

Search Rank Fraud and Malware Detection in Google Play

VEERAMSETTI PARVATHI DEVI

PG Scholar, Department of M.C.A,
S.K.B.R P.G College,
Amalapuram, E.G.Dt., A.P, India.
parvathiveeramsetti414@gmail.com

Mr. NAGA. SRINIVASA RAO*

Asst. Professor, Dept of M.C.A,
S.K.B.R P.G College,
Amalapuram, E.G.Dt., A.P, India.
naagaasrinu@gmail.com

Abstract

Fraudulent behaviors in Google Play, the most popular Android app market, fuel search rank abuse and malware proliferation. To identify malware, previous work has focused on app executable and permission analysis. We show that 75% of the identified malware apps engage in search rank fraud. FairPlay discovers hundreds of fraudulent apps that currently evade Google Bouncer's detection technology.

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

Keywords : Malware, Google, Feature extraction, Androids, Humanoid robots, Pragmatics, Gold

1. INTRODUCTION

1.1 Introduction

The commercial success of Android app markets such as Google Play [1] and the incentive model they offer to popular apps, make them appealing targets for fraudulent and malicious behaviors. Some fraudulent developers deceptively boost the search rank and popularity of their apps (e.g., through fake reviews and bogus installation counts) , while malicious developers use app markets as a launch pad for their malware . The

motivation for such behaviors is impact: app popularity surges translate into financial benefits and expedited malware proliferation. Fraudulent developers frequently exploit crowdsourcing sites (e.g., Freelancer [7], Fiverr [8], Best AppPromotion [9]) to hire teams of willing workers to commit fraud collectively, emulating realistic, spontaneous activities from unrelated people (i.e., "crowdturfing" [10]), see Figure 1 for an example. We call this behavior "search rank fraud". In addition, the efforts of Android

markets to identify and remove malware are not always successful. For instance, Google Play uses the Bouncer system to remove malware. However, out of the 7,756 Google Play apps we analyzed using VirusTotal [12], 12% (948) were flagged by at least one anti-virus tool and 2% (150) were identified as malware by at least 10 tools (see Figure 6). Previous mobile malware detection work has focused on dynamic analysis of app executables as well as static analysis of code and permissions. However, recent Android malware analysis revealed that malware evolves quickly to bypass anti-virus tools [19].

1.2 Purpose:

We seek to identify both malware and search rank fraud subjects in Google Play. This combination is not arbitrary: we posit that malicious developers resort to search rank fraud to boost the impact of their malware.

1.3 Scope:

The efforts of Android markets to identify and remove malware are not always successful. For instance, Google Play uses the Bouncer system to remove malware. However, out of the 7,756 Google Play apps we analyzed using Virus Total, 12 percent (948) were flagged by at least one anti-virus tool and 2 percent (150) were identified as malware by at least 10 tools.

1.4 Motivation:

Fraudulent developers often ex sites (e.g., Freelancer, Fiverr, BestAppPromotion) to rent teams of willing workers to commit fraud place, emulating realistic, spontaneous activities. This is called behaviour search rank fraud. In addition, the efforts of automation markets to identify and exclude malware do not appear to be constantly roaring. As an example, Google Play uses the guard system to urge obviate malware. Previous mobile malware detection work has targeted on dynamic analysis of app executables also as static analysis of code and permissions. However, in recent malware automation analysis discovered that it evolves quickly to bypass anti-virus tools.

1.5 Overview:

We focus on the Android app market ecosystem of Google Play. The participants, consisting of users and developers, have Google accounts. Developers create and upload apps that consist of executables (i.e., apks”), a set of required permissions, and a description. The app market publishes this information, along with the app’s received reviews, ratings, aggregate rating (over both reviews and ratings), install count range (predefined buckets, e.g., 50-100, 100-500), size, version number, price, time of last update, and a list of “similar” apps. Each review consists of a star rating ranging between 1-5 stars, and some text. The text is optional and consists of a title and a description. Google Play

limits the number of reviews displayed for an app to 4,000. Fig. 2 illustrates the participants in Google Play and their relations.

2. LITERATURE SURVEY

1.TITLE: “Opinion Fraud Detection in Online Reviews by Network Effects,” in Proc. 7th Int. AAI Conf. Weblogs Soc. Media, 2013, pp. 2–11.

AUTHORS: L. Akoglu, R. Chandy, and C. Faloutsos

ABSTRACT:

User-generated online reviews can play a significant role in the success of retail products, hotels, restaurants, etc. However, review systems are often targeted by opinion spammers who seek to distort the perceived quality of a product by creating fraudulent reviews. We propose a fast and effective framework, FRAUDEAGLE, for spotting fraudsters and fake reviews in online review datasets. Our method has several advantages: (1) it exploits the network effect among reviewers and products, unlike the vast majority of existing methods that focus on review text or behavioral analysis, (2) it consists of two complementary steps; scoring users and reviews for fraud detection, and grouping for visualization and sensemaking, (3) it operates in a completely unsupervised fashion requiring no labeled data,

while still incorporating side information if available, and (4) it is scalable to large datasets as its run time grows linearly with network size. We demonstrate the effectiveness of our framework on synthetic and real datasets; where FRAUDEAGLE successfully reveals fraud-bots in a large online app review database.

2. TITLE: Discovery of Ranking Fraud for Mobile Apps

AUTHORS: Hengshu Zhu, Hui Xiong

ABSTRACT:

Ranking fraud in the mobile App market refers to fraudulent or deceptive activities which have a purpose of bumping up the Apps in the popularity list. Indeed, it becomes more and more frequent for App developers to use shady means, such as inflating their Apps sales or posting phony App ratings, to commit ranking fraud. While the importance of preventing ranking fraud has been widely recognized, there is limited understanding and research in this area. To this end, in this paper, we provide a holistic view of ranking fraud and propose a ranking fraud detection system for mobile Apps. Specifically, we first propose to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Apps. Such leading sessions can be leveraged for detecting the local anomaly instead of

global anomaly of App rankings. Furthermore, we investigate three types of evidences, i.e., ranking based evidences, rating based evidences and review based evidences, by modeling Apps ranking, rating and review behaviors through statistical hypotheses tests. In addition, we propose an optimization based aggregation method to integrate all the evidences for fraud detection. Finally, we evaluate the proposed system with real-world App data collected from the iOS App Store for a long time period. In the experiments, we validate the effectiveness of the proposed system, and show the scalability of the detection algorithm as well as some regularity of ranking fraud activities.

3. TITLE: Survey on Fraud Ranking in Mobile Apps

AUTHORS: Monali Zende, Aruna Gupta

ABSTRACT:

Ranking fraud in the mobile App business suggest to false or tricky exercises which have a motivation behind, knocking up the Apps in the fame list. Now a days, many shady means are used more frequently by app developers, such expanding their Apps business or posting imposter App evaluations, to confer positioning misrepresentation. There is a limited understanding and research area for preventing ranking fraud. This paper gives a whole

perspective of positioning misrepresentation and describes a Ranking fraud identification framework for mobile Apps. This work is grouped into three category. First is web ranking spam detection, second Is online review spam detection and last one is mobile app recommendation. The Web ranking spam refers to any deliberate actions which bring to selected Web pages an unjustifiable favorable relevance or importance. Review spam is designed to give unfair view of some products so as to influence the consumers perception of the products by directly or indirectly influuating or damaging the product s reputation.

4. TITLE: MobSafe: Forensic Analysis for Android Applications and detection Of Fraud Apps Using CloudStack and Data Mining

AUTHORS: Patil Rohini, Kale Pallavi

ABSTRACT:

Nowadays there are so many applications available on internet because of that user can not always get correct or true reviews about the product on internet. So we can check for more than 2 sites, for reviews of same product. The reviews may be fake on individual sites. But after comparing reviews from 2 sites we can get more clear idea. Hence we can get higher probability of getting real reviews. So we are proposing a system to develop a android application that will take reviews from two

different websites for single product, and analyze them with NLP for positive negative rating. In this, User will give 2 different URLs from 2 different sites for same product to system as input. For every URL Reviews and comments will be fetched separately and analyzed with NLP for positive negative rating. Then their rating will be combined together with average to give final rating for the product. In this paper we propose the system to develop an android app which helps to detect fraud apps using cloudstack and data mining. To develop proposed system we use two methods natural language processing and Kmeans algorithm.

5. TITLE: FairPlay: Fraud and Malware Detection in Google Play

AUTHORS: Mahmudur Rahman, Mizanur Rahman

ABSTRACT:

Fraudulent behaviors in Google's Android app market fuel search rank abuse and malware proliferation. We present FairPlay, a novel system that uncovers both malware and search rank fraud apps, by picking out trails that fraudsters leave behind. To identify suspicious apps, FairPlay's PCF algorithm correlates

review activities and uniquely combines detected review relations with linguistic and behavioral signals gleaned from longitudinal Google Play app data. We contribute a new longitudinal app dataset to the community, which consists of over 87K apps, 2.9M reviews, and 2.4M reviewers, collected over half a year. FairPlay achieves over 95% accuracy in classifying gold standard datasets of malware, fraudulent and legitimate apps. We show that 75% of the identified malware apps engage in search rank fraud. FairPlay discovers hundreds of fraudulent apps that currently evade Google Bouncer's detection technology, and reveals a new type of attack campaign, where users are harassed into writing positive reviews, and install and review other apps.

3. PROBLEM STATEMENT

In the existing system, the malware threat for mobile phones is expected to increase with the functionality enhancement of mobile phones. This threat is increased with the surge in population of smart phones instilled with stable Internet access which provides attractive targets for malware developers.

In the existing system, in the smart phone market, Android is currently the most popular smart phone operating system. Due to this popularity and also to its open source nature,

Android-based smart phones are now an ideal target for attackers. Since the number of malware designed for Android devices is increasing fast, Android users are looking for security solutions aimed at preventing malicious actions from damaging their smart phones.

3.1 Disadvantages

There are no time related co-review behaviors. There is no fraudulent review filter.

4. PROPOSED SYSTEM

Unlike existing solutions, the proposed system builds this work on the observation that fraudulent and malicious behaviors leave behind telltale signs on app markets. The proposed system uncovers these nefarious acts by picking out such trails.

For instance, the high cost of setting up valid Google Play accounts forces fraudsters to reuse their accounts across review writing jobs, making them likely to review more apps in common than regular users. Resource constraints can compel fraudsters to post reviews within short time intervals. Legitimate users affected by malware may report unpleasant experiences in their reviews. Increases in the number of requested permissions from one version to the next, which we will call “permission ramps”, may indicate benign to malware (Jekyll-Hyde) transitions.

Advantages

4.1 Identifying both malware and search rank fraud subjects in Google Play. Implemented Graph Based Opinion Spam Detection.

5. IMPLEMENTATION

5.1 Web Server

In this module, the Web Server has to login by using valid user name and password. After login successful he can do some operations such as View End User and Authorize, View Apps Developer and Authorize, Add Fileter, View all Mobile Manuals, View all uploaded apps with rank and ratings details, View all Apps with review, co review and Recommend details, View all Search Rank Fraud User, View all Malware details for Apps, View all Apps pos and neg behaviors, View Secret key request and response, View App hits in chart(Rank), View App download in chart, View App Rating in chart, View No. Of time App rank fraud in chart.

5.2 Apps Developer

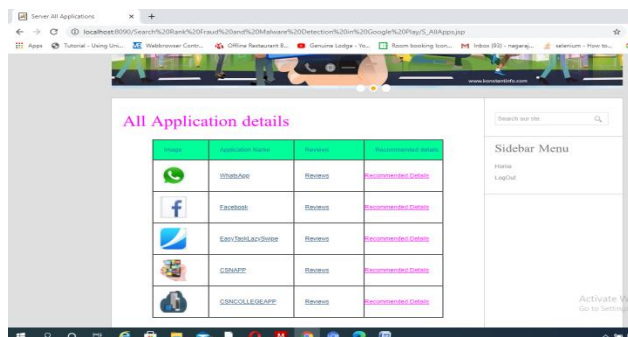
Add App

In this module, the admin can add the applications. If the admin want add the new app, he will enter application name, app description, mobile type, users, file name, application images and click on register. The details will be stored in the database.

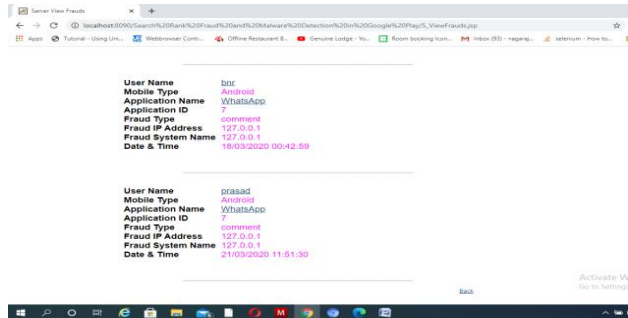
View application

In this module, when the admin clicks on view application, application name, app description, mobile type, users, file name, application images will be displayed.

6. OUTPUT RESULTS




| Image | Application Name | Platform | View Application Details |
|-------|------------------|----------|--|
| | WhatsApp | Android | View Application Details |
| | Facebook | Android | View Application Details |
| | Easy Social App | Android | View Application Details |
| | CSMAFT | Android | View Application Details |
| | CSMCOLEGAFF | Android | View Application Details |



User Name: indr
Mobile Type: Android
Application Name: WhatsApp
Application ID: 7
Fraud Type: comment
Fraud IP Address: 127.0.0.1
Fraud System Name: 127.0.0.1
Date & Time: 10/03/2020 00:42:59

User Name: prasad
Mobile Type: Android
Application Name: WhatsApp
Application ID: 7
Fraud Type: comment
Fraud IP Address: 127.0.0.1
Fraud System Name: 127.0.0.1
Date & Time: 21/03/2020 11:51:30

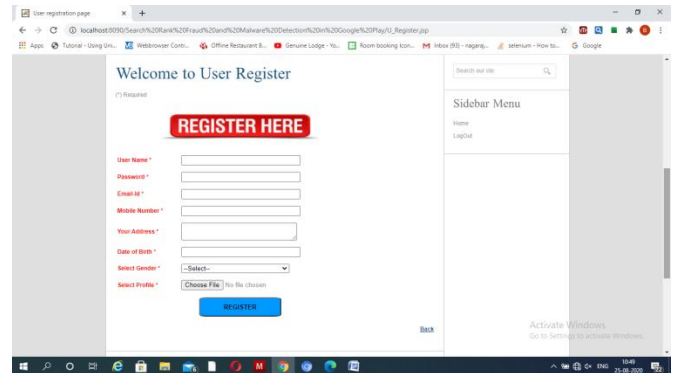


Positive Reviews of : WhatsApp

| Review | Rating | Date & Time | View |
|----------|--------|---------------------|----------------------|
| Best app | 5 | 08/09/2017 12:38:18 | View |
| Best app | 5 | 08/09/2017 12:38:20 | View |
| Best app | 5 | 08/09/2017 12:38:22 | View |
| Best app | 5 | 21/03/2020 11:51:06 | View |

Positive Reviews of : Facebook

| Review | Rating | Date & Time | View |
|---------------------------------------|--------|---------------------|----------------------|
| It's very good app for social network | 5 | 08/09/2017 15:56:16 | View |
| It's very good app for social network | 5 | 08/09/2017 15:56:21 | View |
| It's very good app for social network | 5 | 08/09/2017 15:56:24 | View |

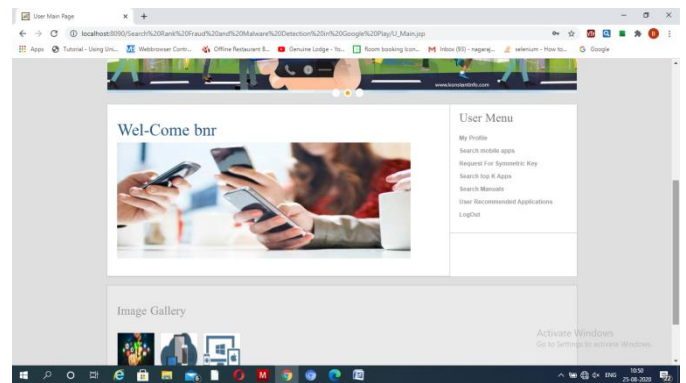


Welcome to User Register

REGISTER HERE

User Name *
 Password *
 Email *
 Mobile Number *
 Your Address *
 Date of Birth *
 Select Gender *
 Select Profile *

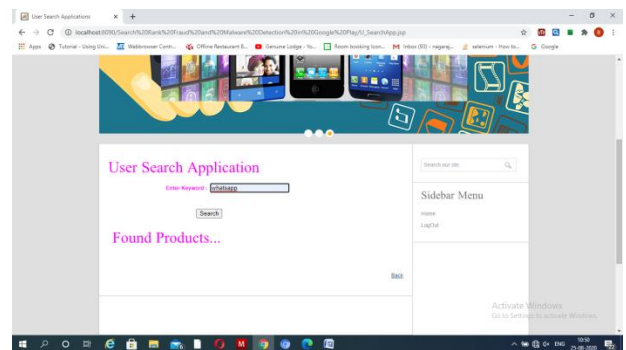
REGISTER



Wel-Come bnr

User Menu

- My Profile
- Search mobile apps
- Request For Appwrite: Key
- Search top 4 Apps
- Search Manuals
- User Recommended Applications
- Logout

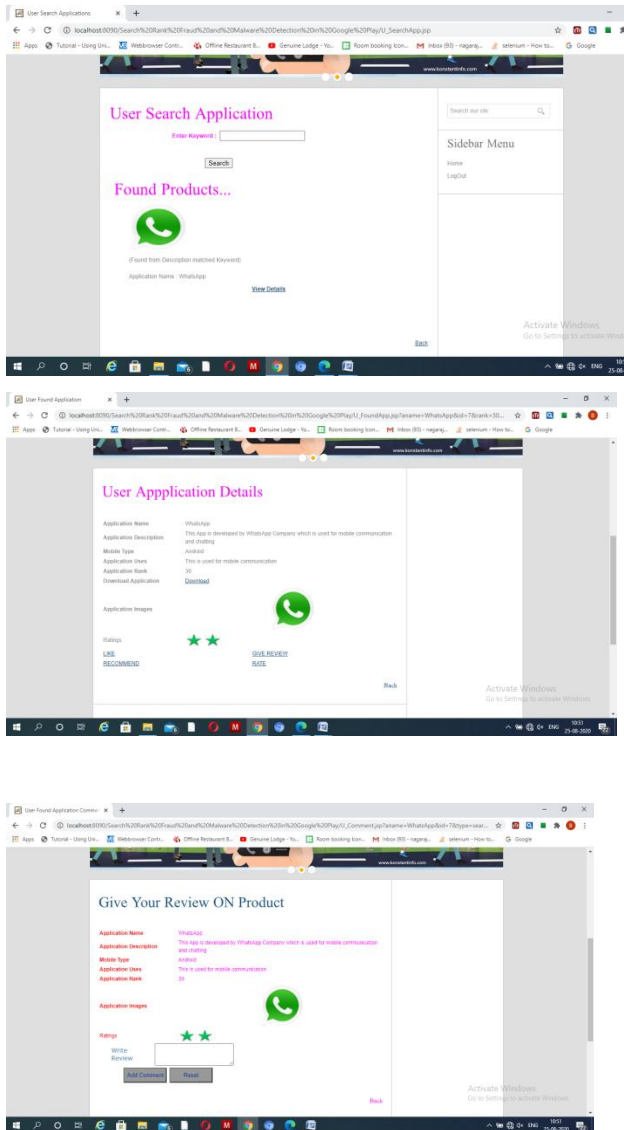


User Search Application

Enter Keyword:

Search

Found Products...



7. CONCLUSION

We have introduced FairPlay, 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 FairPlay.

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

8. BIBLIOGRAPHY

1. Improving product marketing by predicting early reviewers on E-Commerce websites

S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, “Improving product marketing by predicting early reviewers on E-Commerce websites,” Deleted Journal, no. 43, pp. 17–25, Apr. 2024, doi: 10.55529/ijrise.43.17.25.

2. Kodati, Dr Sarangam, et al. “Classification of SARS Cov-2 and Non-SARS Cov-2 Pneumonia Using CNN.” Journal of Prevention, Diagnosis and Management of Human Diseases (JPDMHD) 2799-1202, vol. 3, no. 06, 23 Nov. 2023, pp. 32–40, journal.hmjournals.com/index.php/JPDMHD/article/view/3406/2798, https://doi.org/10.55529/jpdmhd.36.32.40. Accessed 2 May 2024.

3. V. Srikanth, “CHRONIC KIDNEY DISEASE PREDICTION USING MACHINE LEARNING ALGORITHMS,” IJTE, pp. 106–109, Jan. 2023, [Online]. Available: <http://ijte.uk/archive/2023/CHRONIC-KIDNEY-DISEASE-PREDICTION-USING-MACHINE-LEARNING-ALGORITHMS.pdf>

4. V. SRIKANTH, “DETECTION OF PLAGIARISM USING ARTIFICIAL NEURAL NETWORKS,” International

Journal of Technology and Engineering, vol. XV, no. I, pp. 201–204, Feb. 2023, [Online]. Available: <http://ijte.uk/archive/2023/DETECTION-OF-PLAGIARISM-USING-ARTIFICIAL-NEURAL-NETWORKS.pdf>

5. V. SRIKANTH, “A REVIEW ON MODELING AND PREDICTING OF CYBER HACKING BREACHES,” IJTE, vol. XV, no. I, pp. 300–302, Mar. 2023, [Online]. Available: <http://ijte.uk/archive/2023/A-REVIEW-ON-MODELING-AND-PREDICTING-OF-CYBER-HACKING-BREACHES.pdf>

6. S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, “Detection of fake currency using machine learning models,” Deleted Journal, no. 41, pp. 31–38, Dec. 2023, doi: 10.55529/ijrise.41.31.38.

7. “Cyberspace and the Law: Cyber Security.” IOK STORE, iokstore.inkofknowledge.com/product-page/cyberspace-and-the-law. Accessed 2 May 2024.

8. “Data Structures Laboratory Manual.” IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-structures-laboratory-manual. Accessed 2 May 2024.

9. Data Analytics Using R Programming Lab.” IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-analytics-using-r-programming-lab. Accessed 2 May 2024.

10. V. Srikanth, Dr. I. Reddy, and Department of Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, 501301, India, “WIRELESS SECURITY PROTOCOLS (WEP,WPA,WPA2 & WPA3),” journal-article, 2019. [Online]. Available: <https://www.jetir.org/papers/JETIRDA06001.pdf>

10. V. SRIKANTH, “Secured ranked keyword search over encrypted data on cloud,” IJIEMR Transactions, vol. 07, no. 02, pp. 111–119, Feb. 2018, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/1121_approvedpaper.pdf

11. V. SRIKANTH, “A NOVEL METHOD FOR BUG DETECTION TECHNIQUES USING INSTANCE SELECTION AND FEATURE SELECTION,” IJIEMR Transactions, vol. 06, no. 12, pp. 337–344, Dec. 2017, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/976_approvedpaper.pdf

12 . SRIKANTH MCA, MTECH, MBA, “ANALYZING THE TWEETS AND DETECT TRAFFIC FROM TWITTER ANALYSIS,” Feb. 2017. [Online]. Available: <http://ijmtarc.in/Papers/Current%20Papers/IJMTARC-170309.pdf>

14 Srikanth, V. 2018. “Secret Sharing Algorithm Implementation on Single to Multi Cloud.” International Journal of Research 5 (01): 1036–41. <https://journals.pen2print.org/index.php/ijr/article/view/11641/11021>.

5. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, <https://doi.org/10.55529/jeet.34.16.21>. Accessed 20 Aug. 2023.

16. Babu, Dr P. Sankar, et al. “Intelligent Traffic Light Controller for Ambulance.” Journal of Image Processing and Intelligent Remote Sensing(JIPIRS) ISSN 2815-0953, vol. 3, no. 04, 19 July 2023, pp. 19–26, journal.hmjournals.com/index.php/JIPIRS/article/view/2425/2316, <https://doi.org/10.55529/jipirs.34.19.26>. Accessed 24 Aug. 2023.

17. S. Maddilety, et al. “Grid Synchronization Failure Detection on Sensing the Frequency and Voltage beyond the Ranges.” Journal of Energy Engineering and Thermodynamics, no. 35, 4 Aug. 2023, pp. 1–7, <https://doi.org/10.55529/jeet.35.1.7>. Accessed 2 May 2024.

18. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, <https://doi.org/10.55529/jeet.34.16.21>. Accessed 20 Aug