Cyber Security and Awareness in the Modern Digital World

Vanshika Pathekar[1], Dr Neeti Arora[2], Priti Rai [3]*, Dr Anshu Singh[4], Akanksha Singh[5], and Sujeet Kumar [6]

[1]Research Scholar, PhD (Information Technology)
Rabindranath Tagore University, Bhopal, Madhya Pradesh
vanshikapathekar@gmail.com

[2]Assistant Professor- ABES Engineering College, Ghaziabad, U.P.
neetiarora251@gmail.com.

[3]Assistant Professor- Professor- Department of Commerce, College of Vocational Studies, University of Delhi, New Delhi, NCR, India [3] raipritiaxis1992@gmail.com.

[4]Assistant Professor- ABES Business School, Ghaziabad, U.P.
Anshusingh0508@gmail.com

[5]Assistant Professor- ABES Business School, Ghaziabad, U.P.
akankshasingh489@gmail.com

[6]Greater Noida Institute of Technology, Greater Noida, U.P.
sujeetsingh142000@gmail.com

Correspondent Author: Dr. Priti Rai, raipritiaxis1992@gmail.com.

Abstract
Cybersecurity is crucial in today's digital era. The crucial concern is keeping information secure. Cybercrimes, which are on the rise daily, are the primary concern whenever we consider cybersecurity. In order to stop these cybercrimes, numerous governments and businesses are enacting innumerable precautions. Despite many precautions, various people continue to have serious worries about cybersecurity. This paper focuses on explaining the cyber-crimes and issues that can be prevented by cyber awareness using cyber morals and ethics.

Keywords: Cyber threats, cyber-attacks, cyber security, cyber awareness, morals and ethics, data security.

1. Introduction

In the modern digital world, governments and people are emphasizing digitalization by prioritising cashless transactions, improving the Information Technology sector, and launching new technologies to ease human efforts. The use of the Internet and Cyber Media has become a trend and is growing vastly these days. Every new trend comes with some good and bad things. Since almost 60 percent of transactions are done online

P. Johri et al. (eds.), *Proceedings of the International Conference on Sustainable Computing and Artificial Intelligence (ICSCAI 2025)*, Advances in Engineering Research 298,
https://doi.org/10.2991/978-94-6239-674-6_42

today, it is inevitable that Digitalization also comes with a lot of concerns in which data security and awareness are a priority. The Internet hasn't always been utilized for beneficial purposes. A certain group of individuals emerged and attempted to use their newfound power for their own ease, they quickly gained knowledge of programming skills required for being steps forward in the cyber world. There are three different kinds of these individuals, who are referred to as hackers. The three main kinds of hackers are white-hat (ethical) hacks, grey-hat hackers and, black-hat hackers, . This hacker utilises various programming skills to hack into users' systems with illegal means to conduct cybercrime. In order to prevent cyber threats and security issues, Cyber Security came into perspective to help with secure transactions of data in any form, such as email, audio, video, and also online cash transactions. Cybersecurity is needed not only in the Information Technology industry but also in cyberspace, mobile computing, cloud computing, E-commerce, online banking, and many more places.(Sheth A, 2021)

Fig. 1. ***Cyberspace***

The most important question here is why cybersecurity is required? Suppose a hacker impersonates a bank employee and asks you for your card details as they need to update their database with your information. In unawareness, the customer shares his sensitive personal data with the hacker. He can use the data for theft resulting in a big scam. Another example is a hypothetical situation where the IT company stores all their data such as employee details, company information, and sensitive information of their clients on a cloud platform. A hacker conducts various Cyber-attacks on the cloud platform and gets access to all the company data. Now, an attacker can either steal cash using personal data or can make the sensitive data public leading to an even bigger threat to the company's reputation. In order to persuade people that one of modern society's most ignored requirements is cyber security, it must be made clear that not everyone cares enough to take adequate precautions to prevent being hacked. Since a lot more work is now done digitally than in the past, keeping everything updated is crucial to ensuring that everything is secure. they worked on brand occurrence on internet media, brand attitude and brand attachment (Rai p. et al, 2023)

Fig. 2. ***Cyber Security is Important***

2. Need of the Study

Using the National Cyber Security Policy from 2013, The attackers do not decrease behind with the advancement of innovative cyber security technology. They focus the weak points of many businesses worldwide by using refined and better hacking techniques. Military, legislative, financial, medicinal, and corporate organizations collect, use, and store unprecedented amounts of data on PCs and other devices, making cybersecurity critical. (Vallarelli N,2020) Given the constantly changing nature of cyberspace, it is now requisite for certain actions to be consolidated under a National Cyber Security Policy, accomplish with an integrated vision and a set of sustaining and coordinated strategies for implementation.

3. Objective of the Study

- To examine the requirement for cybersecurity in today's digital world to prevent cybercrime with proper cyber awareness using Cyberlaw, ethics, and morals.

4. Review of Literature

Parikh T.P. et al 2017 In the article entitled suggested that since of the unprecedented quantities of data that the military, administration, financial, medical, and commercial sectors collect, practice, and store on PCs or different devices, cybersecurity is critical. (Singh A, 2021), confidential data can make up a sizeable serving of that data, including financial data, intellectual property, private information, and other kinds of data for which unlicensed access or acquaintance could have uncomplimentary effects.
In this article entitled Emerging Issues of Cyber Attacks & Security in our nation studied in this article, she suggests that despite numerous protections, various people continue to have serious cybersecurity fears (Kumar S, 2021). In today's society, where internet access is widely available, data security has emerged as the most significant challenge. To take care of data, one must take precautions such as installation antivirus software, using firewalls, creating strong passwords, and practicing hacker prevention. India needs to adopt a proactive strategy instead of a reactive one, where system protection decisions are made only when cybersecurity incidents occur (Gupta M, Gupta D., and Rai P. 2023)

4.1 Cyber Crime and Issues in Modern World

Any illegal activity that relies heavily on computers for its execution in order to steal data is referred to as cybercrime. The U.S. Department of Justice broadens the definition of "cybercrime" to include any unlawful activity that records data on a

computer. Cybercrimes are crimes committed using processers, also with network intrusions and the distribution of viruses in the computers, as well as computer-based modifications of criminalities already committed, such as fraud identification, trolling, terrorism and, harassment that are now serious problems for both governments and people. Rai. P.(2025), she studies on Artificial Intelligence, how to help in smart business management, in which involved Machine Learning, and IoT Cyber Crimes can be divided into cyber threats, cyber-attacks, and vulnerabilities to enlighten the effects of these illegal activities.

Fig. 3. ***Types of Cyber Crimes***

4.2 Cyber Threats

For decades, there have been cyber security risks to utility assets. Cyber threats create when users with unauthorized access take benefit of weaknesses in cyber structures. Following are the examples of crimes that mainly target PCs network and service like-Malware, viruses, and denial-of-service.

Cyber Theft: To put it simply, it usually involves stealing assets or information online. It is also known as illegal access, and it refers to the act of altering crucial data while using a malicious script to breach network security or a computer system besides the approval or knowledge of the user. The majority of banks, Yahoo, Microsoft, and Amazon have all been targeted by such cyberattacks. Hacking, piracy, espionage, poisoning of DNS caches, and identity theft are some of the methods used by cybercriminals.

Cyber Vandalism: It refers to exploiting or damaging data, as opposed to theft or misusing it which indicates that computer systems have been stopped or interrupted. As a result, only official handlers are able to access the network's data.

Web Jacking: A web server is taken over forcibly when someone gains access to and control over another person's website. This practice is known as "web jacking." Hackers may be tampering with the website's data.

Stealing Cards Information: It helps in gaining access to an online store's server and using that information for malicious purposes.

Online Terrorism: A deliberate act of violence against civilians, usually motivated by politics, carried out using the internet or its resources.

Pornography: It utilizes shared drives on community networks to store, share, or access pornographic content that sexually exploits children and women.

Spam: It includes the violation of the SPAM Act, which occurs when spam is sent without permission by sending emails with immoral or illegal product advertisements.

4.3.Cyber Attacks

The impact of cyberattacks on vital infrastructure and data makes them a significant issue in the cyber world that requires attention. (Sur A, 2022) When someone maliciously gains access to a computer without authorization or makes an attempt at doing so, that is a cyber-attack to conduct scam, identity theft, phishing scams, and cyberstalking which are examples of systems or devices attacks that enable crimes but do not serve as the primary target of those crimes.

Untargeted Attacks: To take advantage of technologies like these, attackers randomly select multiple numbers of individuals and services as they can in order to find the services' or networks' vulnerabilities, such as,

Phishing: It refers to the practice of imposters sending emails to numerous users and requesting sensitive information, such as credit card numbers and passwords.

Water holing: Publishing a fake, dummy, or compromised website to steal user information from users who are visiting it.

Ransomware: This category of malware includes widely disseminated disc encryption extortion software.

Scanning: It is randomly attacking large portions of the Internet.

Fig. 4. ***Hacker Conducting Attacks***

Targeted Attacks: These attacks are specifically directed at a target, including attacks on the target users in the online world.

Spear-phishing: It is sending emails to specific people with links to malicious software and advertisements that could contain malicious software download links for establishing a honeypot. To disrupt the supply chain, it will start a distributed denial of service attack.

Vulnerabilities

Vulnerabilities are holes in the architecture or design of a system that permit outsiders to run a program, access personal data, and/or conduct denial-of-service attacks. Numerous locations can harbor system vulnerabilities. These flaws can be observed within the system's hardware or software, in the rules and procedures put in place to use it, or even in the system's users themselves.

The effort required to fix the vulnerability as well as hardware compatibility and interoperability were factors in its identification. Security flaws exist in operating systems, programs, and command software including communication channels and hardware drives. Software and human factors complexity are mainly two things that can results in defective design of software. In the many cases weaknesses of human lead to technical vulnerabilities.

4.4 Cases of Cyber Crime

In August 2022, Red Alpha, which is reportedly supported by the government of Chine allegedly take off the login pages of NIC (India's National Informatics Centre), which oversees the Indian government's larger IT infrastructure and services. The FIDH (International Federation for Human Rights), Amnesty International, the MERICS (Mercator Institute for China Studies), Radio Free Asia (RFA), the American Institute in Taiwan (AIT), and other global governmental, academic, and humanitarian organisations that operate within the tactical interests of the Chinese government were all impersonated by the China-sponsored hacking group. The group has also targeted specific individuals and organisations within the Tibetan and Uyghur communities directly, according to a statement by the cybersecurity firm Recorded Future.

On 7th June 2021, the personal information of approximately 4.5 million people was compromised by a **cyberattack on the Air India passenger service system**. When a breach involving the release of passenger personal data collected between August 26, 2011, and February 20, 2021, was discovered, Air India was made aware of it. The types of information exposed in the data breach included personal information of passengers, passport information, ticket information, regular flyer data from Star Alliance and Air India and credit card details, including the name of the cardholder, expiry, etc. The attacks got prevented later, but this incident attracted the attention of the government and people towards cybersecurity and awareness, after which cybersecurity was made compulsory.

Some of the major cybercrimes and breaches that drastically affected cyberspace in the past years are listed below,

In May 2021, the data of millions of customers who placed online food orders was compromised by a cyberattack on Domino's database.

In April 2020, during the COVID-19 pandemic, when a lot of users were using Zoom for official tasks, a data breach exposed the information of 5,000 users, and their login information was posted on the dark web.

In January 2021, the data breach, according to Microsoft, happened in January. The incident was caused by a modification to the database's network security group that included incorrectly configured security guidelines. The servers delimited about 250 million records by personal data, including email and IP addresses, IP and many other things.

In the year 2021, 268 million records were exposed as a result of the data breach. According to Bleeping Computer, the stolen information was then posted on various hacking-related forums. Usernames, email addresses, IP addresses, and crypt hashed passwords were among the personally identifiable information that was disclosed.

4.5 Cyber Security Issues and Awareness

The main plan of cybersecurity is to secure a network out of outside threats. It ensures that society will run reasonably and that people will feel secure handling their data.

Information theft can be prevented, workstations can be shielded from theft, PC freezing is decreased, operator privacy is maintained, strict guidelines are proposed, and non-technical people find it challenging to work with cybersecurity. It safeguards computers from worms, viruses, and other unwanted software and serves as the primary source of funding for computer security. Cybersecurity enhances Internet security, boosts cyber resilience, accelerates system performance, and provides information protection for businesses. In addition to defending against identity theft and hacker attacks, it also safeguards networks and resources.

Fig. 5. ***Use of Technology in the IT Industry***

The infrastructure of every business and organization must take cybersecurity seriously. In conclusion, a person, business, or organization that focuses on cybersecurity can succeed in a variety of ways and gain high status because doing so demonstrates the organization's ability to defend sensitive customer and private data from an adversary. To grow and establish itself, a person, business, or organization must first include this security. The use of practical cybersecurity precautions protects information, networks, and data against threats both internally and externally.

As a group of workstations or a network that is only loosely connected, cyber may be distinguished. Security is also the means by which anything is protected. Therefore, the terms "Cyber" and "security" were developed to define the technique of securing user information during or following hostile attacks that could disclose a security break. It is the period of time that was kept for a while after the internet ongoing developing inexorably. Cybersecurity is a benefit that allows any society or user to securing their important data from hackers. The functions of the three major security processes that is, discovery, examination, and remediation help in establishing a unified threat management system that automates improvements in security across specific Cisco Security products. People, processes, and technology are the main factors getting affected and that need to be focused on to ensure security ty the following manner as mentioned below,

People: Basic information security principles, such as choosing strong passwords, being cautious of attachments in email, and backing up data, must be understood and followed by consumers to help in implementing fundamental cybersecurity principles.

Processes: Our authorities need a plan for how to reply to successful and common cyberattacks with a trustworthy framework. It clarifies how to identify occurrences, organizational safeguard, recognize and address threats, and study from positive experiences.

Technology: The system security tools needed to protect people and organizations from cyberattacks are made possible by technology. Endpoint strategies, such as devices, mobiles, systems, routers and our cloud are the most targeted and are at a

higher risk level. Cutting-Edge firewalls, malware protection, DNS filters, and email security, antivirus tools, and outcomes are examples of shared technology used to secure these objects. Hence, it is essential to use technology with security.

Fig. 6. ***Factors Getting Affected in Cyberspace***

4.6 Aim of Cyber Security

Protecting information from being appropriated or intentionally compromised is the key goal of cybersecurity. In order to achieve this, we look at three key cybersecurity objectives.

- Providing data privacy.
- Data is accurate and unaltered.
- Only authorised users can obtain it.

Every organisation and the community follow the CIA standards when they connect a new appeal, create a record, or ensure access to information. All of these safekeeping areas are essential to ensure that the data is entirely safe. It may be incorrect to oversee just one policy because these are safety measures that all work together. The most comprehensive method to assess, select, and implement the appropriate safety measures to reduce risk is the CIA triad.

Confidentiality: Confirming that only approved users can access your compound data and ensuring that no information is revealed to unintended parties. In the event that your key is private and won't be revealed to anyone, this concessions confidentiality. The following helps in protecting the confidentiality

- Two- or multifactor verification
- Data encryption
- Biometric confirmation

Integrity: Confirm that all of your data is accurate, reliable, and does not change by any factor during the presentation. The following methods help in securing the integrity, No illegal person shall have access to the accounts, which can violate privacy. Therefore, there will be controls for machinist contact.

- Available backups that can return fast are required.
- Version controlling has to be close by to prove the change log.

Availability: Ensure that there won't be any contradiction of service or other parallel notices every time the operator requires a resource for a portion of statistics. It is necessary to have access to whole the evidence. The following methods help in securing the availability of the resource
Sorting the possessions into groups according to importance and rank. The most significant ones are always kept back in a secure location.

- Selecting the best security guard deployment policy for each threat.
- One-to-one care any breaches and controlling both data in motion and at rest.
- Reiterative upkeep and addressing any matters that might get up.
- Adjusting policies to switch risk based on earlier evaluations.

Fig. 7. ***Aim of Cyber Security***

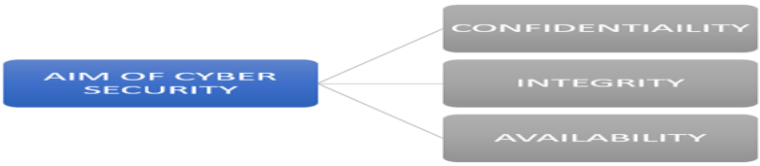

Figure 7: Cybersecurity professionals safeguard servers, networks, intranets, and computer systems. Cybersecurity makes sure that only authorised users can access that data. Below are cybersecurity techniques and countermeasures that can be used to protect users from cybercrimes.
Strong Password Security: The simplest way to increase the security of your system is to use a strong, complex password. Ensure that special characters, numbers, and letters are used in the password. It helps in preventing attacks by routine updates from being cracked by brute force.
Authentication of knowledge: Use caution when using the web and email because programmers (hackers) can abuse them in many different ways. An excellent way to ensure that your information is retrievable and to safeguard and correct any bugs or system flaws is to keep your system up to date and implement a regular backup schedule.
Malware scanners: Use programs that observe all files on a device for hostile code and viruses. Hostile software is devoted to as malware and includes such examples as Trojan horses, worms, and viruses.
Firewalls: They are pieces of software and hardware that assist in preventing viruses, hackers, and worms from infiltrating your device via the internet. The firewall, which is active and examines all messages coming into or going out of the web, blocks any that don't meet the necessary safety standards.
Antivirus Software: To guard your PC network against viruses, installing antivirus software is a crucial step. It carefully checks your emails and system files for viruses

that could infect your operating system. A good antivirus program incorporates regular updates and should be compatible with the system.
Each person has a different level of cyber security awareness, which can be low, medium, or high. Since information technology has undergone a such drastic change in recent years, it become important to emphasize spreading cyber security awareness amongst the people and organizations to ensure security in cyberspace.

Fig. 8. ***Cyber Crime is Cognizable Offence that Leads to Imprisonment***

In today's time where cybercrime is increasing rapidly, some laws have been made regarding cyber crime in India using which people can take action against crime if it is committed. Some of the major laws that come under the Information Technology Act 2000 are mentioned below in the table,

Table 1. CYBER CRIME LAWS

Section	Section Title	Punishment	Cognizable / Non-Cognizable	Bailable/Non-Bailable
43	Compensation and penalty for damage computer, computer system, etc.	Imprisonment – 3 years/Fine – 1 Crore	Non-Cognizable	Bailable
65	Tampering with computer source document	Imprisonment – 3 years/ Fine – 2 Lakhs/both	Cognizable	Non-Bailable
66	Hacking with computer system	Imprisonment – 3 years/Fine – 2 Lakhs/both	Cognizable	Non-Bailable
67	Publishing or transmission of information that is observed in electronic form	Imprisonment – 5/10 years/Fine – 1/2 Lakhs	Cognizable	Non-Bailable
68	Failure of compliance of CA or its employees of orders of CCA	Imprisonment – 3 years/ Fine – 2 Lakhs/both	Cognizable	Non-Bailable

69	Failure of any person to assist any government agency which is intercepting any information transmitted through any resource to decrypt the information	Imprisonment – 7 years	Cognizable	Non-Bailable
70	Access or attempt to access by any unauthorized person, A protected computer system as notified by the government in the official gazette	Imprisonment – 10 years and Fine	Cognizable	Bailable
71	Penalty for misrepresentation of material fact from the CCA for obtaining license or DSC as the case may be	Imprisonment – 3 years/ Fine – 2 Lakhs/both	Non-Cognizable	Bailable
72	Breach of confidentiality and privacy	Imprisonment – 2 years/ Fine – 1 Lakh/both	Non-Cognizable	Bailable
73	Publishing DSC which is false in certain particulars	Imprisonment – 2 years/ Fine – 1 Lakh/both	Non-Cognizable	Bailable
74	Publishing DSC for fraudulent purposes	Imprisonment – 2 years/ Fine – 1 Lakh/both	Non-Cognizable	Bailable

On the internet, it refers to the code. Try not to do anything online that you would consider wrong or illegal is the fundamental rule. Some of the important **cyber morals and ethics** to keep in mind while using the Internet are listed below,

Make use of social media to communicate with others digital platform. Providing facilities to connect with friends, family, and colleagues is made easier by electronic mail and texting. Providing inputs for fresh ideas, information, and understanding with people locally or internationally. Never use an unencrypted network, including unencrypted mail, to transfer or share sensitive information like your bank account

number, password, ATM pin, or other specifics. Ensure that checking the browser's address bar indicates decoded websites by the absence of the lock icon and HTTPS.
Do not sign up for a social networking site or platform unless you are certain that it is authentic and real.
Always remember to update and refresh the operating system. One should install and keep their PCs updated with software like firewalls, antivirus, and anti-spyware programs.
On e-commerce websites or any other website, never click on pop-ups that offer site surveys or studies because they sometimes contain malicious software. Drive-by downloading, which occurs when we acknowledge or click pop-ups, is the process of downloading a file in the background that contains malware and malicious code.
Always keep hold of copyrighted data, and only download legal games or recordings.
Never try to corrupt someone else's PC by sending them any kind of malware.
Avoid using a false name or creating accounts under someone else's name because doing so could get you both in trouble. Trends and Challenges in Green Computing, written by Rai. P. 2023, in the book chapter, mentions the advantages of green computing in human life.

5. Conclusion

The importance of the security of computers is growing reason behind\the world's growing interconnectedness and the reliance on networks for essential commercial transactions. Information security is not an exception to the fact that cybercrime keeps evolving with each passing year. Cybersecurity, cyber law, and cyber awareness play an important role in securing us in cyberspace. Cyber awareness is necessary for us to utilize the internet safely and with the consciousness of our behavior, which is essential for our online security. Despite the lack of a perfect solution, we must do everything within our power to lessen cybercrimes to confirm the safety and security of the future of cyberspace. M. Gupta (2024). They are well written in the paper on how the digital payment system and financial inclusion involve mobile wallets and digital currency, and net banking services. As per this study, we need to be more aware of cyber fraud and keep proper information about cybersecurity, which helps to protect users.

References

1. Sheth A, Bhosale S, and Kurupkar F, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, science/article/pii/S2352484721007289, November 2021.
2. Rai P. et al 2023, Brand Presence on Internet media: Quantitative and Qualitative Study on Brand Attitude and Brand Attachment, EAI Endorsed Transactions on Scalable Information Systems Online First, published on 29 December 2023, P. N. 1-8, doi: 10.4108/eetsis.4724.
3. Vallarelli N,2020 Cyber Security's Influence on Modern Society, cgi/viewcontent.cgi?article=1312&context=honorscollege_theses, May 2020.
4. Parikh T.P. Patel A.P., 2017, Cyber security: Study on Attack, Threat, Vulnerability, IJRMEET_2017_vol05_issue_06_01.pdf, June 2017.

5. Singh A, A Study on Emerging Issues of Cyber Attacks & Security: In India,dia_ijariie13501.pdf, Jan 2021.
6. The Information Technology Act, 2000, /handle/123456789/1999.
7. Kumar S, Athavale V. A. and Kartikey D., Security Issues in Cloud Computing: A holistic view Security-Issues-in-Cloud-Computing-A-holistic-view.pdf, September 2021.
8. Gupta M, Gupta D. and Rai P. 2023, Exploring the Impact of Software as a Service (SaaS) on Human Life, EAI Endorsed Transactions on Internet of Things | Volume 10 | 2024 | P. N. 1-12 published on 11 January 2024, doi: 10.4108/eetiot.482.
9. Rai. P., Velmurugan P (2025), In book: Artificial Intelligence, Machine Learning and IoT for Smart Business Management, published 2025, CRC Press, DOI:10.1201/9781003561873-2
10. Air India Notification of Data Breach, /images/pdf/Air-India-Notification-of-Data-Breach-Update-For-Australian-Customers.pdf, June 2021.
11. Sur A, China-backed hackers targeted India's NIC among others: Report, /news/business/china-backed-hackers-targeted-indias-nic-among-others-report-9070791.html, 22 August 2022.
12. Gupta, M., Gupta, D., Rai, P. (2024). Digital Payment Systems and Financial Inclusion: Examine How Digital Payment Systems, Such as Mobile Wallets and Digital Currencies, Can Improve Financial Inclusion by Providing Access to Banking Services for the Unbanked and Underbanked Population. Third International Conference on Computing and Communication Networks. ICCCN 2023. Lecture Notes in Networks and Systems, vol 917. Springer, Singapore. https://doi.org/10.1007/978-981-97-0892-5_57
13. China-backed hackers spying on govts; India's NIC among victims China's Involvement in India's Internal Security Threats: An Analytical Appraisal.
14. Rai *P.,* Rawat Y (2023)Trends and Challenges in Green Computing BookSustainable Digital Technologies Edition1st Edition, First Published2023, ImprintCRC Press, Pages 26, eBook ISBN9781003348313.
15. Reddy N.G, Reddy G.J, A Study Of Cyber Security Challenges and Its Emerging Trends On Latest TechnologiesFtp/Arxiv/Papers/1402/1402. 1842.Pdf.
16. Shehani H, Weerasuriya R and Fernando M Cyber Security- Research paper, 45631453.
17. Zheng M, Zimo H R, Thapa C. P., Moore T. Cybersecurity Research Datasets: Taxonomy and Empirical Analysis, system/files/conference/cset18/cset18-paper-zheng.pdf.