ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2352-8648
Vol.01, Issue.01
March -2021
Pages: -094-101

A Supervised Learning Technique to Detect FakeApps in Appstore by Using Apkevaluator

[1] *M. Tech., Dept of CSE, Sri Sunflower College of Engineering and Technology. AP, India,* kalyan.murala8@gmail.com

[2] *B. Tech., Dept of CSE, Sri Sunflower College of Engineering and Technology. AP, India,* tandusravani@gmail.com

Abstract:- In social media users can download applications with pay and without paying amount for retrieving data and accessing information from the server. Unfortunately some apps accessing data and using that data for miss use so that we propose the concept of fraud apps detection in social media. Supervised learning techniques we are implemented in this paper those methods support uploading information relevant to apps or not. If it is not relevant to input then only our methods supports to identify which one is fake and which one is genuine. This project supports to social media users by reading comments and likes provided by another user. The main role is from admin side fake detection with respect to apk evaluators. Our evaluators generate keys for the verified apps such apps are only supported for users. No one can access fake apps in social media then we can say that apk evaluators are working properly without any technical failure.

Keywords—Android market, search rank fraud, malware detection.

I. Introduction:-

What Is A Social Network?

Wikipedia defines a social network service as a service which “focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others, and which necessitates the use of software.”

A report published by OCLC provides the following definition of social networking sites: “Web sites primarily designed to facilitate interaction between users who share interests, attitudes and activities, such as Facebook, Mixi and MySpace.”

What Can Social Networks Be Used For?

Social networks can provide a range of benefits to members of an organisation:

Support for learning: Social networks can enhance informal learning and support social connections within groups of learners and with those involved in the support of learning.

Support for members of an organisation: Social networks can potentially be used my all members of an organisation, and not just those involved in working with students. Social networks can help the development of communities of practice.

Engaging with others: Passive use of social networks can provide valuable business,intelligence and feedback on institutional

Copyright @ 2021 **ijearst. All rights reserved.**

services (although this may give rise to ethical concerns).

Ease of access to information and applications: The ease of use of many social networking services can provide benefits to users by simplifying access to other tools and applications. The Facebook Platform provides an example of how a social networking service can be used as an environment for other tools.

Common interface: A possible benefit of social networks may be the common interface which spans work / social boundaries. Since such services are often used in a personal capacity the interface and the way the service works may be familiar, thus minimizing training and support needed to exploit the services in a professional context. This can, however, also be a barrier to those who wish to have strict boundaries between work and social activities.

Examples of Social Networking Services

Examples of popular social networking services include:

Facebook: Facebook is a social networking Web site that allows people to communicate with their friends and exchange information. In May 2007 Facebook launched the Facebook Platform which provides a framework for developers to create applications that interact with core Facebook features

MySpace: MySpace is a social networking Web site offering an interactive, user-submitted network of friends, personal profiles, blogs and groups, commonly used for sharing photos, music and videos..

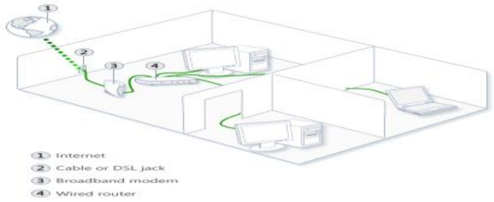
Ning: An online platform for creating social Web sites and social networks aimed at users who want to create networks around specific interests or have limited technical skills.

Twitter: Twitter is an example of a micro-blogging service. Twitter can be used in a variety of ways including sharing brief information with users and providing support for one's peers.

Note that this brief list of popular social networking services omits popular social sharing services such as Flickr and YouTube.

Opportunities and Challenges

The popularity and ease of use of social networking services have excited institutions with their potential in a variety of areas. However effective use of social networking services poses a number of challenges for institutions including long-term sustainability of the services; user concerns over use of social tools in a work or study context; a variety of technical issues and legal issues such as copyright, privacy, accessibility; etc. Institutions would be advised to consider carefully the implications before promoting significant use of such services.



Above diagrams show the clear idea about the networking function

Copyright @ 2021 ijearst. All rights reserved.

For the different computers to be able to distinguish between each other, every computer has a unique ID called MAC-address (Media Access Control Address). This address is not only unique on your network but unique for all devices that can be hooked up to a network. The MAC-address is tied to the hardware and has nothing to do with IP-addresses. Since all computers on the network receives everything that is sent out from all other computers the MAC-addresses is primarily used by the computers to filter out incoming network traffic that is addressed to the individual computer.

When a computer communicates with another computer on the network, it sends out both the other computers MAC-address and the MAC-address of its own. In that way the receiving computer will not only recognize that this packet is for me but also, who sent this data packet so a return response can be sent to the sender.

On an Ethernet network as described here, all computers hear all network traffic since they are connected to the same bus. This network structure is called multi-drop.

One problem with this network structure is that when you have, let say ten (10) computers on a network and they communicate frequently and due to that they sends out there data packets randomly, collisions occur when two or more computers sends data at the same time.

When that happens data gets corrupted and has to be resent. On a network that is heavy loaded even the resent packets collide with other packets and have to be resent again. In reality this soon becomes a bandwidth problem. If several computers communicate with each other at high speed they may not be able to utilize more than 25% of the total network bandwidth since the rest of the bandwidth is used for resending previously corrupted packets. The way to minimize this problem is to use network switches.

- **Server-Based Networks:**

In server-based network data files that will be used by all of the users are stored on the one server. With a server-based network, the network server stores a list of users who may use network resources and usually holds the resources as well. This will help by giving you a central point to set up permissions on the data files, and it will give you a central point from which to back up all of the data in case data loss should occur.

Network Communications:

- Computer networks use signals to transmit data, and protocols are the languages computers use to communicate.
- Protocols provide a variety of communications services to the computers on the network.
- Local area networks connect computers using a shared, half-duplex, baseband medium, and wide area networks link distant networks.
- Enterprise networks often consist of clients and servers on horizontal segments connected by a common backbone, while peer-to-peer networks consist of a small number of computers on a single LAN.

Advantages of Networking:

Copyright @ 2021 ijearst. All rights reserved.

- **Easy Communication:**

It is very easy to communicate through a network. People can communicate efficiently using a network with a group of people. They can enjoy the benefit of emails, instant messaging, telephony, video conferencing, chat rooms, etc.

- **Security:**

Sensitive files and programs on a network can be password protected. Then those files can only be accessed by the authorized users. This is another important advantage of networking when there are concerns about security issues. Also each and every user has their own set of privileges to prevent those accessing restricted files and programs.

- **Speed:**

Sharing and transferring files within networks is very rapid, depending on the type of network. This will save time while maintaining the integrity of files.

II. Literature Survey:-

1) A technique for computer detection and correction of spelling errors

AUTHORS: F. J. Damerau

The method described assumes that a word which cannot be found in a dictionary has at most one error, which might be a wrong, missing or extra letter or a single transposition. The unidentified input word is compared to the dictionary again, testing each time to see if the words match—assuming one of these errors occurred. During a test run on garbled text, correct identifications were made for over 95 percent of these error types.

2) LIBSVM: A library for support vector machines

AUTHORS: C.-C. Chang and C.-J. Lin

LIBSVM is a library for Support Vector Machines (SVMs). We have been actively developing this package since the year 2000. The goal is to help users to easily apply SVM to their applications. LIBSVM has gained wide popularity in machine learning and many other areas. In this article, we present all implementation details of LIBSVM. Issues such as solving SVM optimization problems theoretical convergence multiclass classification probability estimates and parameter selection are discussed in detail.

3) Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs

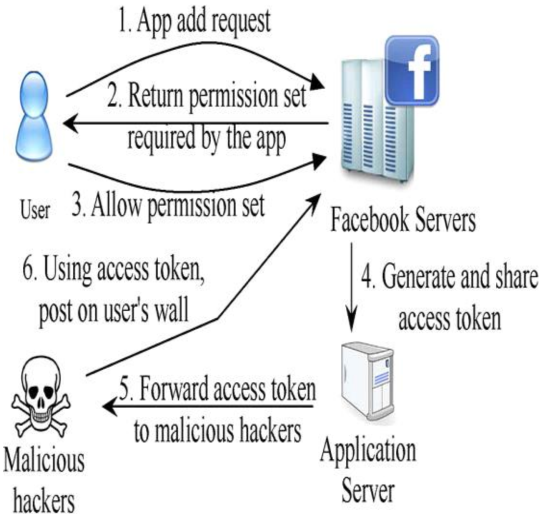
AUTHORS: J. Ma, L. K. Saul, S. Savage, and G. M. Voelker Malicious Web sites are a cornerstone of Internet criminal activities. As a result, there has been broad interest in developing systems to prevent the end user from visiting such sites. In this paper, we describe an approach to this problem based on automated URL classification, using statistical methods to discover the tell-tale lexical and host-based properties of malicious Web site URLs. These methods are able to learn highly predictive models by extracting and automatically analyzing tens of thousands of features potentially indicative of suspicious URLs. The resulting classifiers obtain 95-99%

accuracy, detecting large numbers of malicious Web sites from their URLs, with only modest false positives.

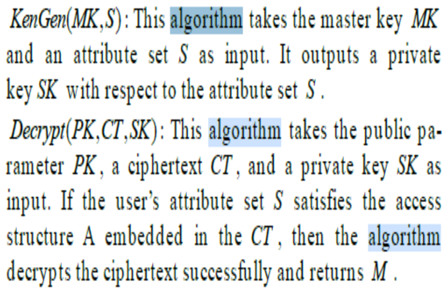
III. Related Work:-

Although ABE has shown its merits, user revocation and attribute revocation are the primary concerns. The revoca-tion problem is even more difficult peculiarly in CP-ABE schemes, because each attribute is shared by many users. This means that revocation for any attribute or any single user may affect the other users in the system. Recently, some work [5-9] has been proposed to solve this problem in efficient ways. Boldyreva et al. [5] presented an IBE scheme with efficient revocation, which is also suitable for KP-ABE. Nevertheless, it is not clear whether their scheme is suitable for CP-ABE. Yu et al. [6] provided an attribute based data sharing scheme with attribute revo-cation ability. This scheme was proved to be secure against chosen plaintext attacks (CPA) based on DBDH assump tion. However, the length of ciphertext and user's private key are proportional to the number of attributes in the attribute universe. In the key generation, encryption and decryption stages, computation involves all attributes in the attribute universe. Hence, it is expensive in com-munication and computation cost for users. Tysowski et al. [8] gave an easy method to perform user revocation operation by combining CP-ABE with re-encryption. In their scheme, each user belongs to a group and holds a group secret key issued by the group. However, their scheme does not resist collusion attack performed by r e-voked users cooperating with existing users. The reason is that each user's group secret key is same in the same group. The attributes of the revoked users can be used by the user in the same group without the specified attrib- utes. Additionally, we point out that there is the same security risk in the schemes [7, 9].

System-Architecture:-


1. App add request
2. Return permission set required by the app
User
3. Allow permission set
Facebook Servers
6. Using access token, post on user's wall
4. Generate and share access token
5. Forward access token to malicious hackers
Malicious hackers
Application Server

I. Basic idea for the SeDaSC methodology.


KenGen(*MK*,*S*): This algorithm takes the master key *MK* and an attribute set *S* as input. It outputs a private key *SK* with respect to the attribute set *S* .
Decrypt(*PK*,*CT*,*SK*): This algorithm takes the public pa-rameter *PK* , a ciphertext *CT* , and a private key *SK* as input. If the user's attribute set *S* satisfies the access structure A embedded in the *CT* , then the algorithm decrypts the ciphertext successfully and returns *M* .

iV Conclusion:-

We have introduced Fair Play, a system to detect both fraudulent and malware Google Play apps. Our experiments on a newly contributed longitudinal app dataset have shown that a high percentage of malware is involved in search rank fraud; both are accurately identified by Fair Play.

Copyright @ 2021 ijearst. All rights reserved.

In addition, we showed Fair Play's ability to discover hundreds of apps that evade Google Play's detection technology, including a new type of coercive fraud attack.

V.References:-

[1]Google Play. https://play.google.com/.

[2] Ezra Siegel. Fake Reviews in Google Play and Apple App Store. Appentive, 2014.

[3] Zach Miners. Report: Malware-infected Android apps spike in the Google Play store. PCWorld, 2014. [4] Stephanie Mlot. Top Android App a Scam, Pulled From Google Play. PCMag, 2014.

[5] Daniel Roberts. How to spot fake apps on the Google Play store. Fortune, 2015.

[6] Andy Greenberg. Malware Apps Spoof Android Market To Infect Phones. Forbes Security, 2014. IEEE Transactions on Knowledge and Data Engineering,Volume:29,Issue:6,Issue Date:June.1.2017 14

[7] Freelancer. http://www.freelancer.com.

[8] Fiverr. https://www.fiverr.com/.

[9]BestAppPromotion. www.bestreviewapp.com/.

[10] Gang Wang, Christo Wilson, Xiaohan Zhao, Yibo Zhu, Manish Mohanlal, Haitao Zheng, and Ben Y. Zhao. Serf and Turf: Crowdturfing for Fun and Profit. In Proceedings of ACM WWW. ACM, 2012.

[11] Jon Oberheide and Charlie Miller. Dissecting the Android Bouncer. SummerCon2012, New York, 2012.

[12] VirusTotal - Free Online Virus, Malware and URL Scanner. https: //www.virustotal.com/, Last accessed on May 2015.

[13] Iker Burguera, Urko Zurutuza, and Simin Nadjm-Tehrani. Crowdroid: Behavior-Based Malware Detection System for Android. In Proceedings of ACM SPSM, pages 15–26. ACM, 2011

. [14] Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer, and Yael Weiss. Andromaly: a Behavioral Malware Detection Framework for Android Devices. Intelligent Information Systems, 38(1):161–190, 2012.

[15] Michael Grace, Yajin Zhou, Qiang Zhang, Shihong Zou, and Xuxian Jiang. Riskranker: Scalable and Accurate Zero-day Android Malware Detection. In Proceedings of ACM MobiSys, 2012.

[16] Bhaskar Pratim Sarma, Ninghui Li, Chris Gates, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy. Android Permissions: a Perspective Combining Risks and Benefits. In Proceedings of ACM SACMAT, 2012.

[17] Hao Peng, Chris Gates, Bhaskar Sarma, Ninghui Li, Yuan Qi, Rahul Potharaju,

Copyright @ 2021 ijearst. All rights reserved.

Cristina Nita-Rotaru, and Ian Molloy. Using Probabilistic Generative Models for Ranking Risks of Android Apps. In Proceedings of ACM CCS, 2012.

[18] S.Y. Yerima, S. Sezer, and I. Muttik. Android Malware Detection Using Parallel Machine Learning Classifiers. In Proceedings of NGMAST, Sept 2014.

[19] Yajin Zhou and Xuxian Jiang. Dissecting Android Malware: Characterization and Evolution. In Proceedings of the IEEE S&P, pages 95–109. IEEE, 2012.

[20] Fraud Detection in Social Networks. https://users.cs.fiu.edu/ ∼carbunar/caspr.lab/socialfraud.html. [21] Google I/O 2013 - Getting Discovered on Google Play. www. youtube.com/watch?v=5Od2SuL2igA, 2013.

[22] Justin Sahs and Latifur Khan. A Machine Learning Approach to Android Malware Detection. In Proceedings of EISIC, 2012.

[23] Borja Sanz, Igor Santos, Carlos Laorden, Xabier Ugarte-Pedrero, Pablo Garcia Bringas, and Gonzalo Alvarez. Puma: Permission ´ usage to detect malware in android. In International Joint Conference CISIS12-ICEUTE´ 12-SOCO´ 12 Special Sessions, pages 289–298. Springer, 2013.

[24] Junting Ye and Leman Akoglu. Discovering opinion spammer groups by network footprints. In Machine Learning and Knowledge Discovery in Databases, pages 267–282. Springer, 2015.

[25] Leman Akoglu, Rishi Chandy, and Christos Faloutsos. Opinion Fraud Detection in Online Reviews by Network Effects. In Proceedings of ICWSM, 2013.

. Comput. Sci., 363(1):28–42, October 2006. [28] Kazuhisa Makino and Takeaki Uno. New algorithms for enumerating all maximal cliques. 3111:260–272, 2004.

[29] Takeaki Uno. An efficient algorithm for enumerating pseudo cliques. In Proceedings of ISAAC, 2007. [30] Steven Bird, Ewan Klein, and Edward Loper. Natural Language Processing with Python. O'Reilly, 2009.

[31] Bo Pang, Lillian Lee, and Shivakumar Vaithyanathan. Thumbs Up? Sentiment Classification Using Machine Learning Techniques. In Proceedings of EMNLP, 2002.

[32] John H. McDonald. Handbook of Biological Statistics. Sparky House Publishing, second edition, 2009.

M.MadhusudhanaRao Assistant Professor in sri sunflower college if engineering and Technology Lankapalli and also received Master degree from JNTUK University, Having 8+ Years of experience in faculty

Tandu Sravani is a student of sri sunflower college if Engineering and Technology Lankapalli Present she is pursuing her M.tech [Computer science & Engineering] degree from this college and she received B.tech(CSE) from the University of JNTU Kakinada

Copyright @ 2021 **ijearst. All rights reserved.**