International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362
IJARST

Identifying and filtering out Inauthentic Users on Social media Platforms

M Praveen Reddy [1],Mala Jagadeesh[2], Mudumbai Mahathi[3],Mohd Shujath[4], Mogal Hashim Baig[5]

[2,3,4,5] UG Scholars, Department of CSE, **AVN Institute of Engineering and Technology,**Hyderabad, Telangana, India.

[1] Assistant Professor, Department of CSE, **AVN Institute of Engineering and Technology**, Hyderabad, Telangana, India.

ABSTRACT

Social networking sites engage millions of users around the world. The users' interactions with these social sites, such as Twitter and Facebook have a tremendous impact and occasionally undesirable repercussions for daily life. The prominent social networking sites have turned into a target platform for the spammers to disperse a huge amount of irrelevant and deleterious information. Twitter, for example, has become one of the most extravagantly used platforms of all times and therefore allows an unreasonable amount of spam. Fake users send undesired tweets to users to promote services or websites that not only affect legitimate users but also disrupt resource consumption. Moreover, the possibility of expanding invalid information to users through fake identities has increased that result in the unrolling of harmful content. Recently, the detection of spammers and identification of fake users on Twitter has become a common area of research in contemporary online social Networks (OSNs). In this paper, we perform a review of techniques used for detecting spammers on Twitter. Moreover, a taxonomy of the Twitter spam detection approaches is presented that classifies the techniques based on their ability to detect: (i) fake content, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users. The presented techniques are also compared based on various features, such as user features, content features, graph features, structure features, and time features. We are hopeful that the presented study will be a useful resource for researchers to _nd the highlights of recent developments in Twitter spam detection on a single platform.

INTRODUCTION

It has become quite unpretentious to obtain any kind of information from any source across the world by using the Internet. The increased demand of social sites permits users to collect abundant amount of information and data about users. Huge volumes of data available on these sites also draw the attention of fake users. Twitter has rapidly become an online source for acquiring real-time information about users. Twitter is an Online Social Network (OSN) where users can share anything and everything, such as news, opinions, and even their moods. Several arguments can be held over different topics, such as politics, current affairs, and important events. When a user tweets something, it is instantly conveyed to his/her followers, allowing them to outspread the received information at a much broader level. With the evolution of OSNs, the need to study and analyze users' behaviors in online social platforms has intensi_ed. Many people who do not have much information regarding the OSNs can easily be tricked by the fraudsters. There is also a demand to combat and place a control on the people who use OSNs only for advertisements and thus spam other people's accounts.

Recently, the detection of spam in social networking sites attracted the attention of researchers. Spam detection is a difficult task in maintaining the security of social networks. It is essential to recognize spams in the OSN sites to save users from various kinds of malicious attacks and to preserve their security and privacy. These hazardous maneuvers adopted by spammers cause massive destruction of the community in the real world. Twitter spammers have various objectives, such as spreading invalid information, fake news, rumors, and spontaneous messages. Spammers achieve their malicious objectives through advertisements and several other means where they support different mailing lists and subsequently dispatch spam messages randomly to broadcast their interests. These activities cause disturbance to the original users who are known as non-spammers. In addition, it also decreases the repute of the OSN platforms. Therefore, it is essential to design a scheme to spot spammers so that corrective efforts can be taken to counter their malicious activities.

Several research works have been carried out in the domain of Twitter spam detection. To encompass the existing state-ofthe- art, a few surveys have also been carried out on fake user identification from Twitter. Tingmin *et al.* provide a survey of new methods and techniques to identify Twitter spam detection. The above survey presents a comparative study of the current approaches. On the other hand, the authors in conducted a survey on different behaviors exhibited by spammers on Twitter social network. The study also provides a literature review that recognizes the existence of spammers on Twitter social network. Despite all the existing studies, there is still a gap in the existing literature. Therefore, to bridge the gap, we review state-of-the-art in the spammer detection and fake user identification on Twitter. Moreover, this survey presents a taxonomy of the Twitter spam detection approaches and attempts to offer a detailed description of recent developments in the domain.

The aim of this paper is to identify different approaches of spam detection on Twitter and to present a taxonomy by classifying these approaches into several categories. For classification, we have identified four means of reporting spammers that can be helpful in identifying fake identities of users.

Spammers can be identified based on:

(i) Fake content,
(ii) URL based spam detection,
(iii)Detecting spam in trending topics, and
(iv)Fake user identification.

Table 1 provides a comparison of existing techniques and helps users to recognize the significance and effectiveness of the proposed methodologies in addition to providing a comparison of their goals and results. Table 2 compares different features that are used for identifying spam on Twitter. We anticipate that this survey will help readers _nd diverse information on spammer detection techniques at a single point.

LITERATURAL SURVEY

TITILE: A break in the clouds: Towards a cloud definition.

AUTHOR: L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner.

This paper discusses the concept of Cloud Computing to achieve a complete definition of what a Cloud is, using the main characteristics typically associated with this paradigm in the literature. More than 20 definitions have been studied allowing for the extraction of a consensus definition as well as a minimum definition containing the essential characteristics. This paper pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. We also describe the relationships and distinctions between the Grid and Cloud approaches.

TITLE: Practical techniques for searches on encrypted data.

AUTHOR: D. X. Song, D. Wagner, and A. Perrig.

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query without loss of data confidentiality. In this paper, we describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms we present are simple, fast (for a document of length , the encryption and search algorithms only need stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

TITLE: A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data.

AUTHOR: Z. Xia, X. Wang, X. Sun, and Q. Wang.

Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF x IDF model are combined in the index construction and query generation. We construct a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results. Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.

TITLE: Searchable symmetric encryption: Improved definitions and efficient constructions.

AUTHOR: R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky.

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions. Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction

TITLE: Public key encryption with keyword search.

AUTHOR: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano.

We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else.

We define the concept of public key encryption with keyword search and give several constructions.

SYSTEM ANALYSIS

Existing System:

The existing multi-keyword search schemes can realize many multi-keyword search related functions such as conjunctive keyword search, disjunctive keyword search and subset search. Ballardetal. Proposed two different conjunctive keyword search schemes, which only return the files containing all the searched keywords, on the basis of Shamir secret sharing and bilinear pairings, respectively. Their scheme is proven secure in the standard model. And disjunctive keyword search scheme was proposed in later, which can return files containing the subset of query keywords. Meanwhile predicate encryption schemes were also presented in order to support both conjunctive keyword search and disjunctive keyword search.

Disadvantages:

1. The data owner has to rebuild the search index tree, which is time-consuming.
2. Traditional solutions have to suffer high computational costs.

Proposed System:

We will propose a secure and effective multi-keyword ranked search scheme supporting update operations efficiently. The index tree based on Bloom filter will be designed to improve the search efficiency. And our scheme utilizes vector space model to build an index vector for every file in the outsourcing dataset. The cosine similarity measure is used to compute the similarity score of one file to the search query and TF×IDF weight will be used to improve the search accuracy.

Advantage:

1. Support dynamic operation properly and effectively.
2. This scheme updates the lower computational cost.
3. Supports dynamic operations that contain deletions or insertions in a document

IMPLEMENTATION

MODULES

1. OWNER
2. USER
3. TRAPDOOR
4. CLOUD
5. ATTACKER

MODULAR DESCRIPTION

1. OWNER

In this application the owner is one of the main module for uploading the files and view the uploads file which are uploaded by the owner before do all these operations the owner should register with the application and the owner should authorized by the cloud.

2. USER

In this application the user also a modules to perform the bloom filter operation to access the files from the cloud, before do the search operations the user should get the search permission from the cloud then only the user can search the files after get the details of the searched file, if the user want to download the user should get the trapdoor key from the trapdoor Generator, then the user can able to download the file.

To do all these operation the user should register with application and the user should accessed by the cloud.

3. TRAPDOOR GENERATOR

The trapdoor is used to generate the trapdoor key for the requested users.

Here the trapdoor should login directly with the application.

4. CLOUD

The cloud is the main module to operate this project in the users activation s , owner activation and also the cloud can check the following operations like search permission provides to the users, can check the top-k searched keyword, top-k similarity in chart, top-k searched keyword in chart.

Primarily the cloud should login. Then only the cloud can perform the above mentioned actions.

5. ATTACKER

The attacker is the unauthorized perform to attack the owner files.

SYSTEM DESIGN

SYSTEM ARCHITECTURE

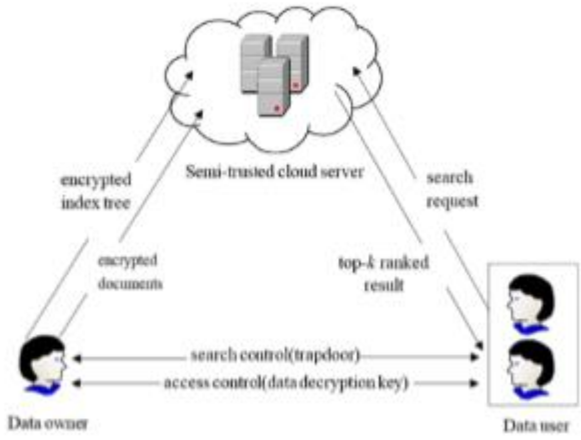
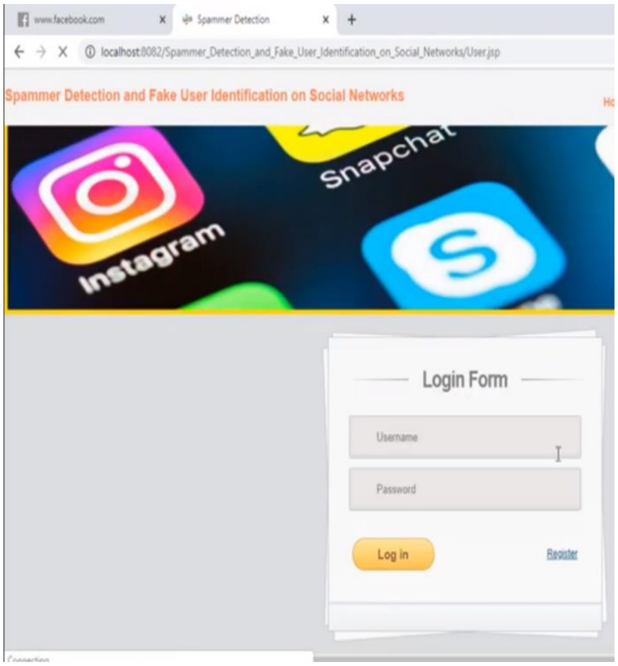


FIGURE 1. Architecture of the search over encrypted cloud data.

Fig. System Architecture

SCREEN SHOTS

Home Page

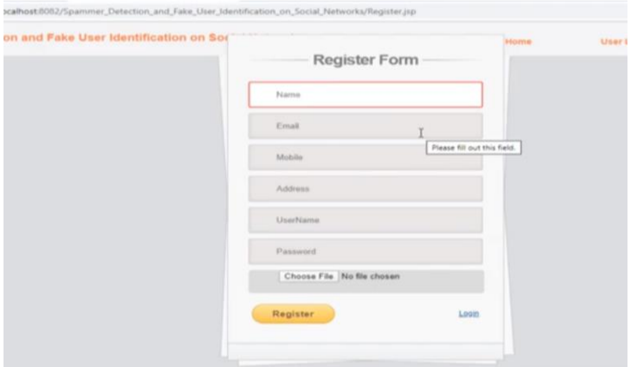


localhost:8082/Spammer_Detection_and_Fake_User_Identification_on_Social_Networks/User.jsp

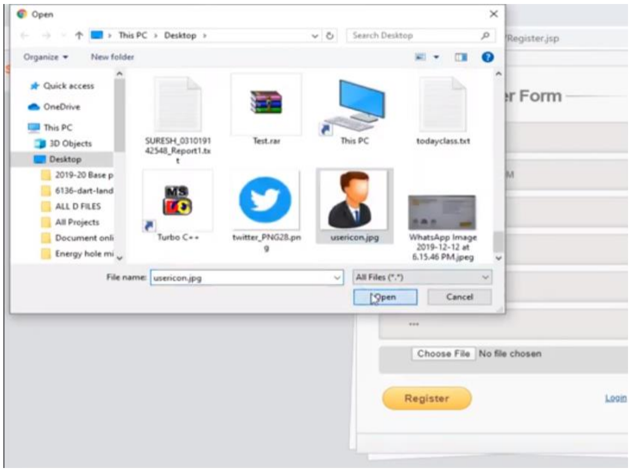
Spammer Detection and Fake User Identification on Social Networks

Login Form

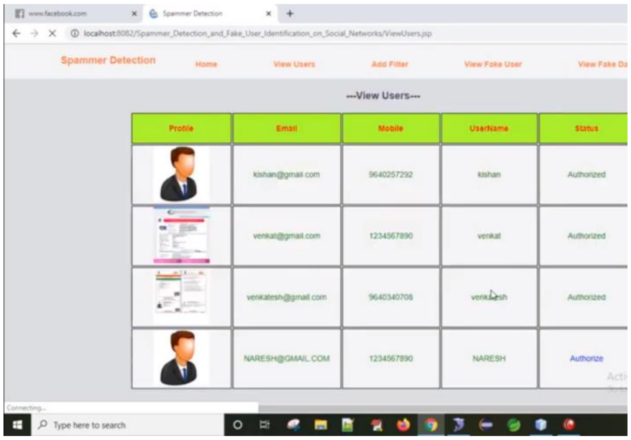
Login form


calhost:8082/Spammer_Detection_and_Fake_User_Identification_on_Social_Networks/Register.jsp
on and Fake User Identification on Soc
Home
User
Register Form
Name
Email
Please fill out this field.
Mobile
Address
UserName
Password
Choose File No file chosen
Register
Login

Register form



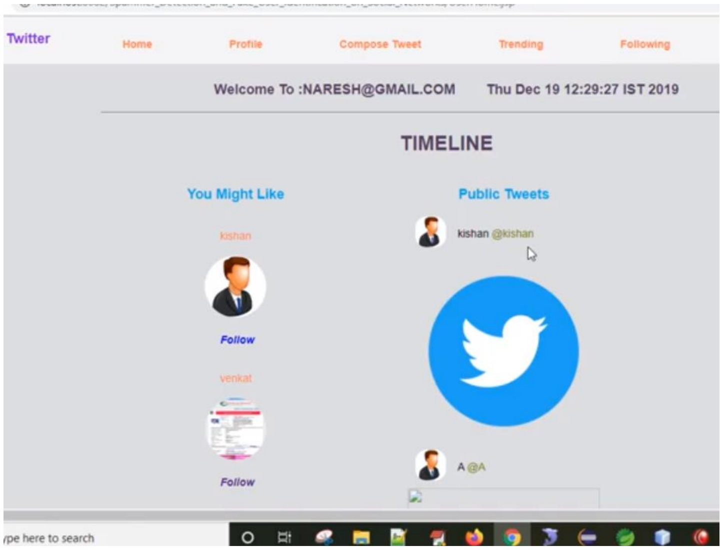
Choose file



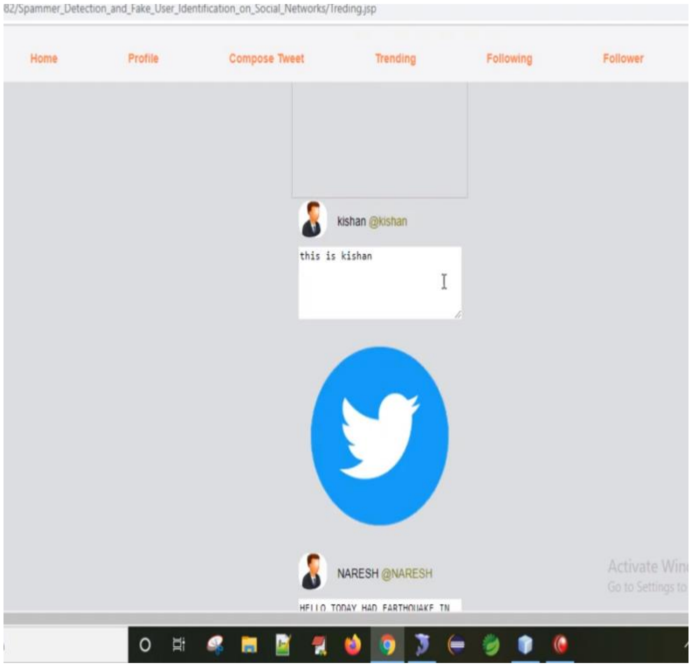
---View Users---

Profile	Email	Mobile	UserName	Status
	kishan@gmail.com	9640257292	kishan	Authorized
	venkat@gmail.com	1234567890	venkat	Authorized
	venkatesh@gmail.com	9640340708	venkatesh	Authorized
	NARESH@GMAIL.COM	1234567890	NARESH	Authorize

View users



Welcome To :NARESH@GMAIL.COM Thu Dec 19 12:29:27 IST 2019



this is kishan

HELLO TODAY HAD EARTHQUAKE IN

CONCLUSION

In this paper, we performed a review of techniques used for detecting spammers on Twitter. In addition, we also presented a taxonomy of Twitter spam detection approaches and categorized them as fake content detection, URL based spam detection, spam detection in trending topics, and fake user detection techniques. We also compared the presented techniques based on several features, such as user features, content features, graph features, structure features, and time features. Moreover, the techniques were also compared in terms of their specified goals and datasets used. It is anticipated that the presented review will help researchers _nd the information on state-of-the-art Twitter spam detection techniques in a consolidated form.

Despite the development of efficient and effective approaches for the spam detection and fake user identification on Twitter, there are still certain open areas that require considerable attention by the researchers. The issues are briey highlighted as under:

False news identification on social media networks is an issue that needs to be explored because of the serious repercussions of such news at individual as well as collective level. Another associated topic that is worth investigating is the identification of rumor sources on social media. Although a few studies based on statistical methods have already been conducted to detect the sources of rumors, more sophisticated approaches, e.g., social network based approaches, can be applied because of their proven effectiveness.

REFERENCES

[1] B. Erçahin, Ö. Akta³, D. Kilinç, and C. Akyol, ``Twitter fake account detection,'' in *Proc. Int. Conf. Comput. Sci. Eng. (UBMK)*, Oct. 2017, pp. 388_392.

[2] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, ``Detecting spammers on Twitter,'' in *Proc. Collaboration, Electron. Messaging, Anti- Abuse Spam Conf. (CEAS)*, vol. 6, Jul. 2010, p. 12.

[3] S. Gharge, and M. Chavan, ``An integrated approach for malicious tweets detection using NLP,'' in *Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT)*, Mar. 2017, pp. 435_438.

[4] T. Wu, S. Wen, Y. Xiang, and W. Zhou, ``Twitter spam detection: Survey of new approaches and comparative study,'' *Comput. Secur.*, vol. 76, pp. 265_284, Jul. 2018.

[5] S. J. Soman, ``A survey on behaviors exhibited by spammers in popular social media networks,'' in *Proc. Int. Conf. Circuit, Power Comput. Tech- nol. (ICCPCT)*, Mar. 2016, pp. 1_6.

[6] A. Gupta, H. Lamba, and P. Kumaraguru, ``1.00 per RT #BostonMarathon # prayforboston: Analyzing fake content on Twitter,'' in *Proc. eCrime Researchers Summit (eCRS)*, 2013, pp. 1_12.

[7] F. Concone, A. De Paola, G. Lo Re, and M. Morana, ``Twitter analysis for real-time malware discovery,'' in *Proc. AEIT Int. Annu. Conf.*, Sep. 2017, pp. 1_6.