ISSN 2278-3091
Volume 10, No.3, May - June 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1461032021.pdf
https://doi.org/10.30534/ijatcse/2021/1471032021

The Role of Machine Learning to Mitigate the Malicious Crime

Imdad Ali Shah, Dr.Noor Ahmed Shaikh, SqnLdr (R) Aneela Kiran,Shahid Hussain Danwar
Department of Computer Science Shah Abdul LatifUniversity Khairpur. Sindh, Pakistan
Shahsyedimdadali@gmail.com,noor.shaikh@salu.edu.pk,Aneelakiranansari73@gmail.com,
shahid.danwar@salu.edu.pk
Dr. Raja Majid Ali Ujjan
School of Computing, Engineering & Physical Sciences Unversity of the West of Scotland
raja_majidali@hotmail.com

ABSTRACT

Machine Learning has quickly impacted modern society in a variety of ways, increasing the machine's role in comparison to diverse human roles. As AI's function expands, it is becoming an increasingly important aspect of every industry. ML has a unique capacity to quickly classify data and detect patterns. This is impossible to find using a human observer to discern trends. The focus of this study was about how transnational criminal groups and cybercriminals might be exploited AI Technology maliciously. AI is a field of study that has the potential to drastically alter society's usage of information technology, notably in terms of how personal data will be linked and how hackers will gain access to private lives. Experts of artificial intelligence dispute over how quickly the technology will advance; however, cognitive scientists agree that the technology will advance at a rapid pace. The goal of this study to peer-review last five year research articles and associated book-chapters for dealing with malicious crime challenges, and the findings will be applied to machine learning algorithms. Furthermore, our research will pave the way for fresh research and professionals.

Key words: Malicious Crime, Machine Learning, Cyber security, Hacking Vulnerability, and Cyber Law

1. INTRODUCTION

The artificial intelligence (AI) research trend is evolving away from applications with a technological bent that concentrate on increasing productivity and performance and toward applications that are focused on supplementing human intelligence with artificial intelligence (Yang, 2021). New issues have emerged as a result of the shift in AI research trends, such as movements from broad sense to transfer intelligence, computation to cognition, customization to adaptation, known to unknown, one-size-fits-all to precision, and technology to humanity (Yang, 2019). People can use computer Vision apps to lower the risk from harmful attacks and transnational criminal groups. The goal would be to enable computers that think, imagine human activities of interest, or solve problems faster and more efficiently than humans. Several tasks and in organization, such as planning, moving, being creative, speaking, and socializing, can be improved using a variety of approaches. An artificial intelligence (AI) application for thwarting cybercrime [1] Hackers' preferred methods have changed. Erynn Tomlinson's bank account was hacked and she lost $30,000 in crypto currencies. This is known as Social Engineering Fraud [2]. Some of your personal information, such as your name, cell phone number, and bank account number, can leave you susceptible. NLP, DL, and ML are all technologies that can be used in conjunction. It can use objects to address cyber security concerns in a precise time frame. Natural Language Generation (NLG) is a component of AI that specifies how to generate text information from inputs. The technique of NLG is used to analyze data; it works by processing textual data and presenting the results in a natural language procedure. The goal of this study is to help people realize the greatest danger of AI before it is too late Figure-1.

AI is a field of study that has the potential to drastically alter society's usage of information technology, notably in terms of how personal data will be linked and how hackers will gain access to

private lives. Experts of artificial intelligence dispute over how quickly the technology will advance; however, cognitive scientists agree that the technology will advance at a rapid pace. In the near future, computing and machine learning are anticipated to have an impact on homeland security. The major goal of this work is to develop future strategies for dealing with malicious crime challenges, and the findings have been applied to machine learning algorithms. Furthermore, our research will pave the way for fresh research and professionals.

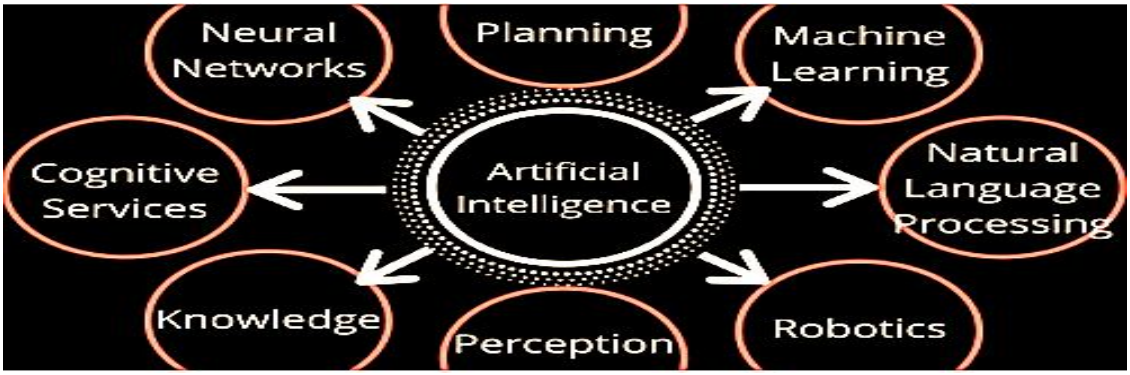


Figure-1 shows the concept of AI [2]

2. LITERATURE REVIEW

Table-1 Present Survey of AI Research Article

Year	Citation	Prose	Cones
2019	[3]	Invited focus mutually inside the private and public sector for growing AI application for detecting fraud	Appraised that AI might benefit from advanced defenses and decrease the influence of criminal attacks.
2020	[4]	Proposed a hybrid approach for computational architectures still proposal the maximum hopeful path with machines performing in an ethical style.	Appraised regarding ML's progress has headed to new concepts regarding the possibility and significance of machine ethics custody speed, through a growing emphasis on security, containment, and organization.
2020	[6]	Focused on determining law-breaking patterns applying real DM procedures.	Described its ability as the greatest relative with National Cyber Defense (NCD) plans, for it would be backing dynamic CDS, which earlier arranged by numerous government performers and can assist the growth of prevention approaches in cyberspace.
2020	[7]	Proposed Deep Learning	Described that AI-empowered cyber arms are already prototyped with autonomous malware.
2020	[9]	Proposed Deep Learning	Described the role of AI in cyber safety & submits suggestions on how administrations might get benefit from AI in cyber security.
2020	[10]	Proposed Deep learning	Described philosophical and political investigation of ethics at stake in confirming cyber security aimed at dangerous infrastructures.
2020	[11]	Risk performers regularly moving and refining violence policy through a specific concentration on the application of AI-driven methods in violence procedure, so-called AI-based cyber-attack might	Described current developments in AI technologies that impressed great emerging in advance and automation. As AI tools propose major profits,they might use them maliciously. AI-based cyber-

		apply to combine through traditional attack methods to reason larger loss. Despite numerous researches on AI and safety, studies have not briefed	attacks sufficient to be capable of knowing an opponent's activities and toward emerging right defenses against violence. Objectives of his research of AI-based cyber-attacks & diagram them in the suggested context, giving insight into new fears and grouping of numerous characteristics of malicious applied AI throughout the cyber-attacks life cycle. Further, this framework delivers sources aimed at their finding to predict forthcoming fears.
2020	[12]	As there is discussion at a pace in which AI research would emerge. No suspicion about authors satisfies, as AI explains the subarea's computer science which studies in what way computers might copy human intellect. Subarea and term of ML & DL stand frequently interference & there changing locations in what way fields interconnect.	Need to work more
2020	[13]	Mostly satisfies through the classification of ML though Jones trusts ML shelters study methods with a human monitor.	Trusts ML methods would categorize as structures that apply a neural network to classify info like humans ensure whereas to give strength enlarged handling accuracy & quickness.
2020	[14]	Focused on the user of AI	In the vast body of the researcher into possible malicious use of AI as an associatively current subset of AI, and numerous universities and organizations concentrate on protection forms aimed at AI. Various authors and ethicists believe that malicious AI remains a possible result of ethical study and that computer scientists would additionally consciously unplanned concerns of their study.

3. COMMON AI ISSUES

i. Computing capacity

Many programmers areirritated by how much energy these authority algorithms take. Machine Learning and DL are the pillars of AI, and to function properly, they require a much number of cores and GPUs. We have concepts and experience to implement DL frameworks in a variety of disciplines, including asteroid tracking, healthcare delivery, cosmic body tracing, and much more Figure-2 [15], [16], [17], [18], [19], [20]

.

Figure-2 shows

ii. **A Lack of Trust**

Uncertain nature of how DL models anticipate the output is one of the most fundamental elements that causes concern for AI. For a layperson, understanding how a certain set of inputs might design a solution for many types of issue is tough. Many people throughout the world are unaware of AI's use.

iii. **Knowledge Limitation**

Although there are numerous areas in the industry where AI may useas a more effective alternative to conventional approaches. The actual problem is AI knowledge,only a small portion of the population is aware of AI's potential, outside from techies, college students, and researchers.

iv.**Human-Level**

This is one of AI's most pressing issues, one that has kept academics on the lookout for AI services in businesses and start-ups. These corporations may advertise accuracy rates of over 90%, but people can outperform them in all of these instances. Allow our model to determine whether it's a picture of a male or a picture of a female, the human can almost always forecast proper outcome, with a remarkable accuracy of over 99%. To achieve similar results, a DL model would need unparalleled fine-tuning, hyper parameter optimization, a big dataset, and a well-defined and accurate algorithm, as well as robust processing capacity, continuous training on train data Figure-3.

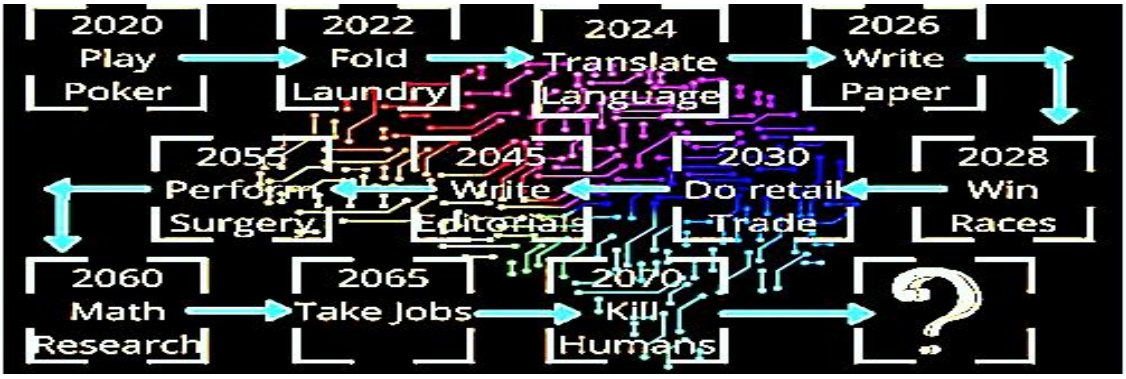


Figure-3 showsdata increasing [15]

v. **Data Security and Privacy**

The accessibility of information and resources to train deep and ML models is maximumsignificantissue to ponder and it is risk and can misuse. This information includes information regarding issues of health etc. To compound the problem andcurrentlyprovides data on the size of the planets. With maximum information reaching in from all directions, it's difficult to keep track of it all. Some businesses have already begun to develop inventive solutions to overcome these obstacles, it uses smart devices for train the data.

vi.**The Bias Issue**

The amount of data used to train an AI system determines whether it is good or terrible. As a result, in the future, the capability to obtain required information will key developing virtuous AI structures. However, information that the organizations collect on a daily basis is weak and has little meaning on its own. They are prejudiced, and they only identify the nature and characteristics of a small group of individuals who share on religion bases. Only by establishing various algorithms that can professionally track these challenges can genuine change be brought about.

vii. **Evolution Malicious Crimes 2021**

a. Microsoft claims that a new wave of cyber-attacks has targeted government institutions and human rights organizations in 24 nations, with majority of which are in the United States. Approximately 3,000 email accounts belonging to more than 150 different organizations were hacked this week (May 2021) Figure-4.

Figure-4 shows targeted attacks [21]

b. We noticed the cyber-attack on Wednesday and swiftly sent in a team of specialized cyber-technology specialists to investigate," Ms Morgan added. The National Cyber Security Centre will also assist us in resolving the situation Figure-5.

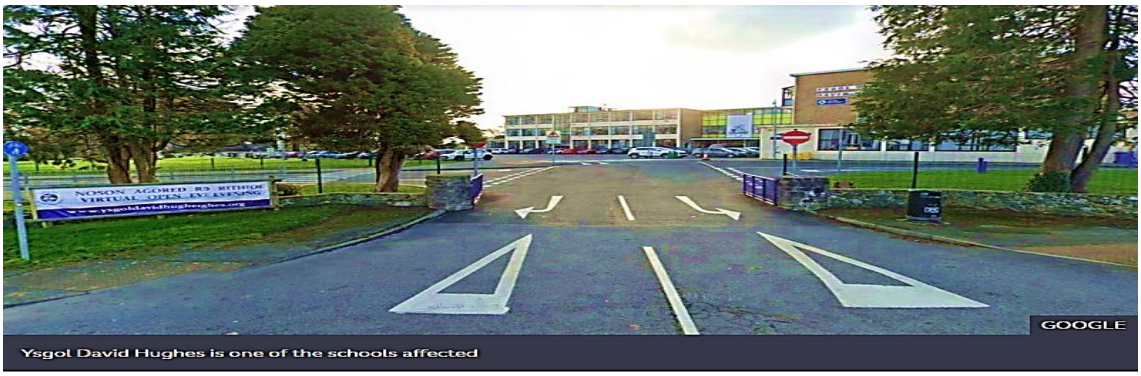


Figure-5 showstargeted attacks [22]

c. Other numbers released by the City of London Police, which coordinates anti-fraud activities, include Figure-6 :

i. Since the outbreak, more than 150 arrests have been made in connection with the pandemic.

ii. Over 2,000 websites, phone numbers, and email addresses associated with the offences have been removed.

iii. Between April and May 2020 and January 2021, when lockdowns were in effect, activity soared.

iv. There were a total of 416,000 fraud and cyber-crime reports.

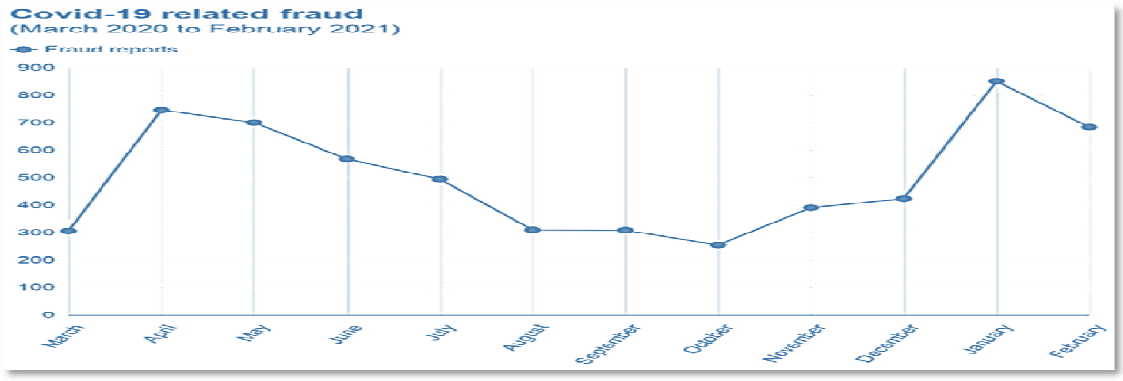


Figure-6 shows covid-19 related fraud [23]

4.DISCUSSION

AI is a field of study that has the potential to drastically alter society's usage of information technology, notably in terms of how personal data will be linked and how hackers will gain access to private lives. Experts of artificial intelligence dispute over how quickly the technology will advance; however, cognitive scientists agree that the technology will advance at a rapid pace. In the near future, computing and machine learning are anticipated to have an impact on homeland security. [4]. Many of these developments excite us, but we also want to focus attention to the ways in which AI might exploit maliciously. We examine such risks in depth so order to prevent or mitigate them, not only to avoid the related harms, but also to avoid delays in the implementation of AI's positive usesFigure-7 [23].

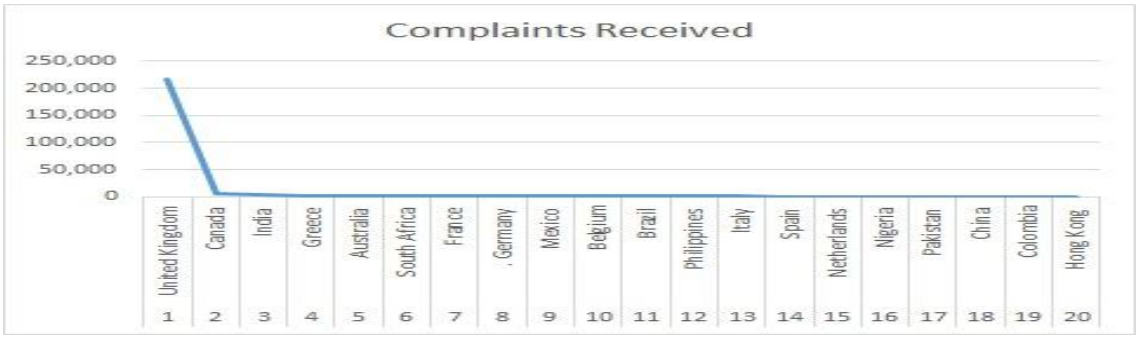
Figure-7 shows the malicious categories [23]

Computer machines that operate on a big scale and affect huge groups of people can make important and sometimes debatable judgments. Automated choices can have an impact on a variety of things, including credit scores, insurance payouts, and health assessments. These types of automation can become problematic when they systematically disfavor particular groups or people. These are instances of diaspora [24].

Medicine is at a juncture in its development. With the growing integration of Artificial Intelligence (AI) into the healthcare profession, the decisions we make now will have a significant impact on the future care of our patients. Globally, demographic healthcare inequities persist, and the impact of medical prejudices on various patient groups is still being investigated by researchers. At a time when clinical trials are on the rise, whether we project existing unfairness into the future or whether we reflect on what we believe to be true and challenge ourselves to be better will be determined by how we move forward. AI provides an opportunity and a mirror for all professions to better their social effect, and the stakes for medicine could not be higher [25].

5.RESULTS

Several research, review articles, and published reports on the issue have been peer-reviewed in the recent five years. Various regions have complained concerning malicious crime, and the same data has been examined using the k-NN algorithm for classification [26].



6.CONCLUSION AND FUTURE WORK

Machine Learning has quickly impacted modern society in a variety of ways, increasing the machine's role in comparison to diverse human roles. As AI's function expands, it is becoming an increasingly important aspect of every industry. ML has a unique capacity to quickly classify data and detect patterns. This is impossible to find using a human observer to discern trends. The focus of this study was about how transnational criminal groups and cybercriminals might be exploited AI Technology maliciously. AI is a field of study that has the potential to drastically alter society's usage of information technology, notably in terms of how personal data will be linked and how hackers will gain access to private lives. Experts of artificial intelligence dispute over how quickly the technology will advance; however, cognitive scientists agree that the technology will advance at a rapid pace. The goal of this study to peer-review last five year research articles and associated book-chapters for dealing with malicious crime challenges, and the findings will be applied to machine learning algorithms. Furthermore, our research will pave the way for fresh research and professionals. It also needs to focus on resolving disagreements about AI.

REFFERNCES

[1]Martin, C. Dianne. "TAKING THE HIGH ROAD White hat, black hat: the ethics of cybersecurity." *ACM Inroads* 8.1 (2017): 33-35.https://dl.acm.org/doi/fullHtml/10.1145/3043955

[2] Technology & Science February 8, 2019 CBC and https://www.upgrad.com/blog/top-challenges-in-artificial-intelligence/

[3] Martin, C. Dianne. "TAKING THE HIGH ROAD White hat, black hat: the ethics of cybersecurity." *ACM Inroads* 8.1 (2017): 33-35.https://dl.acm.org/doi/fullHtml/10.1145/3043955

[4] Harer, Jacob A., et al. "Automated software vulnerability detection with machine learning." *arXiv preprint arXiv:1803.04497* (2018). https://arxiv.org/abs/1803.04497

[5] Russell, Rebecca, et al. "Automated vulnerability detection in source code using deep representation learning." 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, 2018. https://ieeexplore.ieee.org/abstract/document/8614145

[6] Hiller, Janine S. "The benefit corporation and corporate social responsibility." *Journal of Business Ethics* 118.2 (2013): 287-301. https://link.springer.com/article/10.1007/s10551-012-1580-3

[7] Li, Zhen, et al. "VulDeeLocator: A Deep Learning-based Fine-grained Vulnerability Detector." *arXiv preprint arXiv:2001.02350* (2020).https://arxiv.org/abs/2001.02350

[8] Harer, Jacob A., et al. "Automated software vulnerability detection with machine learning." *arXiv preprint arXiv:1803.04497* (2018). https://arxiv.org/abs/1803.04497

[9] Russell, Rebecca, et al. "Automated vulnerability detection in source code using deep representation learning." *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 2018. https://ieeexplore.ieee.org/abstract/document/8614145

[10] Li, Yuwei, et al. "V-fuzz: Vulnerability-oriented evolutionary fuzzing." *arXiv preprint arXiv:1901.01142* (2019). https://arxiv.org/abs/1901.01142

[11] Russell, Rebecca, et al. "Automated vulnerability detection in source code using deep representation learning." *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 2018. https://ieeexplore.ieee.org/abstract/document/8614145

[12] Movahedi, Yazdan, Michel Cukier, and IlirGashi. "Vulnerability prediction capability: A comparison between vulnerability discovery models and neural network models." *Computers & Security* 87(2019):101596.https://www.sciencedirect.com/science/article/pii/S0167404819301581

[13] Al-Msie'deen, Ra'Fat. "Automatic labeling of the object-oriented source code: The lotus approach." *arXiv preprint arXiv:1803.00048* (2018). https://arxiv.org/abs/1803.00048

[14] Seng, Lim Kah, NorafidaIthnin, and Syed ZainudeenMohdShaid. "Automating Penetration Testing Within an Ambiguous Testing Environment." *International Journal of Innovative Computing* 8.3 (2018). https://ijic.utm.my/index.php/ijic/article/view/180

[15] https://www.sciencedirect.com/science/article/pii/S2666920X21000023

[16] Almusaylim, Z. A., Alhumam, A., Mansoor, W., Chatterjee, P., &Jhanjhi, N. Z. (2020). Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things. https://www.preprints.org/manuscript/202007.0476/v1

[17] Shafiq, D. A., Jhanjhi, N. Z., Abdullah, A., &Alzain, M. A. (2021). A Load Balancing Algorithm for the Data Centres to Optimize Cloud Computing Applications. *IEEE Access*, *9*, 41731-

41744.https://ieeexplore.ieee.org/abstract/document/9374987
[18] Hussain, F., Hassan, S. A., Hussain, R., & Hossain, E. (2020). Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges. *IEEE Communications Surveys & Tutorials*. https://ieeexplore.ieee.org/abstract/document/8951180
[19] Singhal, V., Jain, S. S., Anand, D., Singh, A., Verma, S., Rodrigues, J. J., ...&Iwendi, C. (2020). Artificial intelligence enabled road vehicle-train collision risk assessment framework for unmanned railway level crossings. *IEEE Access*, *8*, 113790-113806.https://ieeexplore.ieee.org/abstract/document/9117007
[20] Hasan, Mahmudul, et al. "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches." *Internet of Things* 7 (2019): 100059.https://www.sciencedirect.com/science/article/pii/S2542660519300241
[21]https://www.bbc.com/news/world-us-canada-57280510
[22] Hasan, Mahmudul, et al. "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches." *Internet of Things* 7 (2019): 100059.
https://www.sciencedirect.com/science/article/pii/S2542660519300241
[23] https://www.bbc.com/news/technology-56499886
[24] https://arxiv.org/pdf/2008.07309.pdf
[25]Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ...&Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.https://arxiv.org/abs/1802.07228
[26]https://cdn.comparitech.com/wp-content/uploads/2018/10/Secure-D-compromised-mobile-apps-2021.jpg