A_U \cap A_D$

u = {(a:v) | a ϵA_C ,v is an value of a} and u $\subseteq$ U
d(t) = {(a:v,c(t)) | a ϵ A_C ,v is an value of a ,c (t) is the counter of (a:v) a tuple at time t} and $\exists$ (a:v,c(t)) ϵ D
Output: Inferred time the user has used the service
history = {}
Foreach observation time at t do
$\Delta d(t)$ = {(a:v)| $\exists$(a:v,c(t)) ϵ d(t) s.t (c(t) - c(t-1)) $\geq$1}

if u $\subseteq$ Δ(t) then
history = history U {t:u}
end
end
return history
Algorithm 1 shows the procedure of the inference attack in the case of a single target user and a single third party service. Usually, the attributes of U and D differ from each other. Therefore, the system has to calculate a set of common attributes of AU and AD, which is defined as AC.
$\Delta d(t)$ is the differences between d(t) and d(t-1). If a user u is a subset of the $\Delta d(t)$, the inference system infers that the user has used the service at time t. In this way, we can obtain the service usage history of the user, which is defined as follows:

history = {(t : u) | u exist at time t},
where (t : u) means that a user u used the service at time t.

Algorithm 2.Inference attack for multiple target users
Input: $A_C = A_U \cap A_D$
$u_1, u_2, u_3, \ldots u_n$: n user

u_i = {(a:v)|aϵA_C ,v is an value of a} and $u_i \subseteq$ U
d(t) = {(a:v,c(t)) | a ϵA_C ,v is an value of a ,c(t) is the counter of tuple (a:v) at time t} and $\exists$(a:v,c(t)) ϵD
Output: Inferred time the user
history = {}
Foreach observation time at t do
Δ d(t) = {(a:v)| $\exists$(a:v,c(t)) ϵd(t) s.t (c(t)- c(t-1)) $\geq$1}

If $u_i \subseteq$ Δ d(t) then

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

history = history U {t:u_i}
end
end
end
return history

Algorithm 2 shows the procedure of the inference attack on multiple users. When our inference system obtains Δd(t), the system compares it with each user. If u_i is a subset of Δd(t), the system adds ui into inferred history with time t. Finally, we can have the usage history that shows which users used the service at time t.

V. DISADVANTAGES OF EXISTING SYSTEM

1) An hourly follow also duplicate accept a constraintby reason of Twitter does not correctly add personalinformation about users such as country, browsers, andplatforms.

2) URL is an needed benefit because Twitter customerswho wish to measure long URLs via tweets having lengthrestriction.

VI. ADVANTAGES OF PROPOSED SYSTEM

1) We propose new assault procedures to choose whethera particular client taps on certain abbreviated URLs.

2) As far as we probably are aware, this is the main investigation that finds the historical backdrop of visits to URLs.

3) We only use the public details given by the URL and Twitter abbreviation services (for example, click on Twitter input and analysis).

4) We decide whether an objective client visits an abbreviated URL by relating freely accessible data.

5) It does not require convoluted methods or suppositions, for example, content infusion, phishing, malicious software interruption or Domain name system observing. All we require is openly accessible data.

6) The consequences of the assessment demonstrate that our attacks can correctly deduce click information withhigh accuracy and overload.

VII. COMPARISON BETWEEN EXISTING SYSTEM AND PROPOSED SYSTEM

Existing system needs complicated techniques or assumptions. Attackers should deceive or consume main users or their networks to obtain the browsing history, which relies on strong assumption. In contrast, anyone can access the data of information of Twitter and the public click analytics of URL abbreviated services so that passive monitoring is enough for performing our attack.

The proposed system proposes novel attack methods for inferring whether a specific user clicked on certain shortened URLs on Twitter.raid turn to the aggregate about openly usable report: beat analysis against URL abbreviating services and metadata from Twitter. The aim of the raid is to experience which URLs are beat on by target users. We introduce two different attack methods: (i) an attack to know who click on the URLs restoreed by main clients and (ii) a beat to see which URLs are clicked on by target users. Out advance does not demand elaborateed system either expectations such as characters vaccine, pushing, malware intrusion, or DNS monitoring. Full privately demand is openly usable data.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

VIII. RESULT

Fig. 3 shows that the graph of URL tweets. The x-axis represents user id in the system and y-axis represents tweets count

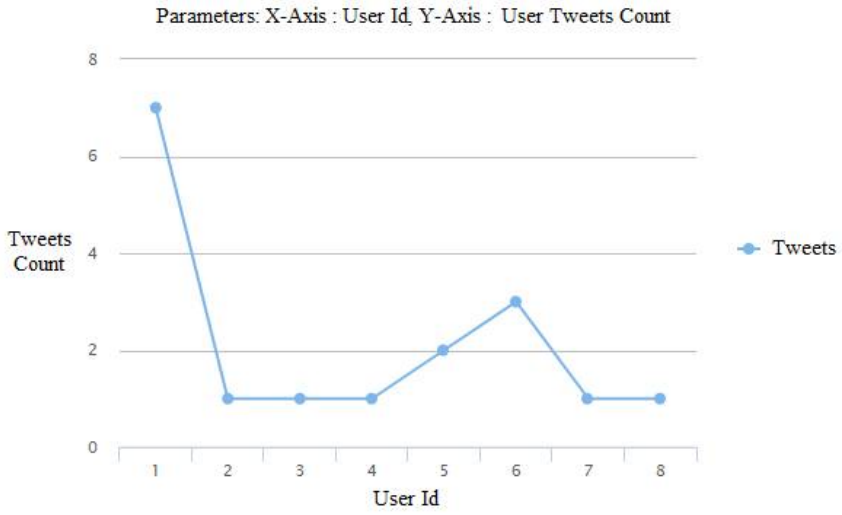

Fig. 2. Graph of URL Tweets

Fig. 4 shows that the graph of users followers. The x-axis represents user id and y-axis represents follower count.

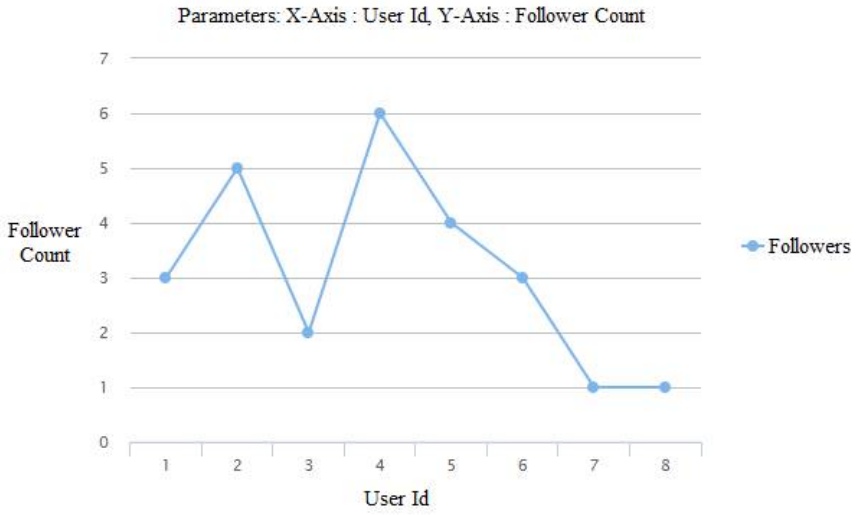

Fig. 3. Graph of Users Followers

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

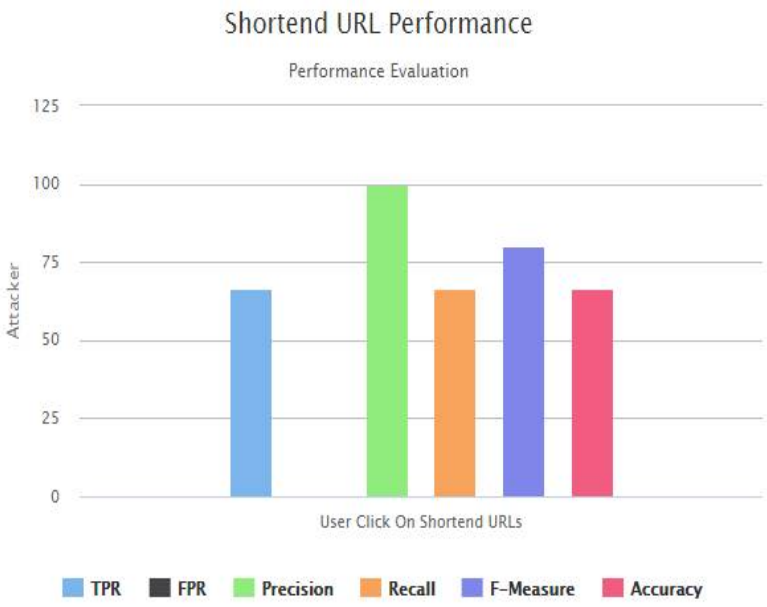

Fig. 4. System Accuracy Graph

Table 1
URL Tweets

Sr. No.	User Id	Tweets
1	1	7
2	2	1
3	3	1
4	4	1
5	5	2
6	6	3
7	7	1
8	8	1

Table 2
Users Followers

Sr. No.	User Id	Tweets
1	1	3
2	2	5
3	3	2
4	4	6
5	5	4
6	6	3
7	7	1
8	8	1

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

The Table 1 show that URL tweets given by users and Table 2 show those user followers. According to our result table we conclude system works efficiently as compare to other state of art systems.

IX. CONCLUSION

An inference attacks to deduce which shortened URLs tapped on by target client. All the data required in these attacks is open data: the click examination of URL shortening services and Twitter metadata. To assess these attacks, they observed the click analytics of URL shortening services and Twitterinformation. Furthermore by utilizing this we discover the attacker details and block that attacker details.

ACKNOWLEDGMENT

The architects would like to thank the analyst as well as publishers for making their expedient to be got and the teachers for their direction. We also thank the college establishment for providing the required base and confirm. Finally, we would like to build out a heartfelt thankfulness to all friends and family members.

REFERENCES

[1] Z. Cheng, J. Caverlee, and K. Lee, You are where you tweet: A contentbased approach to geo-locating twitter users, in Proc. 19th ACM Int. Conf. Inform. Knowl. Manage, 2010, pp. 759768.
[2] E. W. Felten and M. A. Schneider, Timing runs on web secrecy, in Proc.7th ACM Conf. Comput. Comm. Secur. (CCS), 2000, pp. 2532.
[3] C. Jackson, A. Bortz, D. Boneh, and J. C. Mitchell, Protecting search state from web secrecy runs, in Proc. 15th Int. WWW Conf., 2006, pp. 737744.
[4] A. Janc and L. Olejnik, Web browser history detection as a real world privacy threat, in Proc. 15th Eur. Conf. Res. Comput. Secur., 2010, pp. 215231.
[5] J. Lindamood, R.Heatherly,M. Kantarcioglu, and B. Thuraisingham, Inferring private information using social network data, in Proc. 18th Int. WorldWideWeb Conf. (WWW), 2009.
[6] A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel, You are whom to you be informed: Inferring user profiles in on-line mixer net, in Proc. 3rd ACM Int. Conf. WWW Look Up and Information excavation, 2010, pp. 251260.
[7] A. Narayanan and V. Shmatikov, De-Anonymizing mixer nets, in Proc. 30th IEEE Symp. Secur. Privacy, 2009, pp. 173187.
[8] J. Song, S. Lee, and J. Kim, One experience the abbrivated web addresses you dawned on twitter: Inference attack exploitation world dawn analytics and twitter metadata, in Proc. 22nd Int. cyberspace Conf., 2013, pp. 11911200.
[9] G. Wondracek, T. Holz, E. Kirda, and C. Kruegel, A virtual run to deanonymize mixer net clients, in Proc. IEEE Symp. Secur. Privacy, 2010, pp. 223238.
[10] E. Zheleva and L. Getoor, As far as add surgery none to join: The illusion of secrecy in mixer nets with mixed public and private user profiles, in Proc. 18th Int. World Wide Web Conf., 2009, pp. 531540.
[11] Twitter developers, (2012). The t.co url wrapper. [Online]. Available: https://dev.twit.com/docs/tco-abbrivated-cover.
[12] Jonghyuk Song, Sangho Lee, Jong Kim, Inference Attack on Browsing History of Twitter Users Using Public Click Analytics and Twitter Metadata, IEEE Transactions on Dependable and Secure Computing, Vol. 13, No. 3, May/June 2017.
[13] Aaradhana Deshmukh, Reshma Gade, Albena Mihovska and Ramjee Prasad, Inference Attack on URL Visiting History of the Social Networking, I J C T A, 10(9), 2017, pp. 145-152.
[14] J. A. Calandrino, A. Kilzer, A. Narayanan, E. W. Felten, and V.Shmatikov, You might also like: Privacy risks of collaborative filtering, in Proc. IEEE Symp. Secur. Privacy, 2011, pp. 231246.
[15] J. He, W. W. Chu, and Z. V. Liu, Inferring privacy information from social networks, in Proc.4th IEEE Int. Conf. Intell. Secur. Informatics, 2006, pp. 154165.
[16] A. Narayanan and V. Shmatikov, Robust de anonymization of large sparse data set, in Proc. IEEE Symp. Secur. Privacy, 2008, pp. 111125.