iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VIII **Month of publication:** August 2020

DOI: https://doi.org/10.22214/ijraset.2020.31216

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 8 Issue VIII Aug 2020- Available at www.ijraset.com

Cyber Security in the Age of COVID-19: An Analysis of Cyber-Crime and Attacks

Aayad Al Hajj[1], Rony M[2]
[1, 2]*Dept. of Information Technology, College of Applied Sciences, Oman*

Abstract: ***The world has witnessed unprecedented change in all aspects of operations during this COVID-19 pandemic. The pandemic has led to many gullible individuals and organizations being exploited by cybercriminals. The hackers take advantage of heightened anxiety among many internet users to launch attacks and breach data. The current paper adopted a systematic literature review as a suitable method for data collection.***
The findings have revealed that since the pandemic outbreak, there has been an increased incidence of cyber-crimes and attacks. Education and more sensitization about adequate cybersecurity are recommended to mitigate the COVID-19 threats on data security.
Index Terms: COVID-19 pandemic, cyber security, heightened anxiety, cyber-crimes and attacks

I. INTRODUCTION

Today, the world is generating, sharing, and using massive data in different sectors due to advanced technologies. Big Data analytics is used in the healthcare sector to manage volumes of data to improve people's conditions and prevent medical errors [1]. However, with the emergence of cyber technologies, cybercrimes, and attacks have increased.
The increased cyber-attacks is a regional, national, and global security concern and threats. Currently, the COVID-19 tool for cyberattacks has become a threat vector used by hackers and cybercriminals to breach various organizational data [1]. Therefore, it is reasonable to say that the COVID-19 pandemic has become a tool for hackers to commit cyberattacks apart from being an economic and health challenge on individuals, businesses, and governments.
Hence, all the stakeholders must join hands to minimize cyber crimes and attacks by enhancing cybersecurity. Cybersecurity in the age of COVID-19 faces various challenges, such as spoofing, hacking, distributed denial-of-service (DDoS), malicious domains or websites, ransomware, spam emails, and others [4, 12].
The increased nervousness associated with the COVID-19 pandemic has heightened the possibility of successful cyber attacks and increased incidences. This paper aims to critically analyze cybercrimes during this pandemic period through a systematic review of existing literature.

II. PROPOSED METHODOLOGY

The research was carried out through a systematic review of reputable and recent articles from reputable databases, such as Google Scholar and institutional-based online libraries.
Therefore, the proposed methodology was a literature review approach. The COVID-19 cyberattack and crime were the main keywords or search terms used to identify relevant articles.
The specified items discussed the vectors through which cybercriminals use to lure unsuspecting internet users into launching an attack and breach data.
The proposed method was vital for gathering empirical evidence for result analysis and completion of the paper. The process entailed conducting an overview of academic search, which generated numerous articles about the topic. From the populated items, further scrutiny was implemented to narrow the search to the most relevant and recent reports [6]. The methodology was appropriate because the study was about expounding on the existing knowledge about COVID-19 cyber attacks.

A. Block Diagram

Connecting COVID-19 pandemic and cyber attacks or crime was based on timelines for the data breaches and the launching of attacks. Fig. 1 presents a block diagram connecting cyber-crime and attacks to the pandemic.

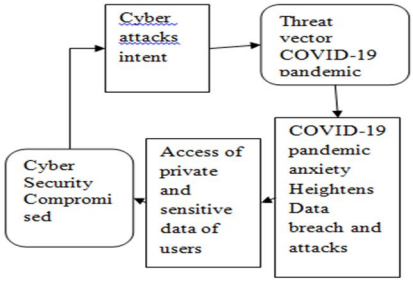


Fig. 1: Block diagram [7]

B. Algorithm

An algorithm is a formulated process to solve a problem leading to accurate results of the study. For An algorithm is a formulated process to solve a problem leading to accurate results of the study. For cybersecurity, a specific algorithm is considered based on timelines for possible cyber-attacks [3]. The timeline offers the patterns or sequences for various attacks. In this paper, the preferred algorithm is time-oriented for three types of cyberattacks. The analogy is "the distribution of malware (m) through phishing (p) which steals payment credentials which are used for financial fraud (f)" [5]. Therefore, the algorithm for this cyber-attack pattern is presented as p,m,f. Analyzing this cyber-attack analogy is significant because it depicts the various sequences of different cyber-attacks where cybersecurity measures could be implemented in a timeline [5]. The timeline displays the subsequence patterns of the cybercrime scenario:

1) "p,m: n=8, 19%
2) p,m,f: n=10, 23%
3) ph,m: n=1, 2%
4) p,ph: n=1, 2%
5) p.m.e: n=5, 12%
6) p,ph,m: n=2, 5%
7) p,ph,f: n=1, 2%
8) p,e: n=1, 2%
9) p,ph,m,f: n=1, 2%" [5]

C. Flow Chart

The flow chart below presents cybercrime elements and attacks based on the COVID-19 pandemic as a vector. The flow chart demonstrates that adequate cybersecurity limits COVID-19 pandemic effects on cyber crimes because of deterrent mechanisms.

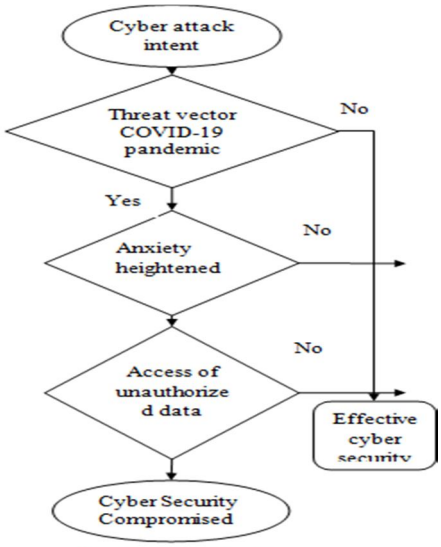


Fig. 2: Flow Chart

III. RESULT ANALYSIS

Lallie et al. [5] point out that most of the private sectors, public sectors, and governments are putting in place or have put in place data structures and information management models to mitigate potential cyber crimes due to COVID-19 gullibility. Figure 3 provides an overview of COVID-19 as a threat vector for cyber-attacks and crime [5]. The diagram reveals that the pandemic compromises workforce efficiency toward security adherence.

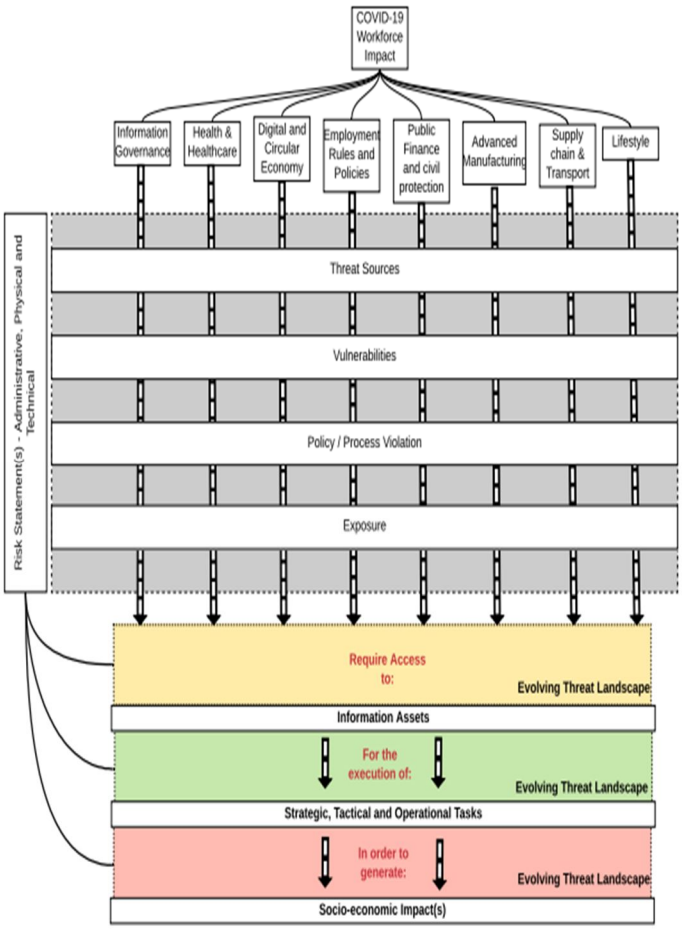


Fig. 1: COVID-19 Impact on Workforce [5]

The effects of the pandemic have led to additional sensitization about cybersecurity measures. WebARX Security [2] demonstrates that most cyber attackers have exploited the vulnerabilities created by COVID-19 pandemic to develop phishing and malware attacks on gullible institutions, organizations, and individuals. Through phishing, cybercriminals steal sensitive data using fake websites or emails [1]. The pandemic changed the way of doing things, and the internet or online transactions became the mostly used transactional channel. Therefore, many unsuspecting individuals who have not used these systems become easy prey for the attackers. According to WebARX [2], since the pandemic started, the phishing attacks increased by 350%. Experts explain that the COVID-19 cyber attack affects many sectors based on the COVID-19 cyberattack instruments. As the global grapples with the pandemic, various sectors have witnessed an increase in traffic due to the online services [1, 15]. Therefore, despite the increased innovation and technological advancement, the pandemic has heightened cybersecurity challenges worldwide. Satellites control over 80% of global operations; hence, its cybersecurity should be prioritized [4]. COVID-19 is an emergency occurrence, which has provided cyberattackers an opportunity to exploit. Khan, Brohi, and Zaman [12] explain that attacker, scammers, and hackers exploit emergencies, mainly when people are desperate, frightened, and most susceptible.

Lallie et al. [5] explain that the cyber-crime cases reported due to pandemic pose severe risks to the security and worldwide economy, hence comprehending associated sequences and propagating the threats is vital. Empirical evidence reveals that numerous solutions are available to analyze cyber threats' various natures [10, 11]. However, the pandemic has thrown some confusion in every aspect of the daily lives.

The Crown Prosecution Service (CPS) guidelines divide cyber-crime into cyber-enabled crimes and cyber-dependent [9]. A cyber-dependent crime depicts a culpable offense using a computer or other information communications technology (ICT)[9]. On the other hand, cyber-enabled crimes are conventional crimes based on ICT exploitation [5, 9]. According to Lallie et al. [5], 43 cyber-attacks over a timeline were further divided as follows:

1) 37 (86%) phishing and smishing
2) 2 (5%) hacking
3) 2 (5%) denial of service
4) 28 (65%) malware
5) 15 (34%) financial fraud
6) 6 (13%) pharming
7) 6 (15%) extortion [5].

Fig. 4 provides a cybercrime tree.

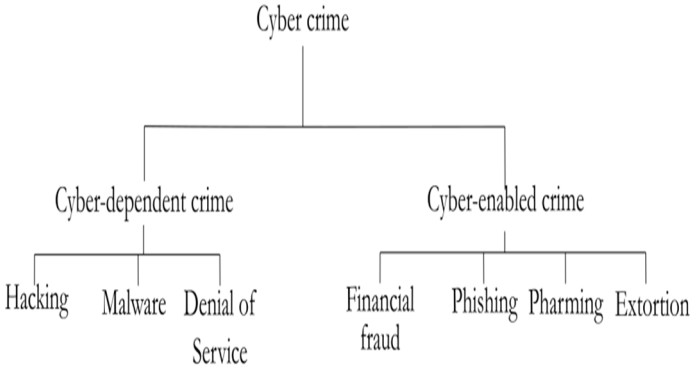


Fig. 2: Cyber-dependent and cyber-enabled crimes [5]

Fig. 5 outlines the most common cyber threats during the pandemic. The risks are DDOS attacks, malicious domains, spam emails, malicious websites, malware, ransomware, vicious social media messaging, mobile threats, business email compromise, and browsing apps [12, 13].

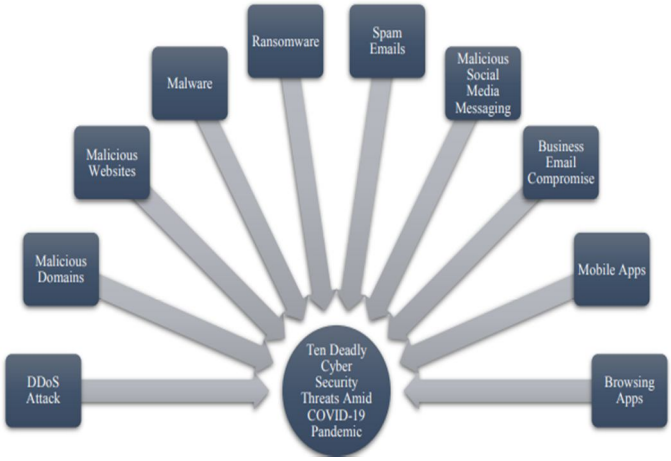


Fig. 3: Top 10 Cyber Security Threats amid COVID-19 Pandemic [12]

Denials of Service (DoS) attacks have become common during the pandemic as cyber-criminals exploit the disease [8]. Phishing or Social Engineering entails attempts by a criminal to induce people to perform an activity, such as visiting a dangerous website or sharing sensitive details, under the disguise of a legitimate entity [5]. Technical attackers conduct malware, hacking, and DoS attacks by compromising system integrity or introducing the malicious application to disrupt operations [5, 8]. Ransomware has become a typical cyber-attack or crime because it integrates extortion and malware attacks [14]. DoS attacks work by flooding the system with illegitimate requests, especially during peak hours, and it forces the method to go offline as the legitimate and illegitimate requests are integrated [5].

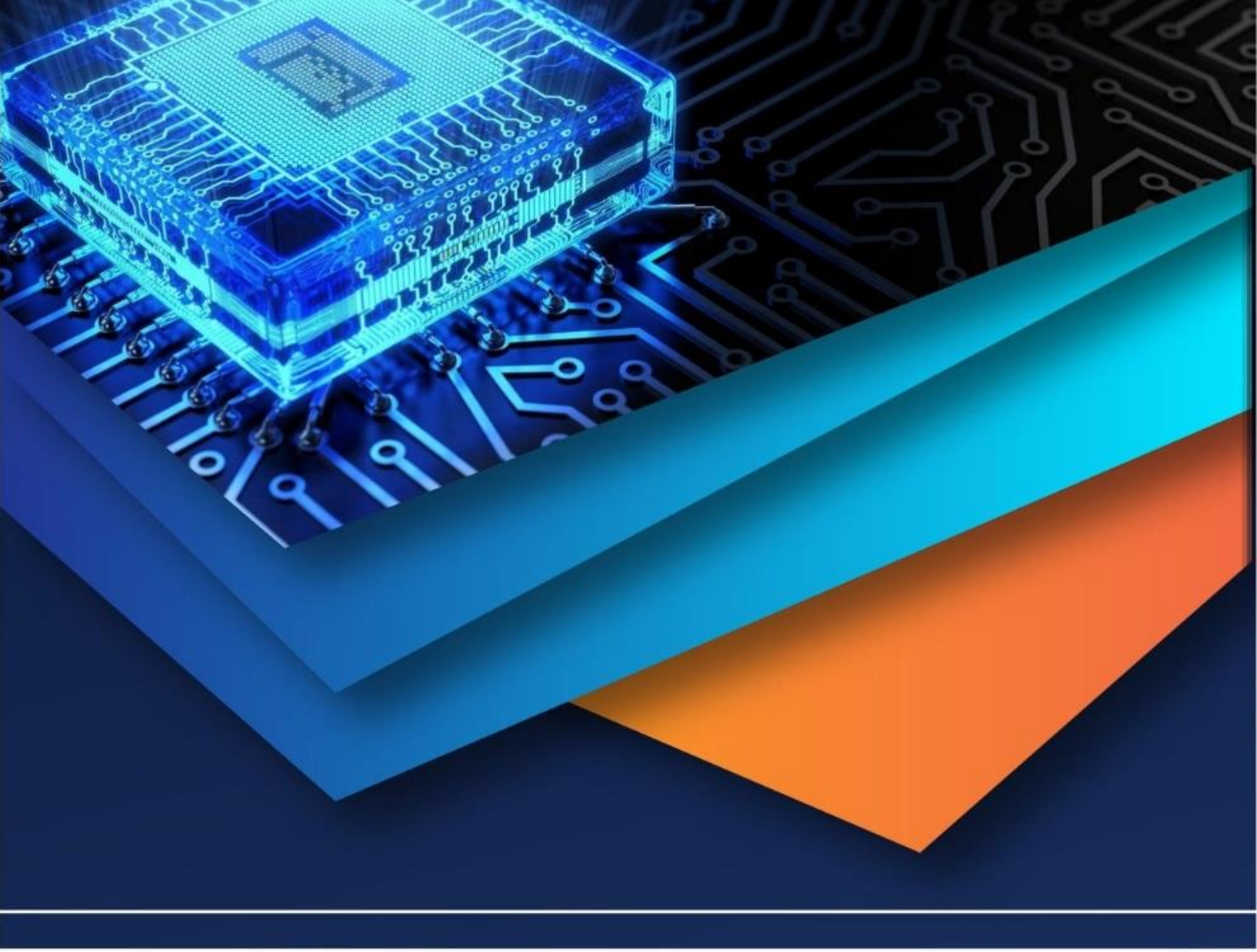
The uniqueness of the attack incidences due to COVID-19 exploitation necessitates a sensitization campaign for individual and group internet users. Proactively training users about the defrauding, malware, phishing, and spamming employed by hackers during the pandemic is a viable means for mitigating effects [1]. In addition, the enterprise risk controls should always be emphasized to ensure that threats are mitigated using practical cybersecurity tools such as Big Data analytics, the SIEM software, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) [1,15]. These measures should be undertaken by all stakeholders, particularly during this pandemic, to ensure that threats are averted. COVID-19 has led to a substantial secondary risk to a technology-driven community because of many indiscriminate cyber-crime and attacks. Working at home has also increased the success rates of various cyber-attacks because of fewer security measures and limited supervision. Cybercriminals are targeting unsuspecting individuals who have heightened stress [5].

IV. CONCLUSION

COVID-19 pandemic has created an emergency, increased anxiety and confusion, and increased online transaction volume. In most cases, most governments, institutions, and individuals find that their existing cyber securities cannot adequately protect all the volumes of data. Therefore, cybercriminals have an opportunity to exploit vulnerabilities created by the pandemic. Cyber-enabled crimes and cyber-dependent crimes are common during this period because hackers and attackers have a broad spectrum to exploit. Various stakeholders must work together to boost security, particularly in this pandemic period. Working from home and increase paperless transactions have presented increased challenges to cybersecurity.

REFERENCES

[1] A. R. Mathew, “Cybersecurity Pros Warn – COVID-19 Pandemic as a Tool,” *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 4, 2020, pp. 2441-2443.
[2] WebARX, "COVID-19 Cyber Attacks," *WebARX Security*, 30 March 2020. [Online]. Available: https://www.webarxsecurity.com/COVID-19-cyber-attacks/
[3] A. R. Mathew, “Cyber Insurance,” *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 6, 2019, pp. 4447- 4451.
[4] A. R. Mathew, “Cyber Security- How Vulnerable are Satellites - to Cyberattacks,” International *Journal for Research in Applied Science & Engineering Technology (IJRASET)* vol. 7, no. 3, 2019, pp. 2427- 2430.
[5] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, “Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic,” *ArXiv:2006.11929v1*, 2020, pp. 1-20
[6] S. Abu, S. R. Selamat, A. Ariffin , and R. Yusof, “Cyber Threat Intelligence – Issue and Challenges,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, No. 1, 2018, pp. 371-379. DOI: 10.11591/ijeecs.v10.i1.pp371-379
[7] A. Mathew, “Research Article Open Access Artificial Intelligence for Intent Based Networking,” *International Journal of Computer Science Trends and Technology (IJCST)*, vol. 8, no. 2, 2020, pp. 13-17.
[8] Kaspersky, “Research Reveals Hacker Tactics: Cybercriminals Use DDoS as Smokescreen for Other Attacks on Business,” 2016, [Online]. Available: https://www.kaspersky.com/about/pressreleases/2016 research-reveals-hacker-tacticscybercriminals-use-ddos-as-smokescreen-for-otherattacks-on-business (Accessed 15 June 2020).
[9] CPS, “Cybercrime - prosecution guidance,” The Crown Prosecution Service (CPS), Tech. Rep., 2019, [Online]. Available: https://www.cps.gov.uk/legal-guidance/cybercrimeprosecution-guidance (Accessed 17 June 2020).
[10] G. Tsakalidis and K. Vergidis, “A Systematic Approach Toward Description And Classification Of Cybercrime Incidents,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 4, 2017, pp. 710–729.
[11] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, “A taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets,” arXiv preprint arXiv:1806.03517, vol. 1, no. 1, 2018, pp. 1-35.
[12] N. A. Khan, S. N. Brohi, and N. Zaman, “Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic,” *TechRxiv Powered by IEEE*, 2020, pp. 1-7.
[13] A. Ren, C. Liang, I. Hyug, S. Broh, and N. Z. Jhanjhi, “A ThreeLevel Ransomware Detection and Prevention Mechanism,” EAI Endorsed Trans. Energy Web, vol. 7, no. 26, 2020, pp. 11-21.
[14] R. Richardson and M. North, “Ransomware: Evolution, Mitigation and Prevention,” International Management Review, vol. 13, no. 1, 2017, pp. 10-21.
[15] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, “A Taxonomy of Cyber-harms: Defining the Impacts of Cyber-attacks and Understanding How They Propagate,” *Journal of Cybersecurity*, vol. 4, no. 1, 2018, pp. 1-15



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY