Ethical Hacking: Importance, Controversies and Scope in the Future

Vishnuram G
School of Computer Science and Engineering,
Vellore Institute of Technology
Chennai, 600127, Tamilnadu, India
vishnuram.g2020@vitstudent.ac.in

Dr. Khushboo Tripathi
Assistant Professor, Department of Computer Science and Engineering,
Amity University, Haryana
khushbootripathi.cse@gmail.com,

Amit Kumar Tyagi[0000-0003-2657-8700]
School of Computer Science and Engineering,
Vellore Institute of Technology
Chennai, 600127, Tamilnadu, India.
amitkrtyagi025@gmail.com

Abstract. With the ongoing digitalisation of the modern world and our quest to digitalise and automate everything, issues related to cybersecurity such as data breaches, security breaches etc., will be in the spotlight. Therefore, ethical hacking and its importance in the future can't be undermined. Ethical hacking technology has spread to almost all fields of the life and especially to all paths of computer industry; the need to protect the important data of the same should be addressed with right technology. In ethical hacking (i.e., white hat hacking) the objective in hand is to find weaknesses in the security systems and find potential data breaches and is in stark contrast to the almost universal definition of hacking i.e., to breach the security systems of individuals or companies with malicious intent and to steal data and plant viruses (black hat hacking). ethical hacking is a way of combatting and neutralising black hat hackers. With this research paper, my objective is to analyse and establish the importance of ethical hacking and also to analyse the controversies surrounding it, its pros and cons, its ethical and moral boundaries and its scope in the future.

Keywords: Data breaches, security breaches, ethical hacking, cybersecurity, white hat hacking, black hat hacking, security systems

I. INTRODUCTION

In the modern world where every transaction, chat, and call can be tracked, traced and deciphered, there is a growing concern for security which inevitably generates the topic of ethical hacking. The digitalisation era has led to great benefits and made life easy but it has repercussions like the increasing number of cases involving hacked online social media accounts, bank accounts, stolen data etc. To combat these Black Hat Hackers (criminals who bypass security protocols and break into computer networks with malicious intent), Ethical hacking has been particularly helpful as it identifies the weakness in the security helping to strengthen it and prevent being hacked. Even though ethical hacking is good, sometimes the ethical hackers venture into the illegal world and become black hat hackers and use their knowledge for harm rather than good. Also, large number of black hat hackers have converted to white hat hacking which has been a huge controversy as they need to be completely trustworthy. This has led many to question the rationale behind the training of ethical hackers and hacking in itself.

978-1-6654-8035-2/22/$31.00 ©2022 IEEE

1.1 Motivation

The motivation to select this topic and study it for research is the complexity of the art of ethical hacking and the huge interest. I have in this particular field. It requires very high level of knowledge regarding programming, computer networks and communications and it requires you to think outside the box and put yourself in the shoes of a black hat hacker causing you to continuously hone the mind in preparation for tackling the various challenges in ethical hacking. It's a very exciting field with tremendous opportunities and has a huge scope in the future. With computers and automatons taking over the world, Cybersecurity will be in the forefront of digitalization in the future and a huge emphasis will be laid on the importance of ethical hacking. The complexity of the subject and my interest in it along with the importance it will have in our future has driven me to select this as my research topic

Organization of work

Section 1 of this paper begins with the abstract which explains the aim and objective of this research paper. Section 2 explains my motivation and desire to take this as my research topic and also how the work has been organized so that the reader can easily navigate through the paper. Section 3 starts off with an introduction followed by the basic pre-requisite knowledge about ethical hacking, the skills required to be a proficient hacker and types of hackers. Section 4 details the importance of ethical hacking and why it's needed now and in the future. Section 5 is about the various pros and cons of ethical hacking. Section 6 has been dedicated to ethics in ethical hacking and a code of ethics for ethical hackers has been laid down. Section 7 is regarding the endless controversies and dilemmas involved in the teaching and practice of ethical hacking. Section 8 realizes the scope for ethical hacking in the future. Section 9 concludes the paper with a conclusion.

II. WHAT IS ETHICAL HACKING

The gaining of unauthorized access to data in a system or computer is called hacking. Hacking into a computer network in order to test or evaluate its security, rather than with malicious or criminal intent is called ethical hacking. This is done by hired professionals called ethical hackers (also known as white hat hackers) who, instead of exploiting the system or network, find the vulnerabilities of your security systems and provide advice and guidelines to improve it.

2022 International Conference on Computer Communication and Informatics (ICCCI) | 978-1-6654-8035-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCCI54379.2022.9740860

They sidestep the framework security system and focus on the chinks in it that could be abused by malicious hackers. This data is then analysed and utilised by the association or company that hired them to potentially limit or wipe out all chances of potential assault.

III. SKILLS REQUIRED TO BE ETHICAL HACKER

3.1 Computer Networking Skills

It's one of the most essential and basic skill to be mastered prior to embarking on the journey of becoming an ethical hacker. The computer networks are basically the interconnection of multiple devices generally called Hosts [8] which are connected through multiple paths to send and receive data or media. Understanding and analysing networks such as DHCP, Subnetting and Supernetting [8] etc. will help hackers understand the nuances of various network and communication systems and help explore the multiple interconnected systems in a network and help predict potential security threats they might create.

3.2 Computer Skills

The skills pertaining to the knowledge and ability that help understand and use computers and computer related technology can be termed as computer skills. The basic skills include creating presentations, writing documents, managing files on the computer, data processing etc…Advanced skills include programming, creating and managing databases, spreadsheet calculations etc…Some of the essential skills for any hacker are Web, Spreadsheets, Email, MS Office, social media, Database management etc.

3.3 Linux Skills

It's a community of open-source UNIX like OS that are based on the Linux kernel. It's free and can be distributed and modified both commercially and recreationally under the GNU General Public License [8]. The reason that Linux is the preferred operating system of majority of hackers is its security. It's more secure than any other operating system but that doesn't mean its 100% malware or spyware free [8] but it's less vulnerable to them and does not require anti-virus software most of the time.

3.4 Programming Skills

Another essential skill and one of the most important skills required to be an ethical hacker is programming skills. A hacker must be an expert programmer and must be able to write intense and long codes. Some of most popular languages include Python, C, C++, SQL, Perl, PHP, JavaScript, Java, Ruby.

3.5 Basic Hardware Skills

The physical components of a computer like the CPU (Central Processing Unit), monitor, mouse, keyboard, sound card, graphic card, computer data storage, motherboard, speakers [8] etc. If the hacker does not have basic hardware skills, it will be tough for him to understand how data is transferred through USB's or cables or how the BIOS and CMOS work together etc.

3.6 Reverse Engineering

The process of recovering the requirement specifications, product design and functions of a product from the analysis of its code is called reverse engineering. Its aim is the expedition of maintenance work by improving the understandability of a system and to produce the necessary documents for a legacy system. It's often used to identify system vulnerabilities or loopholes and security flaws in software security.

3.7 Cryptography Skills

The art of using codes to secure information, data and communications in the presence of third parties called adversaries such that only the person, for whom that message was intended for, could understand it is called cryptography. It contains protocols analysed and developed to prevent malicious third parties from retrieving information shared between two agencies [8]. It deals with converting readable messages to a non-readable form called cipher or ciphertext while only the receiver contains the key to decipher it [8].

3.8 Database Skills

The discipline related to dealing with the creation, upgradation and maintenance of databases is called DBMS (Database Management Systems). Since companies store most of their information in the form of database, they are frequently the target of black hat hackers. An ethical hacker must have a good understanding of data schemes, database engines etc…to help the organization maintain a secure database [8].

3.9 Problem-Solving Skills

The determination of the source of a problem and finding an effective and efficient solution it is called problem-solving. Though the various technical skills mentioned before are vital, the various mental skills as being creative, thinking out of the box, critical thinking and great willpower which help in being a dynamic problem solver are a must for ethical hacking as it involves various mental challenges that require lots of patience. Being able to think from the perspective of a black hat hacker helps in understanding how the system will be attacked. So, the various mental skills and intangibles can't be undermined and are essential to being an ethical hacker.

3.5. Types of Hackers

3.5.1 White hat hackers

As mentioned above, they are hired professionals who sidestep the framework security to find out weak points that could potentially be exploited by malicious hackers. They are

supposed to be trustworthy and not exploit any of the sensitive information they get [5].

3.5.2 Black Hat Hackers

The most well-known type of hackers and with whom hacking is usually associated. Also known as Crackers, they hack into systems to gain unauthorized access to the data and information in them with intention of stealing them or to harm the computer by planting threats like viruses [5], spyware, malware etc. They violate privacy, block network communication, exploit your sensitive data etc...

3.5.3 Grey Hat Hackers

They are a group of hackers who gain unauthorized access to your system by bypassing system framework security but they neither exploit nor help the owner, instead they hack just for fun [5]. They can be called a blend of both white hat and black hat hackers. They usually do it for appreciation or as a bet or for bounty.

3.5.4 Red Hat Hackers

Red hat hackers are again a blend of both black hat and white hat hackers [5]. They usually involve themselves in classified intel like a country's defence and research sectors. They are involved in government and top-information hub and generally anything that falls under the category of sensitive information.

3.5.5 Blue Hat Hackers

A hacker that is employed by agencies and companies who is, outside of computer security consulting firms, used to bug test a system prior to its launch [5]. They look for loopholes and try to close these gaps. Microsoft also uses the term Blue Hat to represent a series of security briefing events [5].

3.5.6 Green Hat Hackers

A green hat hacker (also called a neophyte, noob, newbie etc..) is someone who is new to hacking and has almost no knowledge or experience of working and methods of hacking or hacking related technology [5].

3.5.7 Script Kiddie

Used to describe someone who uses pre-packaged automated tools written by other hackers to break into computer systems and networks with no knowledge of the underlying concepts and working [5].

3.5.8 Hacktivist

A hacker who hacks into webpages, or homepages of organizations usually to announce a social, ideological, cultural or political message. Also called suicide hackers they are not concerned with the consequences of their hacking and aim to damage the victim irrevocably [5]. Usually involves defacement of the site or page and denial-of-service attacks.

IV. IMPORTANCE AND NEED FOR ETHICAL HACKING

With the exponential rise of cybercrimes like Black hat hacking, planting of malware and spyware and viruses on systems, hacking into networks etc. companies and organizations need a counter measure to combat these illegal assaults on their systems. Since it is done by hired professionals it provides an unbiased analysis of a company's security framework and architecture [6]. Ethical hacking ensures that all the systems are protected and not accessible by black hat hackers. These days, there are numerous cases of hacking attacks not just of individuals but even technology and social media giants like Facebook, twitter have been hacked. Ethical hacking tools such as scanners designed to check the network systems are misused by malicious black hat hackers [6]. Excessive use of automated scanners which start searching for vulnerabilities after a period of time have made internet less secure. That's why there is a huge demand for ethical hackers. Governments employ ethical hackers sponsored by them to keep eyes and ears open against enemy states and to secure intelligence and data pertaining to the political scene and internal affairs as well as external affairs. In the era of international conflicts, the threat of cyber-terrorism, and terrorist groups funding cybercriminals, national security is continuously at risk [6].

The Government of India had put in motion a National Cybersecurity Policy in 2013, which aimed to generate a workforce of 500,000 cybersecurity experts, besides several additional provisions. In late 2016 ,2 hackers breached the database of Uber and stole the data of around 57 million users including sensitive information [2]. This led to the dismissal of the then Chief Security Officer and also lot of legal complications. They could further identify individual targets to exploit using the information they stole. Most of the time the repercussions of a security breach can be felt years after the incident. Companies may lose the trust and confidence of the customers and in most cases are held legally responsible for any loss to their customers. The cost can exponentially rise due to legal fees, investigative fees, drop in stock performance, reputation management, customer support etc. Ethical hacking is used to secure important data from enemies. It safeguards you and your computer from blackmail and exploitation by the people who want to exploit the loophole and weaknesses of your systems security to gain sensitive data for selfish gain. Using ethical hacking, a company or organization can find out security vulnerabilities and risks. Many of techs' Goliaths like Google, Microsoft, Apple, Facebook, Uber etc. hire ethical hackers to secure their systems. They also conduct bug bounty programs and campaigns where hackers all over the world are allowed to hack the website or system of the company to find the bugs. They are rewarded for finding bugs. Trained ethical hackers are a must in every company when implementing new software or systems. Dangerous software and viruses like Trojan horses can be prevented from being placed in your computer systems with the help of ethical hacking. Ethical Hacking is a must in order to prevent these potential threats especially as digitalisation is only going to be increasing. Viruses, ransomware, worms, and malware are doubling in

number, with the advancement of technology, making ethical hacking a necessity [6].

V. PROS AND CONS

5.1 Pros and advantages

- It can provide convincing and decisive evidence of real network or system level threat exposures through proof of access [1]. Even though the findings may be negative in nature, it will help expose the potential loopholes and weaknesses in framework security and it can be proactive in improving the overall security of your systems [1]. The results provide a clear picture of the strength of the detection processes and response mechanisms.
- It also identifies the ignorance in systems security administrators or the management as they may not be aware or up to date on the latest technology and methods used by hackers or the gravity of a potential cyberthreat. These findings might help spread awareness on their part and promote the need for better awareness on cybersecurity.
- It plays a huge role in securing the nations' most valuable secrets and deals. A security breach in the data involved in government deals related to defence and research could be devastating for the country's security. Also, Cyberterrorism from other countries can be combatted effectively.

5.2 Cons and disadvantages

- Educating and training people to be ethical hackers can also prove to be counterproductive as the true intentions of people can't be deciphered and they may use their skills to become black hat hackers.
- Ethical Hackers are very costly to hire. They charge exorbitant charges for their service if companies hire them. Also, the company's privacy is compromised as they don't know what kind of information the hacker has retrieved from their systems.
- Any mistake by an amateurish hacker while conducting certain kinds of tests can prove to be dangerous as it might corrupt the files and hamper system operation. Companies must be careful to hire only certified professionals to conduct ethical hacking.

5.3 Ethics in Ethical Hacking

In many fields of work, having a moral code and ethics is a necessary instrument to becoming a trusted professional. The importance of ethics in ethical hacking is paramount to the career of a white hat hacker as a blemish in the background check can cause them to be rejected as untrustworthy. Especially due to the nature of work in ethical hacking they encounter critically confidential and private information and data that they must not exploit or take advantage of. In this regard they must have a code of ethics to guide them in handling such information and data. Their code must focus on the protection of the client's interests and handling their work effectively [2] and efficiently in securing the client's systems from potential cyberthreats.

5.4 Code of Ethics in Ethical hacking

1. Before conducting ethical hacking, the hacker must ensure that he/she understands the nature and characteristics of the client's systems, networks and framework security. This will help them handle and act accordingly to the sensitive and confidential information they encounter.
2. Before and after performing ethical hacking, a hacker must be aware of the degree of sensitivity and confidentiality of the information he/she may be involved with. They should not violate laws, rules and regulations and company policy in handling such information.
3. They should always maintain transparency with the client and must be trustworthy at all times. All relevant information unveiled must be communicated properly to the client. Transparency ensures there is a clear understanding of the procedures done and findings discovered by the hacker.
4. While performing ethical hacking the hacker must be careful to not access any system or software other than what the client signed up for. It's possible for them to have access to certain out of bounds networks but they shouldn't cross the limits set by client. Minimizing exposure of confidential information increases trust and reliability in a hacker.
5. After the completion of Ethical hacking and the agreement signed with client is executed, the hacker must never reveal the data and information he discovered to a third party. Ethical hacking is done to ensure the security of a system [2]. Revealing info would make the process obsolete and ineffective. Private and confidential data must remain private and confidential.

VI. CONTROVERSIES AND DILEMMAS

1. Teaching the art of Ethical Hacking and Training hackers has long been a controversial topic with various debates and arguments both in favour and against. People in favour highlight its importance in averting cybercrimes and improving security systems but people against it highlight the fact that many ethical hackers venture into the dark side to become black hat hackers and that we are spending resources on training the very people we intend to combat and neutralize. They argue it's like giving a loaded gun to a person without knowing his background and intent.
2. Most of the Ethical Hackers are not permanent staff of the company, they are hired professionals who charge for their service, so they are only temporary. Giving access to sensitive and confidential information to such individuals is a huge dilemma for the company as they may misuse that

information for blackmailing for ransom or sell it for money.

3. Every Hacker is a potential malicious threat who may misuse his capabilities for his personal and financial gain. There are possibilities that hackers working for clients might retrieve sensitive information outside of what was agreed upon. Researches have shown that 90% of hacking incidents come from within the organization or with help of an inside person.
4. Legal liabilities are debatable in incidents related to ethical hacking. Laws and legal procedures are a grey area in regards to ethical hacking. If the ethical hacker finds vulnerabilities in a security system and after some time if a malicious hacker hacks into the client's system It's not clear whose fault it is, i.e., whether the ethical hacker did not do his job properly or whether the client had failed to act upon the advice given.
5. The Ethical conflict is a huge controversy due to different theories of ethics at a loggerhead in regards to ethical hacking. In accordance to the Kant theory which pinpoints rights and wrongs based on the duties of humans no matter the cause or outcome, ethical hacking is ethically wrong as it's basically invading the right to privacy by gaining access to sensitive information of others but in accordance with Consequential theory, which defines ethicality based on the cause and outcome, it's ethically correct [2]. So, the ethicality depends on the cause and outcome. This is another huge controversial debate in regards to the ethicality of ethical hacking.
6. Also, once an organization finds a supposedly trustworthy individual who performs ethical hacking successfully and helps them, they might become dependent on them which they may take advantage of in the future by raising the charge for their services or being lethargic in work as they realize they are dependent on them.

VII. SCOPE OF ETHICAL HACKING

Ethical Hacking has a huge scope and will be one of the most important aspects of the digital world in the near future due to the rapid digitalization of the world leading to the takeover of computers and automatons. The huge security risks will have to be neutralized. Tech giants will employ ethical hackers at a large rate and will conduct loss of bug-bounty hunting to find vulnerabilities in their systems to protect their secrets from becoming public or accessed by black hat hackers. Also, the threat of cyberterrorism by enemy countries or terrorist groups will increase and governments will put great emphasis on securing their systems in defence sector, research sector, ministry affairs, home affairs etc. They are also recruited by RAW, CBI, NSA etc, which require their skills for various encryption and decryption tasks and to penetrate enemy systems to gain valuable information to improve national security. The transition to cloud computing is another reason the emphasis on ethical hacking and cybersecurity is only going to increase. Cloud computing is gaining momentum and lot of companies operate on cloud-based storages and software which contain a huge risk of security breach [7]. The 2016 Uber breach was due to the hackers hacking into a private are of GitHub where they found the log in credentials of Uber to the Amazon cloud computing service, AWS (Amazon Web Services) using which they collected personal details, including name, phone number and addresses of staff and customer alike, of almost 57 million users [4]. To prevent such major hacking incidents and security breaches in cloud-based servers, software and systems, ethical hacking is a necessity [7]. The major gap between untapped talent and requirement of professionals well versed in cyber security is huge. In the United States, there is a vacancy of almost 350,000 jobs in cybersecurity which is predicted to increase by tenfold [7]. Companies may be dismayed by this as they would want to retain their cybersecurity experts and ethical hackers [8] but as a hacker the opportunities are tremendous for personal, educational and financial gains and the sky is the limit for everybody aspiring to be ethical hackers. Further, the readers are suggested to read work [9-20] to know more about types of attacks and countermeasures/ techniques, tools, for different sectors etc., for the discussed attacks like sybil, man in middle, worm, Botnet, etc.

VIII. CONCLUSION

Based upon the data and information studied, I have come to the conclusion that ethical hacking, though it has its faults and disadvantages, has the potential to do better than harm when its capabilities are diverted in the correct direction. The ongoing digitalization of almost all daily activities (Net Banking, E-commerce, online meetings and classes) and also the continuous upgrade of computers and technology has made it a mandate for ethical hacking. Taking into account the various advantages and disadvantages, it must be exercised with proper caution and care. To protect from Black Hat hackers who misuse these tools for their selfish gain and also to safeguard security frameworks and prevent cyberthreats, ethical hackers are required. All the companies require ethical hackers to counter check their security systems and find vulnerabilities in them to improve them. They do so by hiring certified professionals or conducting worldwide bug bounty events and programs. Governments and intelligence agencies acquire ethical hackers in abundance as they are important and valuable to encrypt and decrypt messages and also to hack into enemy communications to retrieve valuable data that may help protecting the country from Cyberterrorism by outside agencies. While the controversies and debates surrounding its ethical boundaries are countless, it cannot be discarded on their basis as like every other invention of man it is just a tool which depends on the hand of the person that wields it. In the wrong hands it's a weapon used to destroy and harm, but in the correct hands it's a tool to protect and develop.

REFERENCES

[1] Bhawana Sahare, Ankit Naik, Shashikala Khandey," Study of Ethical Hacking", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Nov-Dec 2014.

[2] Rowena Johansen, Ethical Hacking Code of Ethics: Security, Risk & Issues, Panmore Institute, MARCH 24, 2017

[3] Important Benefits of Ethical Hacking, Cybersecurity Certification Course, edureka, Nov 17,2020
[4] Dave Lee, Uber concealed huge data breach, www.bbc.com, 22 November 2017
[5] Ethical Hacking - Hacker Types, https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_hacker_types.htm
[6] Ethical Hacking and the issues related to it? institute.careerguide.com, https://institute.careerguide.com/ethical-hacking-and-the-issues-related-to-it/
[7] Olivia Marie, Ethical Hacking 101: Definition | Benefits | Importance | Types, colocationamerica, February 20, 2020
[8] Skills Required to Become a Ethical Hacker, geeksforgeeks.org, 22 Jun, 2021, https://www.geeksforgeeks.org/skills-required-to-become-a-ethical-hacker/
[9] Meghna Manoj Nair, Amit Kumar Tyagi, Richa Goyal, Medical Cyber Physical Systems and Its Issues, Procedia Computer Science, Volume 165, 2019, Pages 647-655, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.01.059.
[10] Amit Kumar Tyagi, G. Aghila, "A Wide Scale Survey on Botnet", International Journal of Computer Applications (ISSN: 0975-8887), Volume 34, No.9, pp. 9-22, November 2011.
[11] Amit Kumar Tyagi. Article: Cyber Physical Systems (CPSs) – Opportunities and Challenges for Improving Cyber Security. International Journal of Computer Applications 137(14):19-27, March 2016. Published by Foundation of Computer Science (FCS), NY, USA.
[12] G. Rekha, S. Malik, A.K. Tyagi, M.M. Nair "Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security", Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 72-81 (2020).
[13] S. Mishra and A. K. Tyagi, "Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technolgy," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 123-128, doi: 10.1109/I-SMAC47947.2019.9032557.
[14] Amit Kumar Tyagi, Aswathy S U, G Aghila, N Sreenath "AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology" IJIN, Volume 2, Pages 175-183, October 2021.
[15] Amit Kumar Tyagi, S U Aswathy, Autonomous Intelligent Vehicles (AIV): Research statements, open issues, challenges and road for future, International Journal of Intelligent Networks, Volume 2, 2021, Pages 83-102, ISSN 2666-6030. https://doi.org/10.1016/j.ijin.2021.07.002.
[16] Goyal, Deepti & Tyagi, Amit. (2020). A Look at Top 35 Problems in the Computer Science Field for the Next Decade. 10.1201/9781003052098-40.
[17] Madhav A.V.S., Tyagi A.K. (2022) The World with Future Technologies (Post-COVID-19): Open Issues, Challenges, and the Road Ahead. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. https://doi.org/10.1007/978-981-16-6542-4_22
[18] Mishra S., Tyagi A.K. (2022) The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications. In: Pal S., De D., Buyya R. (eds) Artificial Intelligence-based Internet of Things Systems. Internet of Things (Technology, Communications and Computing). Springer, Cham. https://doi.org/10.1007/978-3-030-87059-1_4
[19] Nair M.M., Kumari S., Tyagi A.K. (2021) Internet of Things, Cyber Physical System, and Data Analytics: Open Questions, Future Perspectives, and Research Areas. In: Goyal D., Gupta A.K., Piuri V., Ganzha M., Paprzycki M. (eds) Proceedings of the Second International Conference on Information Management and Machine Intelligence. Lecture Notes in Networks and Systems, vol 166. Springer, Singapore. https://doi.org/10.1007/978-981-15-9689-6_36
[20] D. Goyal, R. Goyal, G.Rekha, S. Malik and A. K. Tyagi, "Emerging Trends and Challenges in Data Science and Big Data Analytics," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 2020, pp. 1-8, doi: 10.1109/ic-ETITE47903.2020.316.