Volume 4 || Special Issue 4 || ICCEME 2019-2020 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

DETECTING AUTOMATION OF TWITTER ACCOUNTS: ARE YOU HUMAN, BOT OR CYBORGS?

Mr. Amit Rajesh Salunkhe
Department of Computer Science & Engineering
G H Raisoni College of Engineering & Management,Wagholi
salunkheamit367@gmail.com
Ms. Jyoti Mutkule
Department of Computer Science & Engineering
G H Raisoni College of Engineering & Management,Wagholi
mutkulejyoti23@gmail.com
Mr. Balaji Deshmukh
Department of Computer Science & Engineering
G H Raisoni College of Engineering & Management,Wagholi
Mr. Gaurav Shinde
Department of Computer Science & Engineering
G H Raisoni College of Engineering & Management,Wagholi
Prof. Suvarna Satkar
Department of Computer Science & Engineering
G H Raisoni College of Engineering & Management,Wagholi
Suvarna.satkar@raisoni.net

Abstract- Twitter is a new web application playing dual roles of online social networking and micro blogging. Users communicate with each other by publishing text-based posts. The popularity and open structure of Twitter have attracted a large number of automated programs, known as bots, which appear to be a double-edged sword to twitter. Legitimate bots generate a large amount of benign tweets delivering news and updating feeds, while malicious bots spread spam or malicious con- tents.

Keywords- *authorized searchable encryption, traceability, multiple keywords subset search, cloud computing.*

I INTRODUCTION

Twitter is a popular online social networking and micro blogging tool, which was released in 2006. Remarkable simplicity is its distinctive feature. Its community interacts via publishing text-based posts, known as tweets. The tweet size is limited to 140 characters.

Hashtag, namely words or phrases prefixed with a symbol, can group tweets by topic. For example, Justin Bieber and Women's World Cup are the two trending hashtags on Twitter in 2011. Symbol @ followed by a username in a tweet enables the direct delivery of the tweet to that user. Unlike most online social networking sites (i.e., Facebook and MySpace), Twitter's user relationship is directed and consists of two ends, friend and follower. In the case where the user A adds B as a friend, A is a follower of B while B is a friend of A. In Twitter terms, A follows B (namely, the following relationship is unidirectional from A to B). B can also add A as his friend (namely, following back or returning the follow), but is not required. When A and B follow each other, the relationship becomes bidirectional. From the standpoint of information flow, tweets flow from the source (author) to

Subscribers (followers). More specifically, when a user posts tweets, these tweets are displayed on both the author's homepage and those of his followers.

II REVIEW OF LITERATURE

Project Name Author Name Proposed System This Paper We Refer to 1) ""You might also like:" Privacy risks of collaborative filtering," A. Calandrino, A. Kilzer, A. Narayanan, E. W. Felten, and V. Shmatikov, In this paper we develop algorithms which take a moderate amount of auxiliary information about a customer and infer this customer's transactions from temporal changes in the public outputs of a recommender system. Our inference attacks are passive and can be carried out by any Internet user. Idea about Privacy risks of collaborative filtering. 2) "Timing attacks on web privacy," E. W. Felten and M. A. Schneider, This paper presents 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. 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.

III EXISTING SYSTEM

Twitter has been widely used since 2006. To better understand micro blogging usage and communities, studied over 70,000 Twitter users and categorized their posts into four main groups: daily chatter, conversations, sharing information or URLs, and reporting news. Their work also studied 1) the growth of Twitter, showing a linear growth

Twitter has been widely used since 2006. To better understand micro blogging usage and communities, studied over 70,000 Twitter users and categorized their posts into four main groups: daily chatter, conversations, sharing information or URLs, and reporting news. Their work also studied 1) the growth of Twitter, showing a linear growth rate; 2) its network properties, showing the evidence that the networks scale-free like other social networks; and 3) the geographical distribution of its users, showing that most Twitter users are from the US, Europe, and Japan. A group of over 100,000Twitter users and classified their roles by follower-to-following ratios into three groups: 1) broadcasters, which have a large number of followers; 2) acquaintances, which have about the same number on either followers or following; and 3) miscreants and evangelists (e.g., spammers),which follow a large number of other users but have few followers. The information diffusion on Twitter, regarding the production, flow, and consumption of information. The quantitative study on Twitter by crawling the entire Twitter sphere. Their work analysed the follower-following topology, and found manpower-law follower Distribution and low reciprocity, which all mark a deviation from known characteristics of human social networks. Twitter lists as a potential source for discovering latent characters and interests of users. Atwitter list consists of multiple users and their tweets. Their research indicated that words extracted from each list are representative of all the members in the list even if the words are not used by the members. It is useful for targeting users with specific interests. The behaviors of spammers on Twitter by analyzing the tweets originated from suspended users in retrospect. They found that the current marketplace for Twitter spam uses a diverse set of spamming techniques, including a variety of strategies for creating Twitter accounts, generating spam URLs.

IV SYSTEM ARCHITECTURE

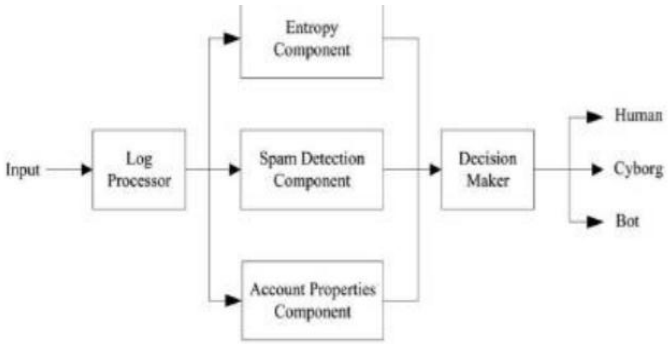

Figure 1. Propose System Architecture

This system design will provide an efficient traceable authorization search system for secure cloud storage, which overcomes all limitations of existing system. Inflexible authorized keyword search, abuse of attribute secret key, inefficient decryption. Sometimes authorized user may intentionally leak the secret key for financial benefit. Thus, tracing and revoking the unauthorized user who abuses secret key needs to be solved imminently.

V ALGORITHM

AES Algorithm

1. Key Expansions

For each round AES requires a separate 128-bit round key block plus one more.

2. InitialRound

AddRoundKey—with a block of the round key, each byte of the state is combined using bitwise xor.

3. Rounds

• SubBytes—in this step each byte is replaced with another byte.

• ShiftRows— for a certain number of steps, the last three rows of the state are shifted cyclically.

• MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

• AddRoundKey
1. Final Round (no MixColumns)
• SubBytes
•ShiftRows
AddRoundKey.

MD5 Algorithm

Computation of the MD5 digest value is performed in separate stages that process each 512-bit block of data along with the value computed in the preceding stage:

1. The first stage begins with the message digest values initialized using consecutive hexadecimal numerical values.
2. Each stage includes four message digest passes which manipulate values in the current data block and values processed from the previous block.
3. The final value computed from the last block becomes the MD5 digest for that block.

Visual Cryptography

1.Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.

2. Visual Cryptography is a wide area of research used in data hiding, securing images, color imaging, multimedia and other such fields.

VI. RESULT

Figure 2: Home Page

Figure 3: Login Page

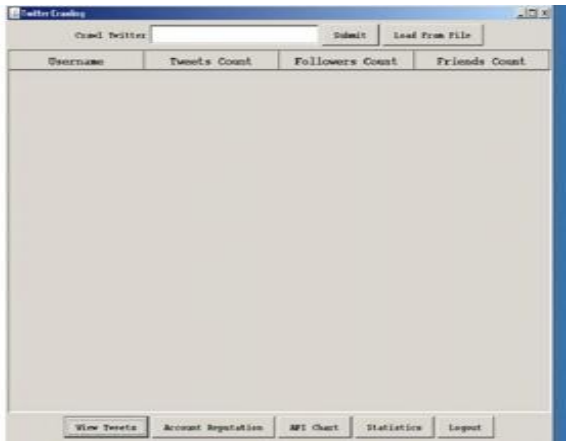

Figure 4: Successful Login

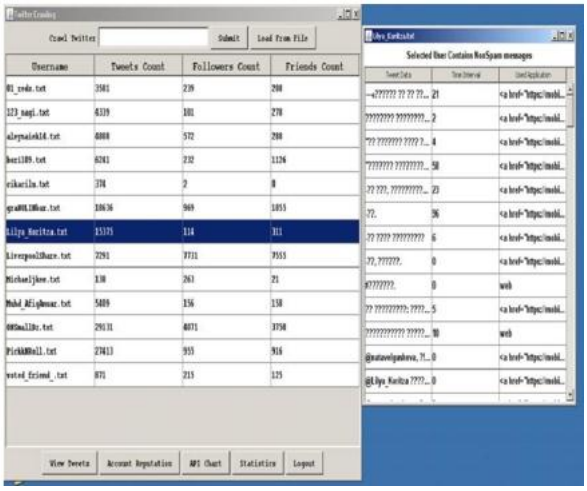

Figure 5: Account Details

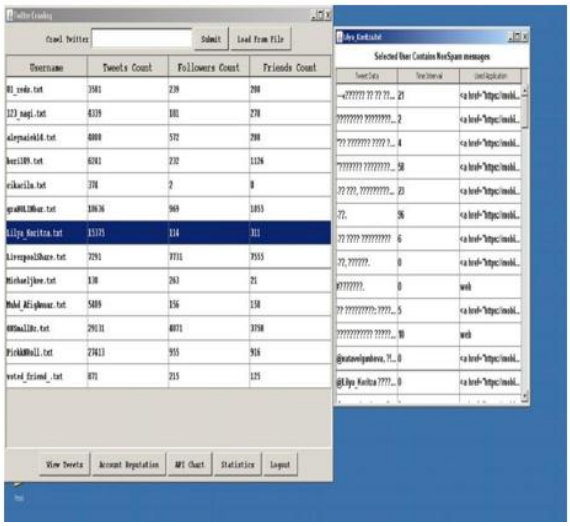

Figure 6: Device Details

VII. APPLICATIONS

1. Social Media

VIII. BENEFITS

1. Affording information to give the ability of self-orientation and mental map of the surroundings.
2.Visual Identifier can avoid accidents.

XI CONCLUSION

In this paper, we have studied the problem of automation bybots and cyborgs on Twitter. As a popular web application, Twitter has become a unique platform for information sharing with a large user base. However, its popularity and very open nature have made twitter a very tempting target for exploitation by automated programs, i.e., bots. The problem of bots on Twitter is further complicated by the key role that automation plays in everyday Twitter usage. To better understand the role of automation on Twitter, we have measured and characterized the behaviors of humans, bots, and cyborgs on Twitter. By crawling Twitter, we have collected one month of data with over 500,000 Twitter users with more than 40 million tweets. Based on the data, we have identified features that can differentiate humans, bots, and cyborgs on Twitter. Using entropy measures, we have determined that humans have complex timing behavior, i.e., high entropy, whereas bots and cyborgs are often given away by their regular or periodic timing, i.e., low entropy. In examining the text of tweets, we have observed that a high proportion of bot tweets contain spam content

REFERENCES

1. “Top Trending Twitter Topics for 2011 from What the Trend,” http://blog.hootsuite.com/top-twitter-trends-2011/, Dec. 2011.
2. “Twitter Blog: Your World, More Connected,” http://blog. twitter.com/2011/08/your-world-more-connected.html, Aug. 2011.
3. Alexa, “The Top 500 Sites on the Web by Alexa,” http:// www.alexa.com/topsites, Dec. 2011.
4.“Amazon Comes to Twitter,” http://www.readwriteweb.com /archives/amazon_comes_to_twitter.php, Dec. 2009.
5. “Best Buy Goes All Twitter Crazy with @Twelpforce,” http:// twitter.com/in_social_media/status/2756927865, Dec. 2009.
6. “Barack Obama Uses Twitter in 2008 Presidential Campaign,” http://twitter.com/BarackObama/, Dec. 2009.
7. J. Sutton, L. Palen, and I. Shlovski, “Back-Channels on the Front Lines: Emerging Use of Social Media in the 2007 Southern California Wildfires,” Proc. Int’l ISCRAM Conf., May 2008.