IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008168 |

Cybersecurity Threats, Challenges and Solutions

Omkar Babar[1], Akash Yesane[2]

U.G. Student, Department of Information Technology, B.K. Birla College of Art, Commerce and Science, Kaylan, Maharashtra, India[1]

U.G. Student, Department of Information Technology, B.K. Birla College of Art, Commerce and Science, Kaylan, Maharashtra, India[2]

ABSTRACT:Just as pollution may be a side effect of the economic revolution, many security vulnerabilities are caused by the rise in Internet connectivity. Cyber-attacks have largely exploited these vulnerabilities. People and companies have found ways to use various security measures to deal with these attacks, The method of attack. But there are some social engineering attacks, and other cyber threats are there which whom many peoples suffer consciously or subconsciously, if people are aware about these kind of attacks, how they actually accurse and with taking safety measures it become easy to tackle. here we discuss about some major and frequently happening cyber-attacks and their solution. So by implementing these solutions every individual and company can handle these kind of attacks and threats. Now a days due to this COVID-19 pandemic the frequency of these attack are increased and we discuss solutions and strategy to protect our self.

KEYWORDS:Cyber-attacks, Malware (bad USB concept), Pegasus Spyware, social engineering attacks (twitter example), Phishing attacks, DDoS attacks, network sniffing..

I. INTRODUCTION

Cyber Security refers to the tactic of protecting programs, networks, computer systems, and their components from unauthorized digital access and attacks. It consists of agroup of techniques that are wont to protect the integrity of networks. Cyber Security is implemented to prevent cyberattacks. only necessary that we educate individual. malware is an all-encompassing term for a variety of cyber-attacks including Trojans, viruses and worm's malware is simply defined as code with malicious intent that typically steals data or destroy something on the computer the way. In the early days, the purpose of writing malware was simple, so was easier to detect. This type of malware can be defined as traditional (simple) malware. However, malware that can run in kernel mode today is more destructive and harder to detect than traditional malware, and can be defined as next-generation (next-generation) malware According to scientific and business reports, approximately 1 million malware files are created a day , and cybercrime will damage the planet economy by approximately $6 trillion annually by 2021[1] some social engineering attacks traditional hacking aims to compromise the safety settings of IT systems and applications. social engineering attackers attempt to exploit the users of these technologies by claiming to be employee's vendors or support personnel the attackers use that to their advantage by deceiving users into revealing information that compromises data security traditional protection. Here we discuss the Twitter hacking case uses social engineering attack technology.to attack each and every one of you, attacker set up an attack or a hack on a place that you might all visit. the watering hole it comes from you know an animal analogy and like a desert Sahara situation all the animals will come to one central place for water and if you can poison that watering hole well then you got everyone who visits so that's attackers do.like above mention there are other vulnerabilities also there which we are going to discuss further with whom most of the peoples suffer there we also going to discuss solution so that by implementing it we can able to overcome this type issues.

II. RELATED WORK

LR-DDoS attacks are likely to continue to pose a threat to systems, especially those centralized systems (for example, the cloud computing platform)[1]. In this article, they design and implement a flexible and modular security architecture to detect and mitigate LR-DDoS attacks in the SDN environment[1]. The modular design allows people to easily replace any module without affecting other modules in the architecture. The IDS module in our architecture is

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008168 |

designed to detect streams using different previously trained ML models, which can be developed using different programming framework.

introduce POSEIDON, a performant, cost-efficient and agile DDoS defence system[2]. Addresses key limitation in current DDoS defence. The POSEIDON language provides the with a simple and modular DDoS strategy abstraction, which can support a number of strategies and protect from the complexity of the underlying hardware.[2]

This survey enables researchers to comprehend the various methods, challenges, and trends for phishing attack detection. Heuristics and data mining methods have a high rate of FP they are better at distinguishing phishing attacks[3]. RF, SVM, C4.5, DT, PCA, k-NN are also common. These methods are most useful and effective for detecting the phishing attack[3]. A portion of the ML procedures can identify TP up to 99%[3].the use of the Golden Hour framework to automatically secure the accounts of tens of thousands of phishing victims also motivates the continued expansion of proactive mitigations within the ecosystem[4]. these phishing attack is subset of social engineering attack so investment in organizational education campaigns offer optimism that social engineering attacks can be reduced[5]. To overcome cyber security incidents involving social engineering attacks, research supports the most effective defence is an educated computer user[6]. investment in organizational education campaigns offer optimism that social engineering attacks can be reduced[6]. USBCaptchaIn implements a new host protection method, which can resist BadUSB attacks[7]. in which general USB devices maliciously mimic the behaviour of HID devices and can also resist malicious software embedded in data in RSDes[7].The proposed approach proactively blocks attacks before they reach the target and does not rely on decision of the users[7]. The popularization of the Internet of Things, 5G and mobile smartphones rapidly creates other innovations[8]. This paper has discussed core attributes/parameters as well as different types of Android malware identification techniques[8]. Various ML techniques such as DT, SVM, MBK and NB are applied to the data set obtained from Cuckoo. The ML technology is evaluated on the dataset and found that DT performs best at classifying unknown malware samples[9]. Various ML techniques such as DT, SVM, MBK and NB are applied to the data set obtained from Cuckoo. The above ML technology is evaluated on the dataset and we found that DT performs best at classifying unknown malware samples[10].

III. METHODOLOGY

3.1 social engineering attacks

Antecedentsandcauses

Last year July 2020 in these ongoing COVID-19 pandemic twitter was hacked and it was a pretty big one high-profile twitter accounts like bill gates, elon musk, president Obama, joe biden, kanye west all taken over, tweeting out a cryptocurrency scam how did this happen?
hacker can tweet from any account on the entire platform you could do anythingby which they could crash the stock market, could start a war, could swing the election they couldreally do anything and that's why This has become a matter of concern among the people.issuesis kind of someone who had access to the twitter backend systems one of the back end there, they're admin panel.
attackerwas able to bypass all security controls so things like strong passwords and two-factor authentication they could just disable those features take over the account make it their own and start tweeting like it's theirs the they didn't hack into the network bypassing firewalls they didn't find bugs and twitter code and exploit vulnerabilities no you see they didn't hack twitter's systems they hacked twitter's people hacking people is a thing every company's greatest security weakness. hacking people this technique this process is called social engineering here are five basic reasons that a social engineering attack is so effective

1. human nature -
2. ignorance
3. fear
4. greed
5. moral obligation

according to the EC counsel are four stages involved in a social engineering attack

1. research
2. select a victim
3. develop a relationship
4. exploit the relationship now

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008168 |

this is one of the most dangerousthreats we have facing us all of thesebig companies and even smallermedium-sized companies investmillions of dollars in their securityinfrastructure but there will always bethat huge gaping hole with their employees.

With cell phone number what these hackers will do is they'll call up your cell phone provider let's say in this case what they'll do is they'll try to impersonate you or maybe your spouse and they'll try to trick this person using social engineering techniques to activate another sim card that's in a cell phone they have and

move your number to their phone and they essentially have your cellphone now which means in a lot of casesthey have control ofall your accounts bank accounts socialmedia accounts.

Solutions

how do you protect your company from your people from your employees one of the best things we can do now is -

1.employee training teaching your employees about social engineeringattacks
2. isolating roles in a company and then implementing least privilege in every area you can.
3. It always comes down to a person and make sure they have enough knowledge to protect themselves.

3.2 Phishing attacks

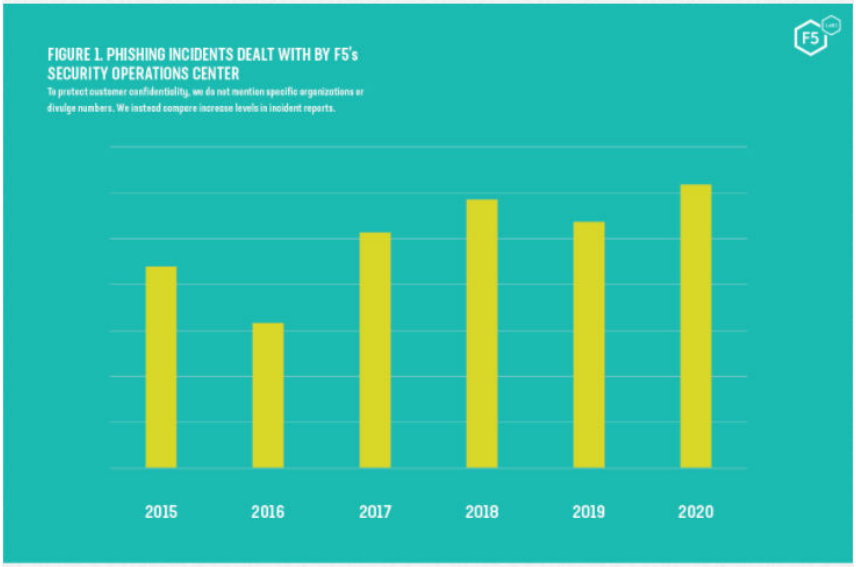
Antecedentsandcauses

it is terrifying how easy it is to do a phishing attack or a fishing hack. in these type of attack hacker primarily need victim's username and password. they get it by social engineering

phase one of attack – to create phishing page

to gain access they set up a fake web page or application which having templet similar to original website. Setting up this fishing page and trying to get victims credentials this is called credential harvesting.

Here the figure below represents the phishing incidents of last five years



https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report

phase two of attack – creation of link

phishing emails this phishing email will craft to make it look like it's coming from original website They will prompt victim to open the link like, might say 'hey you got a really important message from a colleague it's an emergency click on this link'. it doesn't have to be an email it could be a text message which we call a smishing (that "s" stands for SMS) attack, it could be a phone call we call these vishing attack (here "v" stands for voice). They may target specific person these type of phishing is called as spear-phishing. These link is created by social engineering toolkit or SET.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008168 |

Instead of sending link it can be a document which contain malware. After getting the access attacker can mess with that file host file. Host file will override DNS on the system so typically victim when types in website name his computer will ask the DNS server its DNS server start finding the website. Where live and the DNS server will reply with an IP address. Here victim's computer will look in the hosts file first before it asks a DNS server. So here attacker mess with this host file and by change the destination IP address he may redirected to that changed IP address. This is called DNS poisoning.

Solutions

how does individual keep himself safe from phishing attacks?

1. make sure you have some good spam filter.
2. don't even click on links, don't download them
3. if you receive a notification of a secure message from your bank or something just open a new tab log into your bank you'll find the actual notifications.
4. make sure peoples must be educated on how to protect themselves against phishing scams.
5. data mining and heuristics, ML, and deep learning algorithms[3]

3.3 DDoS attack

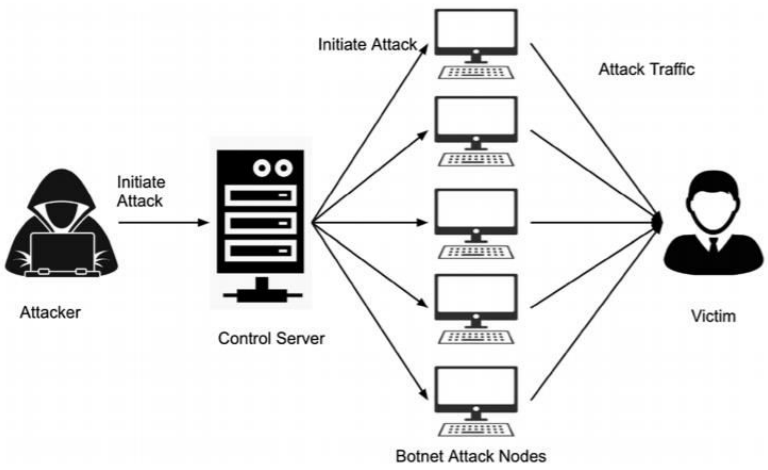
Antecedents and causes

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt a targeted server's, service's, or network's normal traffic by flooding the target or its surrounding infrastructure with Internet traffic. DDoS assaults are effective because they use numerous compromised computer systems as attack traffic sources. Computers and other networked resources, such as IoT devices, are examples of exploited machinery. A DDoS assault is analogous to an unanticipated traffic congestion obstructing the roadway, preventing ordinary traffic from reaching its destination. DDoS assaults are carried out via networks of machines that are linked to the Internet.

Here following is diagrammatic representation of bot net attack:

Fig 1:

[11]



How does a DDoS attack work?

These networks are made up of malware-infected PCs and other devices (such as IoT devices) that can be manipulated remotely by an attacker. Individual devices are known as bots (or zombies), while a botnet is a collection of bots. The attacker can direct an attack once a botnet has been built by delivering remote instructions to each bot. When a botnet targets a victim's server or network, each bot sends requests to the target's IP address, potentially overloading the server or network and causing a denial-of-service to normal traffic. Since each bot is a legitimate internet device, it is difficult to separate attack traffic from normal traffic.

The most obvious symptom of a DDoS attack is that a site or service suddenly becomes slow or unavailable. However, due to many reasons (such as legitimate spike traffic) they can cause similar performance issues, so

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

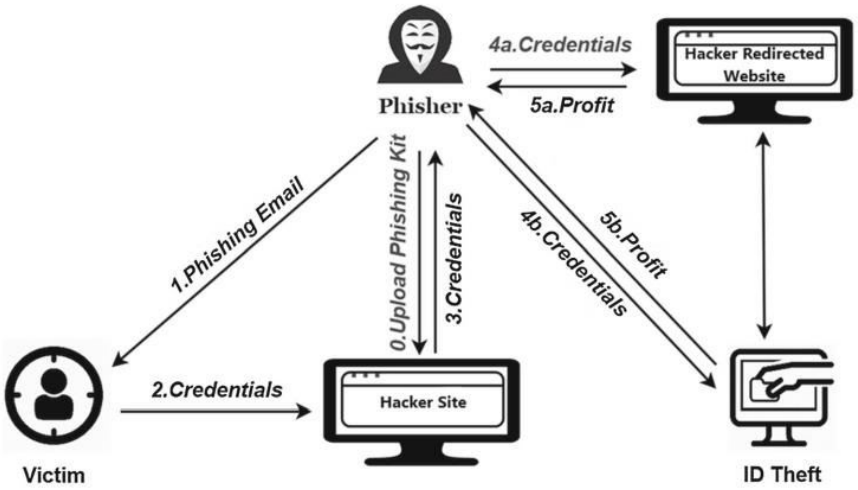
| DOI:10.15680/IJIRSET.2021.1008168 |

further investigation is generally required. Traffic analysis tools can help you find some obvious signs of DDoS attacks:

- Suspicious traffic from a single IP address or IP range
- Large amounts of traffic from users who share a single behavioural profile (such as device type, geographic location, or web browser version)
- Unexplained spike in requests for individual pages or endpoints
- Strange traffic patterns, such as spikes at strange times of the day or patterns that seem unnatural (such as spikes every 10 minutes)

There are other more specific signs of a DDoS attack, which may vary depending on the type of attack.
Fig 2:
[3]

Phishing attack diagram



Solution and process for mitigating:

The main problem in mitigating DDoS attacks is to distinguish between attack traffic and normal traffic.
For example, if a product launch floods a company's website with eager customers, it would be wrong to cut off all traffic. If the company's traffic from known attackers suddenly increases, it may need to work to mitigate the attack.
On the modern Internet, DDoS traffic takes many forms. Traffic design may vary, from non-spoofing single-source attacks to sophisticated adaptive multi-vector attacks.
The Multi-vector DDoS attack uses multiple attack paths to suppress the target in different ways, which may distract mitigation efforts on any trajectory. Attacks on multiple layers of the protocol stack at the same time, such as DNS amplification (for layer 3/4) combined with HTTP flooding (for layer 7), is an example of multi-vector DDoS.
Mitigating multi-vector DDoS attacks requires multiple strategies to deal with different trajectories.
Generally speaking, the more complex the attack, the more difficult it is to separate the attack traffic from the normal traffic. The attacker's goal is to mix in as much as possible to make the mitigation effort as inefficient as possible.
Mitigation attempts that involve indiscriminately dropping or restricting traffic can rule out good traffic along with bad traffic, and attacks can also modify and tailor evasive countermeasures. To overcome complex destruction attempts, a layered solution will bring the greatest benefits.

3.4 malware attack using badUSB

categorizing kind of malware:
Files and infect other clean files, they can spread uncontrollably, destroy core system functions, delete or damage files that are usually displayed as executable files, you may have downloaded from the Internet, now this type of Malware disguised as legitimate software or bundled with legitimate software that can be tampered with will often act as the creator and create a backdoor in your security, allowing other malware to commit crimes.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

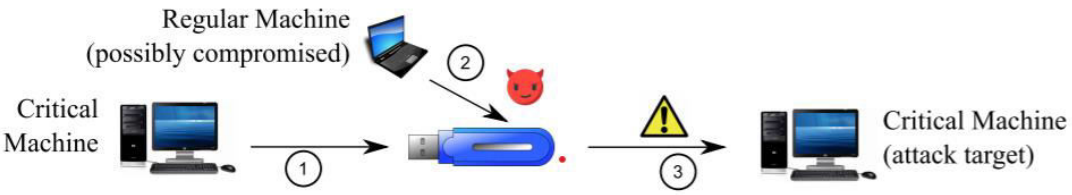
|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008168 |

A worm: is actually the entire network of devices, whether it is local or through the Internet using a network interface, each continuously infected machine is used to infect more, and then we have a botnet, for example, a botnet is a network of infected computers, They are in an attacker's controller, so if you have some operating system vulnerabilities or download some legitimate L software from somewhere, you can basically find malware.

Solution:
Stop clicking suspicious links.
Always study the URL Consciously and make sure you are not on a counterfeit site.
Updating your firewall constantly
use antivirus software They will prevent the transfer of large data files over the network in hope to weed out attachment that may content malware. Use most up to date security Updates.

Bad USB:
bad USB it's designed by hackers to hack the pc . it does is pretend to be a keyboard .when you plug in a USB flash drive like this into a computer will recognize it as a mass storage device but when you plug bad USB in its recognized as an HID device which stands for human interface device.
you plug this USB in it's going to launch this inject.bin file which is the script hacker going to load.
To represent how bad USB actually works let see first below diagram for understanding:
Fig 3:
[7]



Solution:
How do we protect ourselves?
1. don't plug in USB flash drives that you don't know what they are.
2. always lock your computer when you done with your work.
3. require the user to be educated and to protect themselves all the time which we know human error.
4.enable password authentication for administrative access.

IV. CONCLUSION

The COVID19 pandemic has created an extraordinary and unique social and economic environment used by cybercriminals. Our analysis of events, explaining and discussing possible solution in above discussion other aspects rather than this shows that there seems to be a weak correlation between advertisements and corresponding cyber-attacks. The COVID19 pandemic and the increase in the rate of cyber-attacks caused by it has a broader impact that goes beyond the goals of such attacks. Changes in work practices and socialization mean that people now spend more time online. In addition to the unemployment rate has also risen, which means that more people are sitting at home in line; some of them may use cybercrime to support themselves. The increase in the level of cyberattacks and cybercrimes means that can have an impact on police services around the world, and law enforcement agencies around the world must ensure that they are able to respond to crimes.

The analysis and study of attack in this article highlights the common modus operandi of many cyberattacks. Many cyberattacks start with phishing campaigns that direct victims to download files or visit URLs. The file or URL acts as a carrier of malicious software and, after installation, acts as a carrier of financial fraud. The analysis also shows that to increase the likelihood of success, phishing campaigns use media and government advertisements.Our investigation offers opportunities for further research. This study shows that the direct and inverse correlation between incidents and cyber-attacks is the best description.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008168 |

In above articles we discuss about the most common attacks and solution, we discuss issues in recent news and also suggest the necessary precautions to tackle this attacks this problem at initial stage. This article may help further researchers, companies and common peoples about how to hand this attacks.

REFERENCES

[1] J. A. Perez-Diaz, I. A. Valdovinos, K. K. R. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[2] M. Zhang *et al.*, "Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches," no. February, 2020, doi: 10.14722/ndss.2020.24007.

[3] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, 2021, doi: 10.1007/s11235-020-00733-2.

[4] A. Oest *et al.*, "Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale," *Proc. 29th USENIX Secur. Symp.*, pp. 361–377, 2020.

[5] B. J. Dorr *et al.*, "Detecting Asks in Social Engineering Attacks: Impact of Linguistic and Structural Knowledge," *AAAI 2020 - 34th AAAI Conf. Artif. Intell.*, pp. 7675–7682, 2020, doi: 10.1609/aaai.v34i05.6269.

[6] N. Y. Conteh and P. J. Schmick, "Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks," *Int. J. Adv. Comput. Res.*, vol. 6, no. 23, pp. 31–38, 2016, doi: 10.19101/ijacr.2016.623006.

[7] F. Griscioli and M. Pizzonia, "USBCaptchaIn: Preventing (un)conventional attacks from promiscuously used USB devices in industrial control systems," *J. Comput. Secur.*, vol. 29, no. 1, pp. 51–76, 2021, doi: 10.3233/JCS-191404.

[8] M. A. Omer *et al.*, "Efficiency of Malware Detection in Android System: A Survey," *Asian J. Res. Comput. Sci.*, vol. 7, no. 4, pp. 59–69, 2021, doi: 10.9734/ajrcos/2021/v7i430189.

[9] N. Usman *et al.*, "Intelligent Dynamic Malware Detection using Machine Learning in IP Reputation for Forensics Data Analytics," *Futur. Gener. Comput. Syst.*, vol. 118, no. May, pp. 124–141, 2021, doi: 10.1016/j.future.2021.01.004.

[10] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, and N. T. K. Son, "Performance evaluation of Botnet DDoS attack detection using machine learning," *Evol. Intell.*, vol. 13, no. 2, pp. 283–294, 2020, doi: 10.1007/s12065-019-00310-w.

[11] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Networks*, vol. 169, no. March 2020, p. 107094, 2020, doi: 10.1016/j.comnet.2019.107094.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details