iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XI **Month of publication:** November 2021

DOI: https://doi.org/10.22214/ijraset.2021.38780

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

The Predicting and Prevention of Malware from Cyber Hacking Breaches in Online Social Network

Dr. C. K. Gomathy[1], Yadiki Jeevan Kumar Reddy[2], T. Suneel[3]
[1]*Assistant Professor, Dept. Of CSE, SCSVMV (Deemed to be University), Kanchipuram, TamilNadu, India*
[2, 3]*UG Scholar, Dept. Of CSE, SCSVMV (Deemed to be University), Kanchipuram, TamilNadu, India*

Abstract: ***Analyzing cyber incident information units is an essential approach for deepening our information of the evolution of the risk situation. This is a notably new studies topic, and plenty of research continue to be to be done. In this paper, we record a statistical evaluation of a breach incident information set similar to 12 years (2005–2017) of cyber hacking sports that encompass malware attacks. We display that, in evaluation to the findings suggested withinside the literature, each hacking breach incident inter-arrival instances and breach sizes need to be modeled through stochastic processes, instead of through distributions due to the fact they show off autocorrelations. Then, we recommend specific stochastic method fashions to, respectively, match the inter-arrival instances and the breach sizes. In this paper we be aware that, through reading their actions, we are able to classify malware right into a small quantity of Behavioral classes, every of which plays a restrained set of misbehaviors that signify them. These misbehaviors may be described through tracking capabilities belonging to exclusive platforms. In this paper we gift a singular host-primarily based totally malware detection machine in OSN which concurrently analyzes and correlates capabilities at 4 levels: kernel, application, person and package, to come across and prevent malicious behaviors. It has been designed to do not forget the ones behaviors traits of virtually each actual malware which may be observed withinside the wild. This prototype detects and efficaciously blocks greater than 96% of malicious apps, which come from 3 massive datasets with approximately 2,800 apps, through exploiting the cooperation of parallel classifiers and a behavioral signature-primarily based totally detector.***

Keywords: Cyber security, Malware, Emerging technology trends, Emerging cyber threats, Cyber attacks and countermeasures

I. INTRODUCTION

The Smartphone's and pills have turn out to be extraordinarily famous withinside the ultimate years. At the quit of 2014, the range of energetic cellular gadgets global turned into nearly 7 billions, and in evolved countries the ratio among cellular gadgets and those is envisioned as 120.8%. Given their huge distribution, and additionally their capabilities, withinside the ultimate years cellular gadgets have have become the principle goal for attackers. Android, the open supply operative system (OS) brought via way of means of Google, has presently the most important marketplace share, that's more than 80%. Due to the openness and popularity, Android is the principle goal of assaults towards cellular gadgets (98.5%), with extra than 1 million of malicious apps presently to be had withinside the wild. Malicious apps (generically known as malware) represent the principle vector for protection assaults towards cellular gadgets. Disguised as ordinary and beneficial apps, they conceal treacherous code which plays movements withinside the heritage that threatens the person privacy, the tool integrity, or maybe person's credit. Some not unusualplace examples of assaults achieved with the aid of using Android malicious apps are stealing contacts, login credentials, textual content messages, or maliciously subscribing the person to high priced top rate services. Furthermore, most of these misbehaviors may be achieved on Android gadgets with out the person noticing them (or while it's far too late). It has been these days reported1 that nearly 60% of present malware ship stealthy top rate charge SMS messages. Most of those behaviors are exhibited with the aid of using a class of apps known as Trojanized that may be observed in on-line marketplaces now no longer managed with the aid of using Google. However, additionally Google Play, the respectable marketplace for Android apps, has hosted apps that have been observed to be malicious2 . Along with the full-size boom of Android malware, numerous safety answers had been proposed with the aid of using the studies community, spanning from static or dynamic evaluation of apps, to making use of safety rules implementing statistics safety, to run-time enforcement. However, those answers nevertheless gift big drawbacks. In particular, they may be attack-specific, i.e. they commonly cognizance on And address a unmarried type of safety attack, e.g. privateness leaking, or privilege escalation (jail-breaking). Moreover, those frameworks typically require a custom OS. Apart from those advert hoc safety solutions, in an try to restriction the set of (dangerous) operations that an app can perform, Android has added its local safety mechanisms withinside the shape of permissions and apps isolation. These mechanisms, respectively, implement get admission to manipulate to safety important sources and operations, and keep away from that an app can intervene with the execution of every other one. However, each permissions and isolation mechanisms have proven weaknesses.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

II. LITERATURE SURVEY

A. Developments in Cyber Criminology

This article takes a examine how cybercrime evolved and the way these days cybercrime is frequently has its roots in pre-virtual technologies. The record additionally identifies a hit cybercrime manipulate examples that exhibit how capability danger regions have been addressed earlier than huge crime evolved. The paper examines the in all likelihood trajectory of cybercrime withinside the coming years and identifies approaches wherein destiny dangers can be minimized. It is concluded that technological tendencies have, in fact, fostered crime and that the ones liable for designing crime in new merchandise have now no longer absolutely understood the sights that era gives to people who are sufficiently inspired to dedicate crime. In the virtual age.

B. Cyber Security in the Banking Sector

This paper reviews the findings from a studies undertaking on cyber protection within side the Nigerian Internet banking enterprise, with the aid of using imparting the principle cyber protection breaches it has skilled, in conjunction with its cyber protection functionality and practices. An on-line survey changed into performed with a hundred skilled expert running in each the Nigerian banking and banking protection carrier sectors. Our findings screen a metamorphosis of the Nigerian cybercrime enterprise from low-tech cyber-enabled crimes to high-tech state-of-the-art breaches, with viruses, worms or Trojan infections; digital junk mail mails; and hacking being the pinnacle 3 maximum skilled breaches. In time period of cyber protection practices, banking specialists have obtained ok control in each guide and training. The loss of superior technology to save you and deal with cyber protection breaches and the unsatisfactory degree of legislative compliance, together, appear like the number one elements which have decreased cyber protection functionality in our pattern of bank

C. Socioeconomic Lifestyles

In Nigeria, youths worried in cybercrime, typically called the yahoo-boys, were extensively diagnosed as preserving a special life-style that confers a completely unique and/or an infamous identification on them within side the society. Against this background, this paper tested the perceptions of college students of a few decided on universities at the socioeconomic life of college students worried in cybercrime. Multi-level sampling method turned into hired for the choice of respondents; information turned into accrued via questionnaire and consciousness organization dialogue methods. Findings determined out that, 11 aleven though the majority of the respondents (59.5%) described the monetary strengths of Nigerian College Collegecollege students involved in cyber-crime as huge, plenty of them however, perceived this organization of university college students to be extravagant. A huge proportion of the respondents (62.5%) further believed that the perpetration of cybercrime negatively affects the academic average overall performance of university college students involved in it.

D. Report on Cyber Threat Calls

The exponential boom of the Internet interconnections has caused a full-size boom of cyber assault incidents regularly with disastrous and grievous consequences. Malware is the number one desire of weapon to perform malicious intents within side the cyberspace, both with the aid of using exploitation into present vulnerabilities or usage of precise traits of rising technologies. The development of more modern and effective malware safety mechanisms has been seemed asa urgent requirement inside facet the cyber safety network. To assist in accomplishing this goal, we first present an define of the most exploited vulnerabilities in contemporary hardware, software, and network layers. This is accompanied through evaluations of current latest mitigation strategies as why they do or do not work. We then speak new assault styles in rising technology including social media, cloud computing, phone technology, and essential infrastructure. Finally, we describe our speculative observations on destiny studies directions.

E. Online Fraud Drains Nigeria over N500 Billion

Nigeria can also additionally have misplaced over a whooping sum of N500 billion in 7 years on said and unreported instances of on-line fraud/cybercrime throughout predominant sectors of the economic system consisting of banking and telecommunication, CFAtech.ng investigations have shown. Despite 2015 being a first-rate yr. for cyber security in Nigeria, on the length whilst the the cybercrime invoice turned into signed into regulation through erstwhile President Goodluck Jonathan. The implications of this to people and companies are that cybercrime is thought to have been well described and felony results are connected to any defiance of this regulation.

F. Computer Crimes and Counter Measures in the Banking Sector

The growth within side the use of the facts and communique technology (ICT) centers which include computer systems and the Internet within side the perpetration of crook sports like spamming, credit score card frauds, ATM frauds, phishing, identification theft, denial-of-service, and a number of others has lend credence to the view that ICT is contributing to crime within side the banking sector.

An extra knowledge of such laptop crimes can also additionally supplement present protection practices through probable highlighting new regions of counter measures. This paper accordingly assesses whether or not those crimes may be absolutely eliminated or now no longer and whether or not the brand new technology banks revel in greater pc crimes than the antique era banks in Nigeria.

Based at the findings of this study, the paper concludes that overall eradication of laptop crimes isn't always viable however may be exceptionally decreased if inner manage measures are correctly installed vicinity inside a bank's organizational shape and that new era banks appear to revel in greater crimes than their antique era opposite numbers because of the truth that majority in their services, which can be automated, are subjected to technological modifications at a fast rate.

G. Cybercrimes: Analysis, Detection and Prevention

Over the years, the alarming boom of the internet and its vast splendor has brought on boom in protection threats. In Nigeria to- day, severa internet assisted crimes known as cybercrimes are committed each day in severa forms collectively with fraudulent virtual mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing. Cybercrime is a hazard in opposition to various establishments and those who're related to the net both thru their computer systems or cell technologies.

The exponential growth of this crime within side the society has come to be a robust difficulty that have to now no longer be overlooked.

The effect of this form of crime may be felt at the lives, financial system and worldwide recognition of a nation. Therefore, this paper specializes in the outstanding cybercrimes completed within side the numerous sectors in Nigeria and gives a quick evaluation of cybercrimes in tertiary establishments in Ekiti-State. In conclusion, detection and prevention strategies are highlighted with a purpose to fight cybercrimes in Nigeria.

III. EXISTING STATUS

It has been currently reported1 that nearly 60% of current malware ship stealthy top rate price SMS messages. Most of those behaviors are exhibited via way of means of a class of apps known as Trojanized that may be determined in on-line marketplaces now no longer managed via way of means of Google.

However, additionally Google Play, the reputable marketplace for Android apps, has hosted apps that have been determined to be malicious2. Along with the giant growth of Android malware, numerous safety answers were proposed via way of means of the studies community, spanning from static or dynamic evaluation of apps, to making use of safety regulations imposing statistics safety, to run-time enforcement.

However, these answers nonetheless gift good sized drawbacks. In particular, they may be attack-specific, i.e. they normally cognizance on and address a unmarried type of protection attack, e.g. privateness leaking , or privilege escalation (jail-breaking). Moreover, those frameworks typically require a custom OS.

Apart from those advert hoc protection answers, in an try and restriction the set of (dangerous) operations that an app can perform, Android has delivered its local protection mechanisms withinside the shape of permissions and apps isolation.

IV. PROPOSED METHOD

The essential novelty of framework is its cross-layer method, and a unique integration of techniques (a number of which already existing) that gives excessive efficacy with low overhead.

It has been conceived to show that a multilevel method makes it viable to dynamically come across maximum of current malware, proper at the tool with restricted overhead. To affirm that such method is certainly viable, a massive huge set of checks were executed to show empirically its efficacy.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

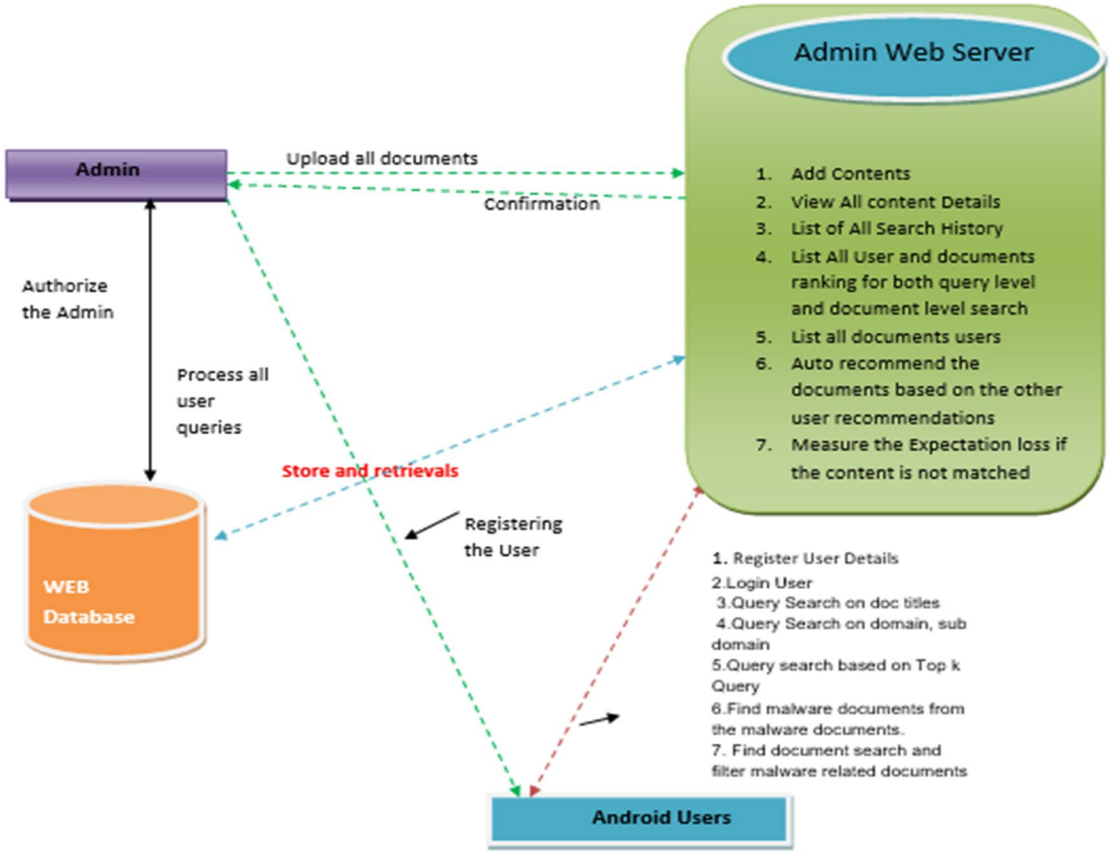


Figure 1: System Architecture

A. Advantages

1) This approach is able to detect misbehaviors from malware behavioral classes that consider 125 existing malware families, which encompass most of the known malware.

2) To the best of our knowledge, It is the first system which aims at detecting and stopping at run-time any kind of malware, without focusing on a specific security threat, using a behavior-based and multi-level approach. Not only the accuracy of the runtime detection is very high, but it also achieves low performance (1.4%) and energy overhead (4%).

V. IMPLEMENTATION

A. Android User

The android User should register before processing operations with web servers. After registration, he has to login by using authorized user name and password. Login successful he will do some operations like Query Search on doc titles, Query Search on domain, sub domain, Query search based on Top k Query and scanning type of document and contents to check whether the document contains malware. If documents are malware related then those documents will be scanned and never takes to view in the android mobile.

B. Admin

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as add contents, view all content details, list of all search history, List All User and documents ranking for both query level and document level search, List all documents users, Auto recommend the documents based on the other user recommendations, Measure the Expectation loss if the content is not matched and logout.

1) *Add Document:* In this module, the admin can add the document. If admin wants to add the new document, then he will enter document name, enter a document title, domain, sub domain, browse the document then submit and that data will stored in data base.
2) *View Documents:* In this module, the admin can view the document details i.e., document name, document title, domain, sub domain, file name, and document content, related images.
3) *View of all Users:* In this module, the Admin can view list of all users. Here all register users are stored with the details such as user name, DOB, e-mail, mobile, and location and user images.
4) *View User Search History:* In this module, the Admin can view all search comparisons. Here all users search history are stored with the details such as user name, document ID, document name, document title, domain, sub domain, date and time and view details.
5) *View Documents Ranking:* In this module, when you click on document ranking, the ranking details of each document will be displayed such as document rank, document name, document title, domain, and sub domain.
6) *Query Search on Document:* In this module, user browse the data and submit then details will be displayed such as document name, document title, domain, sub domain, related images and document rank.
7) *Query Search on Domain:* In this module, user selects the domain, sub domain, and click on submit. Then corresponding details will be searched and downloads the file.
8) *Measure the Expectation:* In this module, expectation measurement details will be displayed, i.e., user name, matched documents, expected results, expectation loss, date and time

VI. RESULTS

Fig 2: Menu Screen

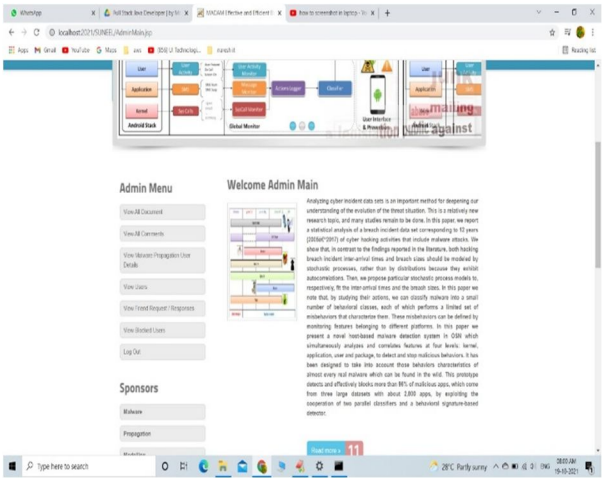


Fig 3: Admin Page

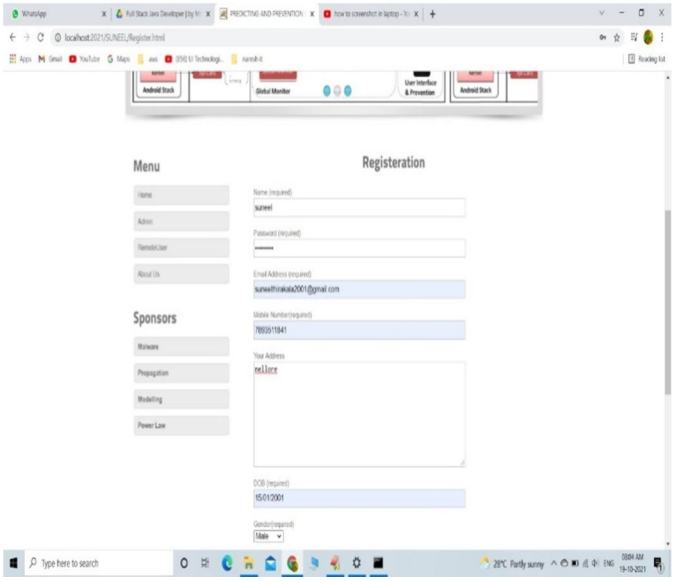


Fig 4: Registration page

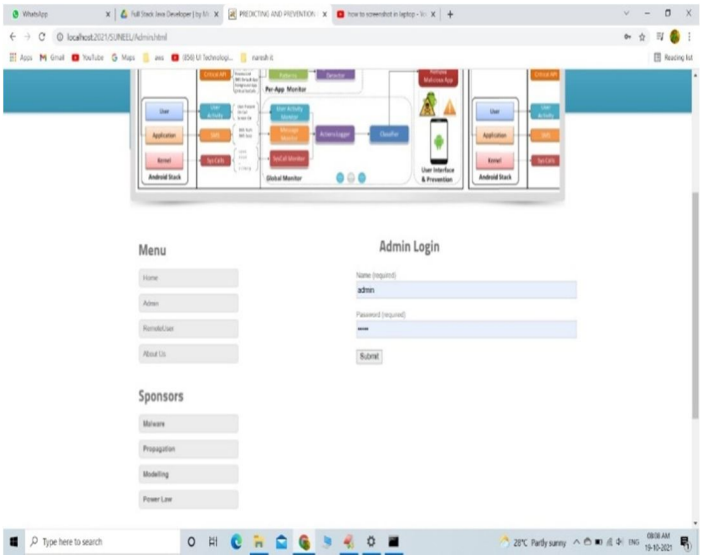


Fig 5:Admin Login

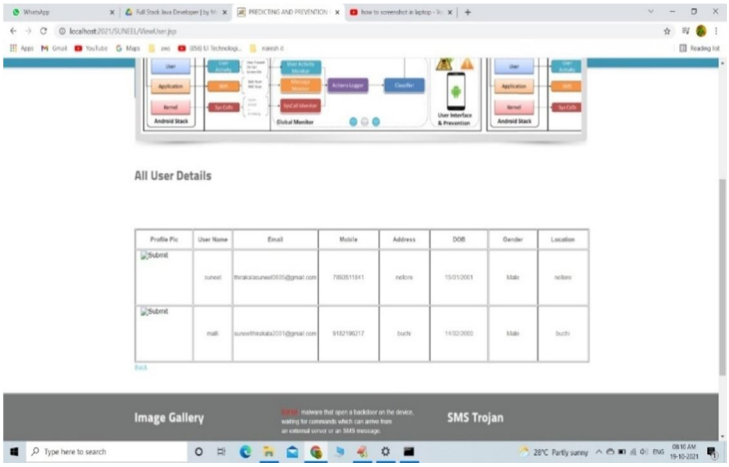


Fig 6:All user details Screen

Fig 7:Malware propogation user Files

Fig 8: User details Page

VII. CONCLUSION

The Starting from the stop of 2011, attackers have accelerated their efforts in the direction of Android smartphones and tablets, generating and dispensing loads of heaps of malicious apps. These apps threaten the person records privacy, cash and tool integrity, and are tough to come across due to the fact they reputedly behave as proper apps bringing no harm. This paper proposes a multi-degree host-primarily based totally malware detector in social media.

REFERENCES

[1] Dr.C K Gomathy, Article: An Effective Innovation Technology In Enhancing Teaching And Learning Of Knowledge Using Ict Methods, International Journal Of Contemporary Research In Computer Science And Technology (Ijcrcst) E-Issn: 2395-5325 Volume3, Issue 4,P.No-10-13, April '2017

[2] Dr.C K Gomathy, Article: A Semantic Quality of Web Service Information Retrieval Techniques Using Bin Rank, International Journal of Scientific Research in Computer Science Engineering and Information Technology (IJSRCSEIT) Volume 3 | Issue 1 | ISSN : 2456-3307, P.No:1563-1578, February-2018

[3] Dr.C K Gomathy, Article: A Web Based Platform Comparison by an Exploratory Experiment Searching For Emergent Platform Properties, IAETSD Journal For Advanced Research In Applied Sciences, Volume 5, Issue 3, P.No-213-220, ISSN NO: 2394-8442,Mar/2018

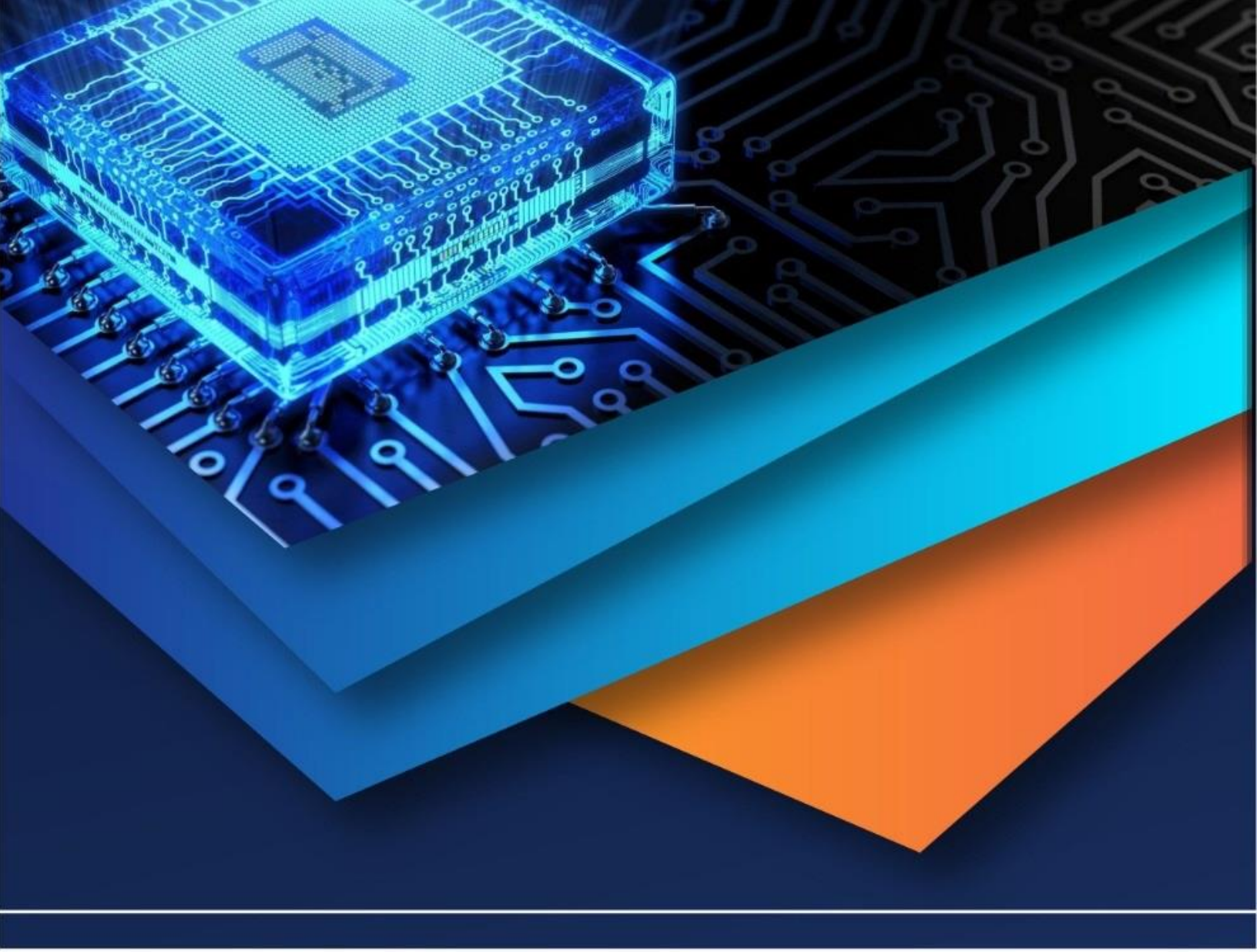
[4] Dr.C K Gomathy, Article: Supply chain-Impact of importance and Technology in Software Release Management, International Journal of Scientific Research in Computer Science Engineering and Information Technology (IJSRCSEIT) Volume 3 | Issue 6 | ISSN : 2456-3307, P.No:1-4, July-2018

[5] Dr.C K Gomathy, Article: A Scheme of ADHOC Communication using Mobile Device Networks, International Journal of Emerging technologies and Innovative Research (JETIR) Volume 5 | Issue 11 | ISSN : 2349-5162, P.No:320-326, Nov-2018

[6] Dr.C K Gomathy, Article: A Study on the recent Advancements in Online Surveying , International Journal of Emerging technologies and Innovative Research (JETIR) Volume 5 | Issue 11 | ISSN : 2349-5162, P.No:327-331, Nov-2018

[7] Mohammed, Z., . NITDA Raises Alarm over Potential Cyber Attacks to Banks. Govt Agencies, Others Retrieved from. https://www.nigerianews.net/nitdaraisesalarm-potentialcyber-attacks-banks-govt-agencies/.

[8] Nhan, J., Bachmann, M., . Developments in cyber criminology. In: Maguire, M., Okada, D. (Eds.), Critical Issues in Crime and Justice: Thought, Policy, and Practice. Sage, London, p Oates, B., .Cyber crime: how technology makes it easy and what to do about it. J. Inf. Syst. Secur.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY