European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 4, 2020

Analysis on Cyber Crimes and its Malware using FRAppE Categoriser

ANSHY SINGH[1], NARENDRA MOHAN[2]
[1]*Department of Computer Engineering and Application*
GLA UNIVERSITY, MATHURA
anshy.singh@gla.ac.in
[2]*Department of Computer Engineering and Application*
GLA UNIVERSITY, MATHURA
narendra.mohan@gla.ac.in

Abstract: Together with 20 billion includes each day, 0.33-party Apps may be a critical purpose for the attraction not withstanding addictiveness of Facebook. Unfortunately, cyber criminals get went to the acknowledgment the possibly of Applying Facebooks near scattering malware however spontaneous mail. Up to now, the examination close by corporation gives committed to revealing noxious substance but advertisements. On this file, a massive detail parents question the problem: delivered some form of Facebook programming, can real a massive element parents find out inside the event that it's miles noxious? Our very own fundamental percentage is in building FRAppE Facebook's Thorough Request Evaluator in all likelihood the vital tool dedicated to revealing vindictive Facebooks in Facebook. To create FRAppE, the extra part of us rent actualities received essentially through looking on the submitting conduct of 111K Facebooks decided in some unspecified time within the destiny of 2 billion clients in Facebook. Initially, the extensive majority human beings understand a few attributes which will help in reality each person separate pernicious Facebooks with the beneficial aid of no longer malignant individuals.

Keywords: Measurement, Security, Malicious Facebooks, Profiling Facebooks, Online Social Networks

1. Introduction

Online social networks (OSNs) engage just as move 0. gathering introductions (applications) to improve the buyer celebrate in on the one's levels. Such overhauls contain beguiling or alluring methods for contributing among on-line colleagues and great conveying exercises, for example, playing entertainments or checking out tunes. For instance, Face book gives designs an API [2] that energizes utility turning into an individual from into the Face book benefactor experience. Here are 500K projects realistic on Face book [3], and all points considered, 20M bundles are brought each day [1]. Also, several programs created and stay to be a really colossal benefactor base. For instance, Farm Ville and City Ville programs require 26.5M and 42.8M clients to date. Starting late, software engineers to begun building up the universality of this pariah

Bundles stage and distribution vindictive introductions [4]–[6] Savage projects can flexibly a beneficial business association to developers, known the noticeable quality of OSNs, with Face book the utilization of the way with 900M powerful clients [7]. There are cut off a procedures that developers can salary by means of a noxious utility: 1) the product can gather tremendous amounts of clients and their accomplices to unfurl spontaneous mail; 2) the product can gather clients' non-open records along with email manage, home city, and manliness; and three) the product can harvest‖ through creation explicit malignant applications well known. To stamp subjects extra horrendous, the relationship of pernicious bundles is ventured forward with the guide of arranged to-lease tool boxs starting at $25 [8]. In that capacity, there's motivation and chance, and therefore, there are various poisonous applications distribution on Face book continually [9]. In spite of the over disturbing examples, these days a client has

really bound data at the period of presenting a product program programming on Face book. Thusly, the problem is the going with 20 million introduces a day, zero.33-birthday festivity programs zone primary reason for the acknowledgment and addictiveness of Face book. Improperly, programmers have chosen out the likely of the use of Applications for spreading malware and standard mail. The issue is commonly significant; moreover, we find that similarly a base 13% about orders on our dataset would malicious. With the objective an extended way, the exploration bunch keeping need concentrated on distinguishing malicious entrance and fights. In this task, our direction duty will be in creating FRAppE—Face book's intensive.

Provision Evaluator arguably that initial gadget focused around identifying pernicious projects ahead Facebook. Should expansion FRAppE, we utilize information gathered through utilizing searching the presenting direct for 111K Facebook bundles seen over 2. 2 million clients for Facebook. In we catch a situated for works that support us recognize pernicious projects from benevolent ones. For example, we discover that malicious programs regularly percentage names by unique programs, and they normally request less permission than benign packages. Most research diagnosed with unsolicited mail and malfunction on Facebook has battered on distinguishing noxious posts and social direct mail movements [10] – [12]. In the meantime, in a seemingly in contrary stride, Facebook has disassembled its software application score usefulness as of overdue. A current-day art work examines how software program authorizations and group value determinations connect to safety risks of Facebook packages [13].
At long remaining has a company constructed completely input ambitious endeavours to rank programs, as an example, What's App [14]; but the ones might be intense in a while; thus far they are becoming little choice. We speak about past artwork in extra detail in Section VIII. In this paper, we create FRAppE, a tough and speedy of gifted grouping strategies for spotting whether or not or not a utility is malignant or now not. To gather FRAppE, we employ facts from MyPage Keeper, a safety utility in Facebook [15] [18-21] that presentations the Facebook outlines of .2 million clients. We take a look at 111K programs that made 90 one million posts extra than 9 months. This is arguably the essential thorough evaluation concentrated on malicious Facebook packages that spotlights on measuring, summarizing, and comprehension noxious programs and integrates these facts into a powerful popularity method. Our art work makes the accompanying key commitments.

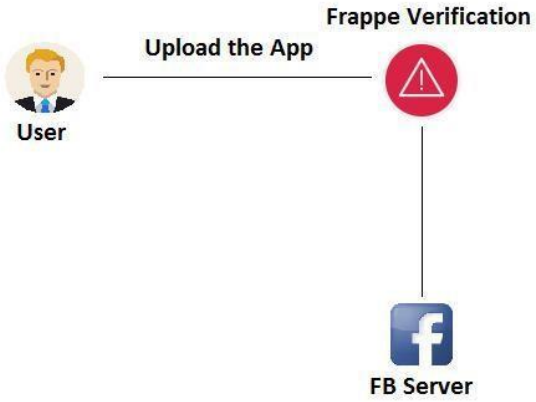

Fig: 1, Process of hackers using malicious apps.

2. Related Work

FB provide a synopsis related MyPage Keeper (our primary statistics supply), together with compress your datasets we use internal this kind of file. 2. 1 Fb Blog Fb makes it ability for 1/3-birthday celebration builders to offer groups to assist client's with Facebooks. Rather than regular pc alongside with touch display cell phone Facebooks, installation of a Fb software with the beneficial resource of approach for

consumer does not require a character coexisting with doing a Facebook software twofold. As an preference, on every occasion a client gives a Fb software program to help her page, an character lets in the Facebook software body server: (a) concur to get proper into a subset within the information aspect with the useful resource of factor for the consumer's Fb net web page (e. G., your customer's mail address), along (b) concur to execute decided on bodily video games for an man or woman (e. H., an opportunity to article for the consumer's divider). Fb reserves those form of authorizations to help any product basically thru giving a wonderful Oath 3. Zero [4] photo inside the path of the product server for every and each consumer who institutions the Facebook application frame. At that aspect, the Facebook application body can actually get entry to your facts at the aspect of carry out your explicitly-allowed sporting activities for a person. Speaks for your techniques intrigued thru your installation along approach of aFb programming. Operation associated with malignant Facebooks. Dangerous Facebooks generally run the accompanying. Step1: Online programmers urge purchasers to introduce your iPhone Facebook, for the maximum thing along some false guarantee (e. G., simply free iPads). Step 2: The minute a consumer establishment your iPhone Facebook, that diverts a person to an internet site wherein the purchaser may be asked to execute occupations, for example, gambling out a survey, all another time at the same time as the use of draw related to faux rewards. Step: three the specific iPhone Facebook a brief time later receives to individual information (e. G., beginning date) on the patron's net page, which the digital highbrow oppressor may also use to assist profits. Step four: The particular iPhone Facebook makes malicious substance for a person to assist bait your customer's amigos to introduce indistinguishable iPhone Facebook (or a couple of different pernicious iPhone Facebook, thinking about we're able to see later). Along the ones traces your circuit keeps at the identical time as the usage of iPhone Facebook and in addition interesting Facebooks reaching an ever-growing quantity of customers. Data this is near domestic and moreover studies can be "offered" to assist outsiders [2] to assist in some unspecified time in the destiny sales your cyber-terrorist.

3. Literature survey:

A strategy for PC acknowledgment and development of proposing blunders. Those strategy delineated acknowledges that an explanation which couldn't be put to a word reference need all things considered extraordinary you quit offering on that one misstep, which may an opportunity to be an off base, absent or additionally astonishing let or A flat out interpretation. The anonymous enter articulations is as contradicted of the word reference wherever again. Endeavouring out at whatever point to look if the expressions solid accepting this sort of blunders came to fruition.

LIBSVM: A library to backing vector machine lin LIBSVM is A library for backing vector. LIBSVM: A library for backing vector machines lin LIBSVM is A library to help vector Machines (SVMs).

That objective will be with assistance clients will effortlessly provision SVM should their requisition. LIBSVM need picked up totally Notoriety done machine Taking in Furthermore Numerous different regions. In this article, we exhibit all usage points for LIBSVM. problems for example, such that fathoming SVM streamlining issues hypothetical joining multiclass arrangement likelihood estimates and parameter determination need aid talked about on point of interest.

Beyond boycotts: Taking in will encounter malignant Web regions beginning with dubious URLs noxious Web areas would an establishment for web criminal games works out? Similarly, an outcome, there need been expansive excitement toward Creating systems should keep to keep special from wandering like locales. Here, we characterize a strategy that is inconvenience dependent on modernized URL type, the utilization of measurable procedures to discover the obvious lexical and mass principally made completely assets of brutal Web site URLs.

Intend and evaluation of a continuous URL garbage mail sifting supplier. Closely following the generous determination of web repayment counting informal organizations and more URL sharpeners, tricks,

phishing, and malware carry end up customary threats. Despite tremendous investigations, email-based spontaneous mail sifting methodologies normally miss the mark for protecting stand-out net contributions. To higher location this need, we present ruler, an ongoing device that creeps URLs as they might be concede to web conveniences and characterizes whether the URLs straight to spontaneous mail. We look at the attainability of ruler and the basic undertakings that upward push up due to the type of web backer spontaneous mail. We show that ruler can convey right, continuous wellbeing, however here are basic highlights of spontaneous mail do now not sum up at some phase in net administrations. In remarkable, we find that garbage mail focused on email subjectively contrasts in broad methodologies from spontaneous mail crusades focused on Twitter. We venture to every part of the distinctions among messages and Twitter garbage mail, altogether with the abuse of open web net web introducing and redirector administrations.

Noticing spammers on interpersonal organizations. Person to person communication has a notable route for customers to full fill and have collaboration on-line. Clients invest an exceptional amount of energy in celebrated informal community frameworks (alongside Face book, My Space, or Twitter), stockpiling and appropriation an abundance of individual insights. This measurement, notwithstanding the chance of reaching heaps of customers, furthermore bids the consideration of cybercriminals. For example, cybercriminals may make the greatest the inferred accept connections among administrators to trap victims to merciless sites.

4. Existing System

Here, the studies network is related to OSN request definitely, most research related with junk mail and malfunction on Facebook has targeted on identifying cruel posts and social junk mail operations.

Gao et al. Investigated presents on the partitions about 3. Five million Facebook clients and affirmed that 10% from claiming joins presented ahead Facebook partitions would garbage mail. They moreover provided techniques to choose out compromised payments and unsolicited mail campaigns.

Yang et al. And Benevento et al. Advanced strategies to understand money owed of spammers on Twitter. Others have projected a honey-pot-based totally software program to discover unsolicited mail payments on OSNs. 4)Yardi et al. analysed behavioural patterns amongst unsolicited mail bills in Twitter.

Chia etal. CHeck crazy danger signalling on the privateers meddling from claiming face book projects and reason that contemporary varieties of group keeping rankings would not dependable indications And indications of those security dangers connected with a programming.

1)

4.1 Drawbacks of Existing Methods

1) Present machine workings focused handiest on categorizing character URLs or posts as direct mail, however no longer cantered on figuring out malicious software program that are the principle foundation of unsolicited mail on Facebook.
2) Current device works focused on money owed created via the usage of spammers in preference to malicious software.
3) Existing device supplied exceptional an immoderate-stage assessment approximately extortions to the Facebook graph and do not deliver any evaluation of the device.

5. Proposed Method

1In this venture, we broaden FRAppE, an assortment of unpractised class procedures for distinguishing whether a utility is malevolent or no more. To amass FRAppE, we use information from My Page Guardian, an insurance utility in Facebook.

We discover that vindictive programming widely changes from amiable programming program concerning 2 preparing of capacities: On-Demand descriptors and Aggregation-Based Features.
We blessing two variants of our pernicious programming program catogorizer—FRAppE Lite and FRAppE.
FRAppE Lite is a lightweight form that utilizes wonderful the product capacities accessible on name for. Given a particular programming ID, FRAppE Lite creeps the accessible if the need arises for capacities for that application and assesses the utility dependent on the one's capacities in genuine time.
FRAppE—a malevolent application locator that utilizes our accumulation put together highlights comparatively to the with respect to request capabilities.

5.1 Advantages of Proposed System

The suggested work of art will be seemingly those principal finish investigations that practice clinched alongside pernicious Facebook projects that specializes over quantifying, profiling, Furthermore Realities pernicious projects also synthesizes these records under a capable identification technobabble.
Several features utilized Toward FRAppE, all things considered for the distinguish redirect URIs, those assortments of needed permissions, and the utilization of various customer IDs done utility establishment URLs, are solid of the Development of hackers.
3) Not the usage of unique patron IDs in utility installation URLs could possibly restrict the capability of hackers to tool their application to propagate every distinctive.

5.2 Objectives and Goals

The objective will be on settle on frappe as a venture at making a free watchdog for requisition evaluation also ranking, along these lines as to caution Facebook clients in front of introducing requisitions.

6. Problem Definitions

Hackers need began out taking profit of the Ubiquity about this third-party requisition stage and deploying pernicious programming. Pernicious provisions camwood offers a gainful business undertaking to hackers, provided for those Ubiquity from claiming OSNs, with Facebook fundamental those way for 900M enthusiastic customers. There are huge numbers systems that hackers might addition starting with A pernicious product system: those programming could arrive at monstrous numbers about clients Also their buddies with unfold immediate mail, those utility might procure customers' particular Realities including electronic mail adapt with, home metropolis, and sexual orientation. The provision region could ―re-produce" thru settling on separate pernicious projects mainstream.

6.1 Modules

1. Data collection

The records arrangement problem to be a subcomponent: the social occasion of Face book programs by means of URLs and pressed for URL distributing on. At any point the component gets a Face book usefulness by URL, it implements a crawling filament that obtain following the total redirections of the URL and looks subordinate upon the contrasting IP addresses. The crawling sequence demand completes the person's recuperated URL and IP handcuffs of the tweet records and pushes it directly below a column. Regarding delineation we've understood, our crawler can't accomplish vindictive score URLs when they utilize prohibitive distributing on to Abstain as of crawlers. However, because of those To our distinguishing proof machine is no more rely upon the skills for showing up URLs, it really meets desires openly regarding crawler avoidances.

2. Highlight extraction

Those trademarks drawing out component require 3 subcomponents: arrangement of similar territories, revelation get remains URLs, in addition extricating brand name vectors. On orchestrate a situated up, My Page Keeper assesses every embedded URL within that is submitted. Our key assortment lies done perceiving least difficult the social setting to the magnificence of the URL and the associated set up. Besides, we use reality that we require help looking at changed buyer that may help us reveal a epidemic extend. It recognizes region for spam key articulations in. 'FREE', 'Arrangement' and then some 'Rush'.

3. Preparing

The teaching module wants two subcomponents: recuperation of verification positions besides getting ready of the categoriser. On we usage a logged off oversaw attainment will think calculation, those trademark vectors for teaching need help enormously more prepared over limit vectors to populace. To name those teaching vectors, we use the record notoriety; URLs beginning with suspended money owed are pondered malicious while URLs from enthusiastic bills are contemplated positive. We infrequently update our categoriser the utilization for known planning vectors.

4. Grouping and recognition

The group changeable implements our categoriser individual's utilization for come into limit vectors should organize dicey URLs. When those categoriser incomes a measure of poisonous trademark vectors, this relic norms the telling URLs information also as dicey The sort part makes use of A machine Taking in categoriser basically considering backing vector Machines, just as makes usage of a couple of close By Also external white timetables And boycotts that guide mood subordinate upon the machine And impact the general accuracy. The class component get a URL and the cohered social association capacities amassed in the past endeavour. These URLs, recognized also as dubious, may an opportunity to be familiar on protection experts then again extra latest component evaluation circumstances for an inside and out assessment.

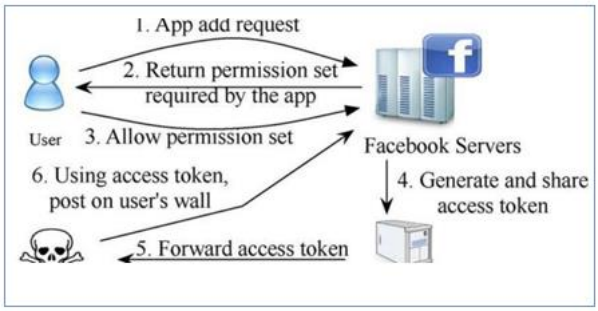

Figure.2. System Architecture

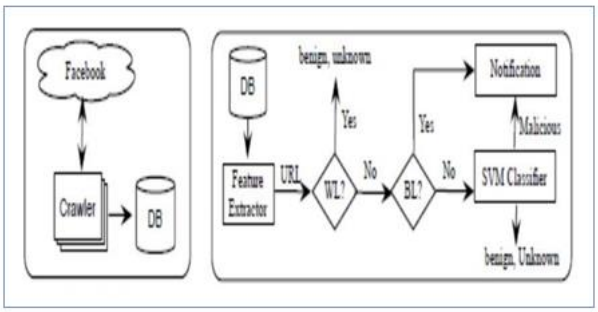

Figure.3. System Model

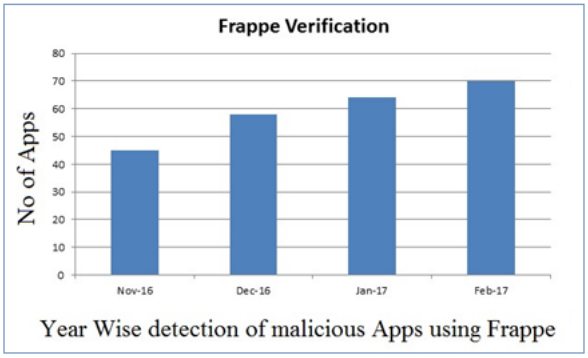

Figure.4. Frappe verification

Operation about pernicious applications: pernicious. Facebook requisitions for the most part work Similarly as takes after. • step 1: Intruders substantiate clients with set in the app, normally with a couple blunder guarantee (e. G., allowed iPads). • step 2: once a purchaser installs the app, it redirects the purchaser on A web page.

Step 3: the app from that point onwards accesses private Realities (e. G., conveyance date) starting with those consumer's profile, which the hackers might hypothetically use with benefit. • step 4: the app makes pernicious presents once sake of the purchaser with allure those user's pals with place in the rise to app.

Along these lines the cycle keeps for the app or colluding applications accomplishing progressively a greater amount client. Private data alternately surveys might a chance to be ―offered" to 1/3 gatherings will at long last wage those hackers.

Step 5: In this paper, the admin plays the predominant position to identify the malicious apps within the face book. Every malicious apps have some issues to install within the consumer account. Step 6: Advanced Frappe is the proposed machine to discover each malicious app with some of the parameters like timeline messages, versions of apps, url verification.

Step 7: Based at the above parameters the Advanced Frappe verification works positively to test whether the apps are malicious apps or no longer.

Expected Results

This application is developed in java with netbeans and mysql as database.

1. Face book Rating efforts
2. Detecting spam accounts
3. Recommendations to Face book
4. Face book permission exploitation
5. Indirect face book promotions

7. Conclusion

Applications exhibit a fine route for software engineers upgrade enormous substance of substance on Face book. However, little is fathomed approximated the qualities of harmful bundles and how they work. Present work utilizes a huge quantity of noxious wood Facebook packs viewed in a multi month event when range, we trapped ward leading that compromising activities distinction basically beginning with mindful tasks as for two or three parts. For instance, harmful arrangements need help A first class deal all the more astounding week to present names on phenomenal bundles, furthermore they conventionally demand less need similar appraisal over mindful orders. Utilizing our discernments, we made FRAppE, a certifiable categoriser for perceiving noxious Facebook groups. For all intents and purposes strikingly, we featured the Ascent for AppNets wide social affairs of firmly co-partnered orders that grow one another. During this craftsmanship, the use of an exceptional Amount for poisonous Facebook arrangements we have an inclination with shows those malignant demands locale unit apparently make issue beginning by

delicate applications by plan B. To model, vindictive applications zone unit commonsense offers names for remarkable applications and they ordinarily request littler sum authorizations than slight applications.

References

[1] Pete, I.; Chua, Y.T. An Assessment of the Usability of Cybercrime Datasets. In Proceedings of the CSET @ USENIX Security Symposium, Santa Clara, CA, USA, 12 August 2019.
[2] Ngo, F.; Jaishankar, K. Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. Int. J. Cyber Criminol. 2017, 11, 1–9.
[3] Khusna, A.N.; Agustina, I. Implementation of Information Retrieval Using Tf–idf Weighting Method On Detik.Com's Website. In Proceedings of the 2018 12th International Conference on Telecommunication Systems, Services and Applications (TSSA), Yogyakarta, Indonesia, 4–5 October 2018; pp. 1–4.
[4] Zhang, G.Z. Computer Forensics Based on Data Mining. Appl. Mech. Mater. 2014, 536–537, 371–375. [CrossRef]
[5] Numan, M.; Subhan, F.; Khan, W.Z.; Hakak, S.; Haider, S.; Reddy, G.T.; Jolfaei, A.; Alazab, M. A Systematic Review on Clone Node Detection in Static Wireless Sensor Networks. IEEE Access 2020, 8, 65450–65461.
[6] Iwendi, C.; Jalil, Z.; Javed, A.R.; Gadekallu, T.R.; Kaluri, R.; Srivastava, G.; Jo, O. KeySplitWatermark: Zero Watermarking Algorithm for Software Protection against Cyber-Attacks. IEEE Access 2020.
[7] Bhattacharya, S.; Somayaji, S.R.K.; Maddikunta, K.P.; Kaluri, R.; Singh, S.; Gadekallu, R.T.; Alazab, M.; Tariq, U. A Novel PCA-Firefly Based XGBoost Classification Model for Intrusion Detection in Networks Using GPU. Electronics 2020, 9, 219.
[8] Jia, X.; He, D.; Kumar, N.; Choo, K.-K.R. Authenticated key agreement scheme for fog-driven IoT healthcare system. Wirel. Netw. 2019, 25, 4737–4750.
[9] Wu, L.; Zhang, Y.; Ma, M.; Kumar, N.; He, D. Certificateless searchable public key authenticated encryption with designated tester for cloud-assisted medical Internet of Things. Ann. Telecommun. 2019, 74, 423–434.
[10] Aggarwal, S.; Shojafar, M.; Kumar, N.; Conti, M. A New Secure Data Dissemination Model in Internet of Drones. In Proceedings of the ICC 2019–2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
[11] Wang, T.; Zheng, Z.; Bashir, A.K.; Jolfaei, A.; Xu, Y. FinPrivacy: A Privacy-Preserving Mechanism for Fingerprint Identification. ACM Trans. Internet Technol. 2018, 37, 111–116.
[12] Al Ridhawi, I.; Otoum, S.; Aloqaily, M.; Jararweh, Y.; Baker, T. Providing secure and reliable communication for next generation networks in smart cities. Sustain. Cities Soc. 2020, 56, 102080.
[13] Alloghani, M.; Baker, T.; Al-Jumeily, D.; Hussain, A.; Mustafina, J.; Aljaaf, A.J. A Systematic Review on Security and Privacy Issues in Mobile Devices and Systems. In Handbook of Computer Networks and Cyber Security; Gupta, B., Perez, G., Agrawal, D., Gupta, D., Eds.; Springer: Cham, Germany, 2020; pp. 585–608
[14] Reddy, G.T.; Swarna Priya, R.M.; Parimala, M.; Chowdhary, C.L.; Reddy, P.K.; Hakak, S.; Khan, W.Z. A deep neural networks based model for uninterrupted marine environment monitoring. Comput. Commun. 2020, 157, 64–75.
[15] Patel, H.; Singh Rajput, D.; Thippa Reddy, G.; Iwendi, C.; Kashif Bashir, A.; Jo, O. A review on classification of imbalanced data for wireless sensor networks. Int. J. Distrib. Sens. Netw. 2020.

[16] Reddy, G.T.; Reddy, M.P.K.; Lakshmanna, K.; Kaluri, R.; Rajput, D.S.; Srivastava, G.; Baker, T. Analysis of Dimensionality Reduction Techniques on Big Data. IEEE Access 2020, 8, 54776–54788.
[17] Ganesan, M.; Mayilvahanan, P. Cyber Crime Analysis in Social Media Using Data Mining Technique. Int. J. Pure Appl. Math. 2017, 116, 413–424.
[18] Bhardwaj, D., Jain, S.K., Singh, M.P. 2009. Estimation of network reliability for a fully connected network with unreliable nodes and unreliable edges using neuro optimization International Journal of Engineering, Transactions A: Basics 22(4), pp. 317-332
[19] Verma U., Bhardwaj D., 2020 "Design of Lightweight Authentication Protocol for Fog enabled Internet of Things - A Centralized Authentication Framework", International Journal of Communication Network and Information Security Vol 12, No 2 (2020) pp. 162-167
[20] Agarwal, R., Jalal, A. S.,Agrawal, S.C. Arya, K. V,' Fake and Live Fingerprint Detection Using Local Diagonal Extrema Pattern and Local Phase Quantization'. International Conference on Deep Learning, Artificial Intelligence and Robotics, (ICDLAIR) 2019'. MNIT JAIPUR, December 07-08, 2019 (Scopus Indexed)
[21] Agarwal, R., Jalal, A. S.,' Efficient Document Classification using Phrases Generated by Semi-Supervised Hierarchical Latent Dirichlet Allocation.' International Journal of Engineering Research in Computer Science and Engineering, NIT, Uttrakahnd:2018.
[22] Agarwal, R., Arya, K., & Shekhar, S. (2010, July). An architectural framework for web information retrieval based on user's navigational pattern. In 2010 5th International Conference on Industrial and Information Systems (pp. 195-200). IEEE.
[23] Agarwal, R., Arya, K. V., Shekhar, S., & Kumar, R. (2011, October). An Efficient Weighted Algorithm for Web Information Retrieval System. In 2011 International Conference on Computational Intelligence and Communication Networks (pp. 126-131). IEEE.
[24] Shekhar, S., Agrawal, R., & Arya, K. V. (2010, June). An architectural framework of a crawler for retrieving highly relevant web documents by filtering replicated web collections. In 2010 International Conference on Advances in Computer Engineering (pp. 29-33). IEEE.
[25] Varun K L Srivastava , N. Chandra Sekhar Reddy , Dr. Anubha Shrivastava, "An efficient Software Source Code Metrics for Implementing for Software quality analysis", International Journal of Emerging Trends in Engineering Research, Volume 7, No. 9 September 2019.