A Study of Cyber Security Difficulties and the Rising Trends in Related To New Technologies

Patel Mahima Rambali[1] Nadigottu Lavanya Lingaiah[2]
[1,2]G.M Momin Women's Collage, Bhiwandi, Maharashtra, India

Abstract— Cybersecurity is the practice of securing critical systems and sensitive data from digital attacks. Cybersecurity measures, also known as information technology (IT) security, are intended to combat threats to networked systems and applications, whether they originate within or outside of an organization. Cyber security refers to the technologies and processes that are designed to protect computers, networks, and data from unauthorized access and cybercriminal attacks delivered via the internet. Through, cyber security is the important for the network, data and application security. Cyber Security is critical in the field of information technology. Today, one of the most difficult challenges is securing information. When we think of cyber security, the first thing that comes to mind is 'cyber crimes' which are increasing at an alarming rate. With the increase in cyber-attacks, every organization requires a security analyst to ensure the security of their system. These security analysts face numerous cybersecurity challenges, such as protecting government organizations confidential data, securing private organization servers, and so on. We have some cyber security challenges like Ransomware Attacks: Ransomware is the biggest concern now in the digital world. IoT Attacks (Internet of Things): The Internet of Things or IoT is the most vulnerable to data security threats. Cloud Attacks, Phishing Attacks, Cryptocurrency and Blockchain Attacks. Cyber security is the prevention of cyber-attacks on internet-connected systems, including hardware, software, and data. We have some advantages of cyber security: 1) It will protect us from hackers and viruses. It enables us to navigate a secure website. 2) All incoming and outgoing traffic on our computer is processed. 3) The cyber security developers will update their database once a week, so new viruses will be detected. 4) Every week, we must update the cyber security application on our computer. Various governments and businesses are taking numerous steps to combat cybercrime. Aside from various measures, many people are still concerned about cyber security. The Central Government has taken steps to raise awareness about cybercrime, such as issuing alerts/advisories, building capacity/training for law enforcement personnel/prosecutors/judicial officers, and improving cyber forensic facilities. This paper focuses on the latest technological challenges in cyber security. It also focuses on the most recent cyber security techniques, ethics, and trends that are changing the face of cyber security.

Keywords: Cyber Security Difficulties, New Technologies

I. INTRODUCTION

Cyber Security is critical in the field of information technology. Today, man can send and receive any type of data, whether it is an e-mail or an audio or video file, with the click of a button, but has he ever considered how securely his data is being transmitted or sent to the other person safely without any leakage of information?? The solution is found in cyber security.

The Internet is now the fastest growing infrastructure in daily life. Many new technologies are changing the face of humanity in today's technological environment. However, because of these emerging technologies, we are unable to effectively protect our private information, and as a result, cybercrime is on the rise. Because commercial transactions are now conducted online, this field necessitated a high level of security to ensure transparent and efficient transactions. As a result, cyber security has emerged as a hot topic. The scope of cyber security extends beyond securing information in the IT industry to various other fields such as cyber space, etc.

Even cutting-edge technologies like cloud computing, mobile computing, E-commerce, and internet banking require a high level of security. Because these technologies contain sensitive information about a person, their security has become critical. Improving cyber security and safeguarding critical information infrastructure are critical to each country's security and economic well-being. Making the Internet safer (and protecting Internet users) has become an essential component of both the development of new services and government policy. The fight against cybercrime requires a more comprehensive and secure approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies have the ability to effectively investigate and prosecute cybercrime. Many nations and governments are now enforcing stringent cyber security laws in order to prevent the loss of critical information. Every individual must be trained in cyber security in order to protect themselves from the growing number of cyber-crimes.

II. CYBER CRIME

A cybercrime is a crime committed with the use of a computer. The computer could have been used in the crime or it could be the target. Cybercrime can jeopardize someone's security or financial well-being. When confidential information is intercepted or disclosed, whether lawfully or illegally, there are numerous privacy concerns.

Any illegal activity that uses a computer as its primary means of commission and theft is referred to as cyber-crime. The United States Department of Justice broadens the definition of cybercrime to include any illegal activity that makes use of a computer to store evidence. The growing list of cyber-crimes includes crimes made possible by computers, such as network intrusions and the spread of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying, and terrorism, all of which have become major issues for individuals and nations. In layman's terms, cybercrime is defined as a crime committed by using a computer and the internet to steal a person's identity, sell contraband, stalk victims, or disrupt operations with malicious software. As technology continues to play an increasingly important role in people's lives, cybercrime will increase in tandem.

III. CYBER SECURITY:

Data privacy and security will always be top security priorities for any organization. Cybersecurity is the practice of guarding against digital attacks on systems, networks, and programs. These cyberattacks are typically intended to gain access to, change, or destroy sensitive information; extort money from users; or disrupt normal business processes. Implementing effective cybersecurity measures is especially difficult today due to the fact that there are more devices than people, and attackers are becoming more creative. We currently live in a world where all information is stored digitally or in cyberspace. Social networking sites provide a safe environment for users to interact with friends and family. Social networking sites provide a safe environment for users to interact with friends and family. Cybercriminals would continue to target social networking sites to obtain personal data from home users. Not only during social networking, but also during financial transactions, a person must take all necessary security precautions.

Cyber security incidents have more than quadrupled in the last two years, nearly tripling between January and August of this year (compared to year 2019). According to official data, such incidences more than quadrupled in 2018 and increased by 89% last year. According to data compiled by the Indian Computer Emergency Response Team (CERT-In), 3.9 lakh cyber security incidents were reported in 2019, with the figure expected to rise to nearly 7 lakh by August 2020, according to a Lok Sabha reply by Sanjay Dhotre, Minister of State for Electronics and Information Technology.

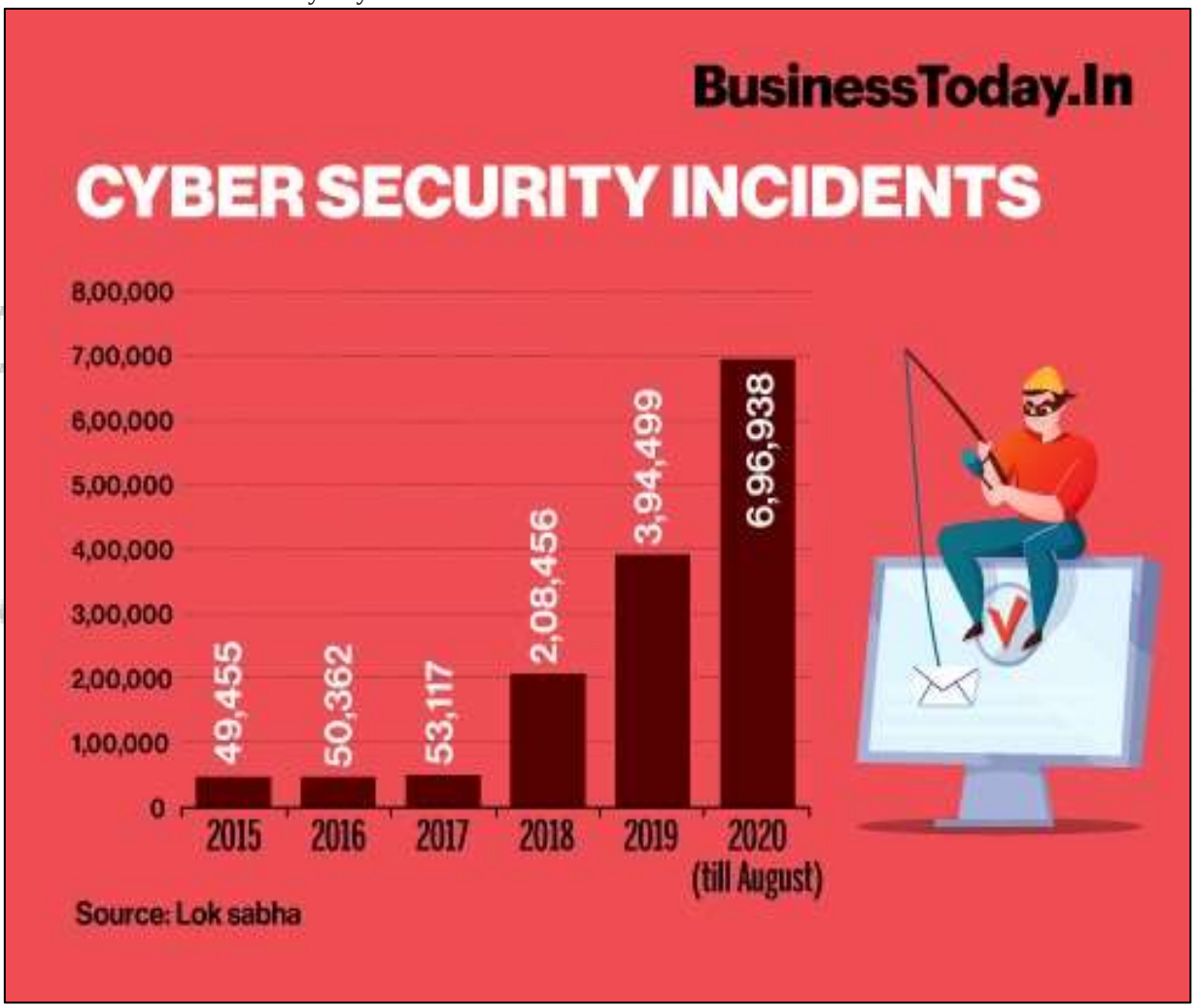

Fig. 1:

According to Siddharth Vishwanath, Partner - Cyber Advisory Leader at PwC, there has been an uptick in cyber security events recently. People are connecting from faraway regions, sometimes using their own devices, which has created several chances for hackers to become more active. The Indian government has made a number of steps to improve cyber security and avoid cyber-attacks. These include sending out regular notifications and advisories about the most recent cyber risks via CERT-In, conducting cyber security drills, and developing a Cyber Crisis Management Plan to combat cyber assaults and cyber terrorism.

There will be new assaults against Android-based devices, but they will be limited in scope. Because tablets and smartphones use the same operating system, they will be targeted by the same malware in the near future. The quantity of malware specimens for Macs would continue to rise, but far more slowly than for PCs. Because Windows 8 will allow users to construct programs for nearly any device (PCs, tablets, and smart phones) running Windows 8, harmful applications similar to those for Android will be feasible; hence, these are some of the projected cyber security trends.

IV. TRENDS CHANGING CYBER SECURITY:

Here mentioned below are some of the trends that are having a huge impact on cyber security:

A. Web Servers

A web server is computer software and underlying hardware that accepts requests via HTTP or its secure variant HTTPS. A user agent, commonly a web browser, initiates communication by making a request for a web page using HTTP, and the server responds with the content of that resource. A web server can also accept and store resources sent from the user agent if configured to do so.[1] [2] The hardware used to run a web server can vary according to the volume of requests that it needs to handle.

The potential of web application assaults to harvest data or deliver harmful code remains. Cybercriminals deploy harmful malware using genuine web servers that they have hacked. However, data-stealing assaults, many of which garner public attention, pose a significant hazard. Now, we need a greater emphasis on securing web servers and web applications. Web servers are the ideal platform for these cyber thieves to collect data. As a result, in order to avoid being a victim of these crimes, one should constantly use a safer browser, especially during critical transactions.

B. Cloud Computing and It's Services

Simply described, cloud computing is the transmission of computer services such as servers, storage, databases, networking, software, analytics, and intelligence via the Internet ("the cloud") in order to provide faster innovation, more flexible resources, and economies of scale. The technique of storing, managing, and processing data on a network of distant servers housed on the internet rather than a local server or a personal computer.

Cloud services are being gradually used by all small, medium, and large businesses these days. In other words, the planet is gradually approaching the clouds. This current trend poses a significant problem for cyber security since communications can bypass established sites of inspection.

Furthermore, as the number of cloud-based apps rises, policy controls for web applications and cloud services will need to adapt in order to prevent the loss of vital data. Even while cloud services are building their own models, several concerns have been raised concerning their security. Although the cloud offers several advantages, it should be emphasised that as the cloud grows, so do its security issues.

C. APT'S and Targeted Attacks

APT (Advanced Persistent Threat) is a completely new level of cybercrime software. For years, network security features such as web filtering or intrusion prevention systems (IPS) have played an important role in detecting such targeted assaults (usually after the initial penetration). As attackers get more daring and deploy more evasive strategies, network security must connect with other security services to identify assaults.

As a result, we must strengthen our security measures in order to prevent future threats.

D. Mobile Networks

Today, we can communicate with anyone, anywhere in the globe. However, security is a major worry for these mobile networks. Firewalls and other security protections are growing more permeable as people utilise devices such as tablets, phones, PCs, and so on, all of which require additional safeguards in addition to those provided by the programmers used. We must continuously consider the security of these mobile networks. Furthermore, because mobile networks are so vulnerable to cybercrime, extreme caution must be exercised in the event of a security breach.

E. IPv6: New Internet Protocol

IPv6 is the most current Internet Protocol version (IP). It is intended to provide IP addressing and enhanced security to enable the anticipated expansion of linked devices in IoT, manufacturing, and new fields such as autonomous driving. IPv6 is the new Internet protocol that is replacing IPv4 (the previous version), which has served as the backbone of our networks and the Internet in general. It is not enough to just port IPv4 capabilities to protect IPv6.

While IPv6 is a complete replacement in terms of increasing the number of accessible IP addresses, there are certain basic modifications to the protocol that must be addressed in security policy. As a result, it is always preferable to convert to IPv6 as soon as feasible in order to avoid the dangers associated with cybercrime.

F. A.6 Encryption of the Code

Encryption is the technique of encrypting communications (or information) in such a way that it cannot be read by eavesdroppers or hackers. An encryption technique encrypts a message or information using an encryption algorithm, resulting in unreadable cypher text. This is normally accomplished through the use of an encryption key, which defines how the message should be encoded. Encryption safeguards data privacy and integrity from the start. However, increased encryption use creates new issues in cyber security. Encryption is also used to safeguard data in transit, such as data exchanged across networks (such as the Internet or ecommerce), mobile phones, wireless microphones, wireless intercoms, and so on. As a result, by encrypting the code, one may determine whether or not there is any leakage of information.

Hence the above are some of the trends changing the face of cyber security in the world. The top network threats are mentioned in below Fig -2.

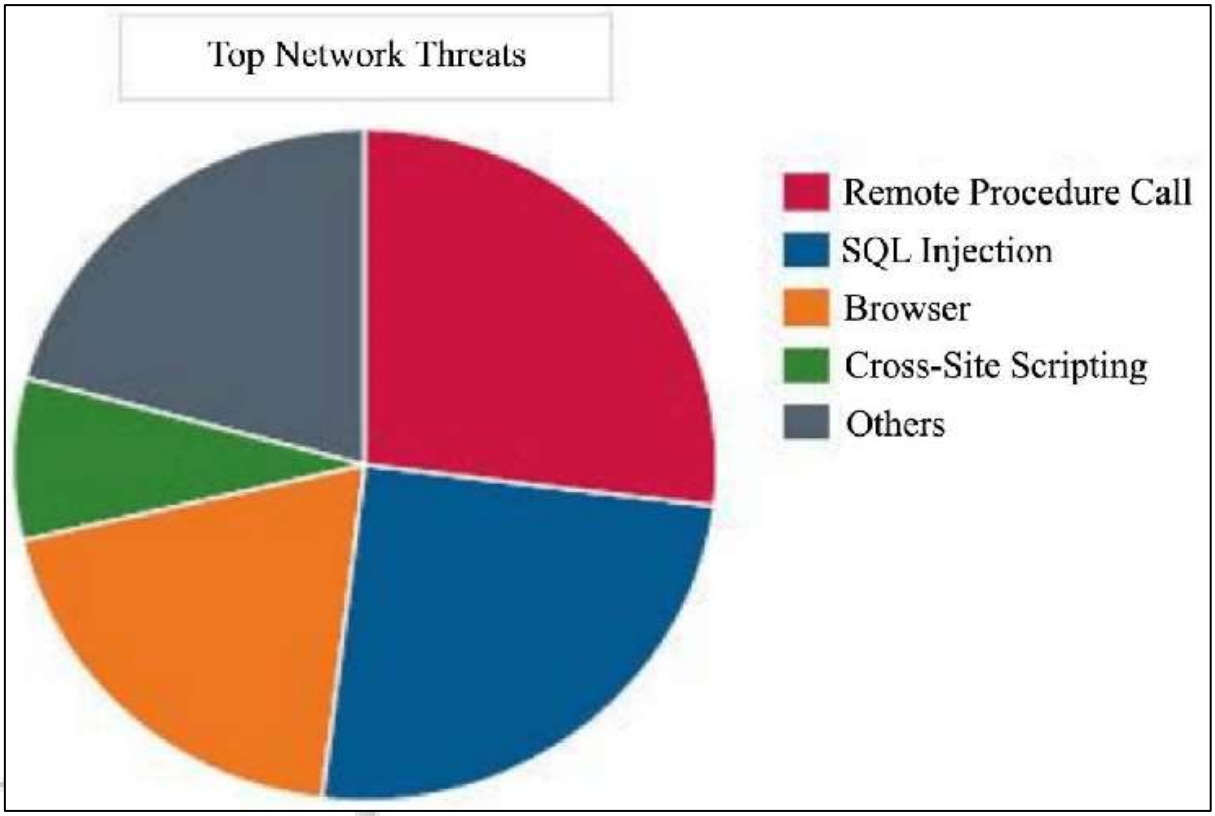

Fig. 2:

The above pie chart shows about the major threats for networks and cyber security.

V. Role of Social Media and in Cyber Security:

Companies must develop innovative methods to secure personal information as we become more social in an increasingly connected world. Social media has a significant role in cyber security and will contribute significantly to personal cyber dangers. The use of social media among troops is increasing, as is the possibility of an assault. Because most people use social media or social networking sites every day, it has become a large platform for cyber criminals to breach private information and steal important data.

Companies must guarantee that they are equally as rapid in spotting risks, responding in real time, and preventing any type of breach in a world where we are eager to give over our personal information. Because users are readily drawn to these social media platforms, hackers exploit them as bait to obtain the information and data they seek. As a result, users must take proper precautions, particularly while engaging with social media, to avoid data loss.

Individuals' power to share knowledge with an audience of millions is at the heart of the unique challenge that social media provides to corporations. In addition to granting anybody the ability to broadcast economically sensitive information, social media also grants the same ability to transmit incorrect information, which may be equally devastating. One of the rising threats listed in the Global Risks 2013 report is the fast spread of incorrect information via social media.

Though social media might be exploited for cybercrime, these organizations cannot afford to cease utilizing it because it is vital for brand PR. Instead, they need solutions that will alert them to the problem so that they can solve it before any serious damage is done. Companies, on the other hand, should comprehend this and recognize the value of analyzing information, particularly in social discussions, and give suitable security solutions to avoid hazards. Certain regulations and technology must be used to manage social media.

VI. Cyber Security Techniques

A. Access Control and Password Security

The notion of a user name and password has been a key method of securing personal data. This might be one of the earliest cyber security measures.

B. Authentication of Data

Before downloading, the papers we receive must always be validated, which means they must have come from a reputable and credible source and have not been altered. The anti-virus software installed on the devices often authenticates these documents. As a result, robust anti-virus software is also required to safeguard the devices from infections.

C. Malware Scanners

This is software that searches all of the files and documents in the system for malicious code or viruses. Malicious software such as viruses, worms, and Trojan horses is commonly lumped together and referred to as malware.

D. Firewalls

A firewall is a piece of software or hardware that helps to filter out hackers, viruses, and worms that try to connect to

your computer via the Internet. All messages entering or leaving the internet are routed through the firewall, which inspects each message and bans those that do not fit the established security standards. 0As a result, firewalls are critical in detecting malware.

E. Anti-Virus Software

Antivirus software is a computer application that detects, stops, and responds to dangerous software programs such as viruses and worms. Most antivirus products contain an auto-update capability that allows the program to download updated virus profiles so that it can detect new viruses as soon as they are detected. Anti-virus software is a needed and a basic requirement for each system.

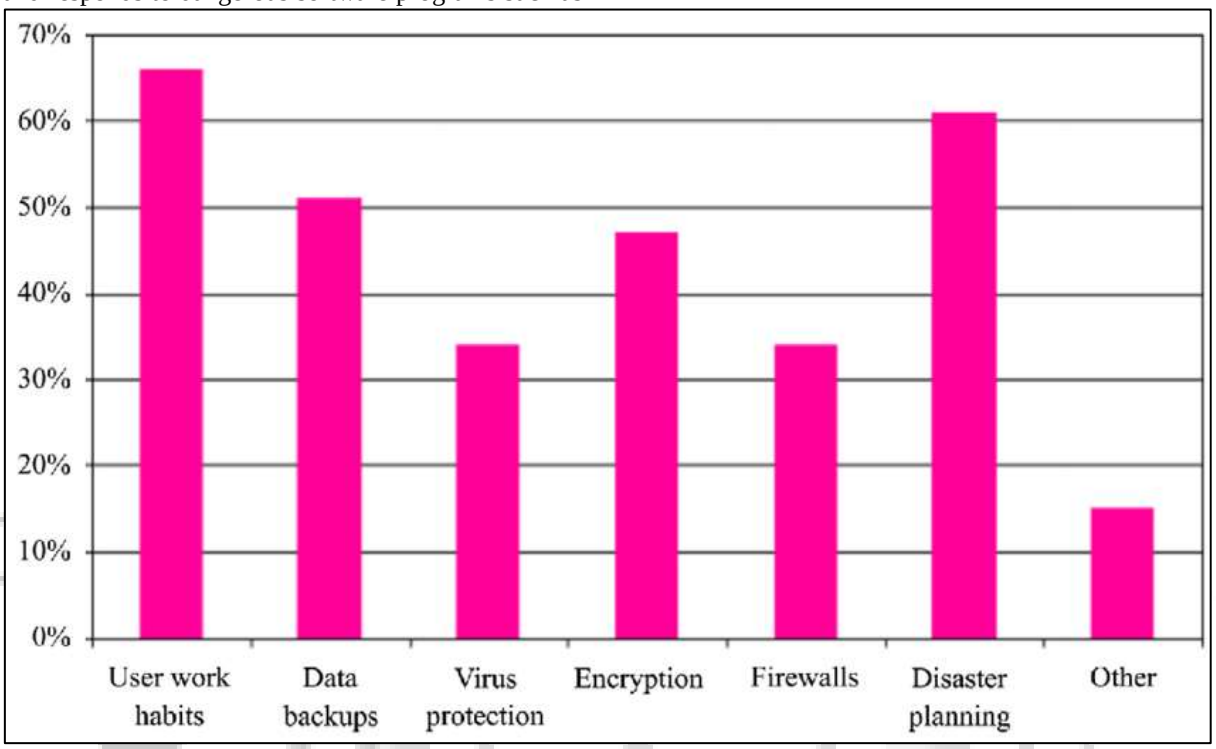

Fig. 3: Techniques in cyber security

VII. CYBER ETHICS:

Cyber ethics are simply the rules of the internet. When we adopt these cyber ethics, we have a better chance of utilizing the internet properly and safely. Here are a few examples:

- DO make use of the Internet to communicate and interact with others. Email and instant messaging make it simple to interact with friends and family, stay in contact with co-workers, and share ideas and information with folks across town or halfway around the world.
- On the Internet, don't be a bully. Do not call individuals names, tell lies about them, email them embarrassing images, or do anything else to injure them.
- Because the Internet is regarded as the world's largest library, containing information on every topic in any subject area, accessing this material in a correct and legal manner is always necessary.
- Do not operate others accounts using their passwords
- Never attempt to corrupt other people's systems by sending malware.
- Never give out your personal information to anyone since there is a good probability that people will misuse it and you will end yourself in trouble.
- When you're online, never pretend to the other person and never try to create a phony account on someone else's behalf since it will get you and the other person in trouble.
- Always respect copyrighted information and only download games or videos if they are legal.

The following are some cyber ethics to keep in mind when using the internet. We have always thought about correct rules from the beginning, and the same is true in cyberspace.

VIII. CONCLUSION:

Computer security is a broad topic that is growing increasingly vital as the world becomes more interconnected, with networks utilized to carry out critical transactions. With each New Year that passes, cybercrime continues to take diverse pathways, as does information security. The most recent and disruptive technologies, as well as new cyber tools and threats that emerge on a daily basis, are presenting businesses with new challenges in terms of not just securing their infrastructure, but also requiring new platforms and intelligence to do so. There is no ideal answer to cybercrime, but we should do all possible to reduce them in order to have a safe and secure future in cyberspace.

REFERENCES:

[1] A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
[2] Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole.
[3] Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
[4] A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
[5] International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry.
[6] IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
[7] CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.
[8] https://www.ibm.com/in-en/topics/cybersecurity.
[9] https://www.javatpoint.com/cyber-security-challenges.
[10] https://www.google.com/search?q=how+the+government+taken+various+action+on+cyber+security+crimes&client=avast-a-1&ei=meaJY9CPJ9qW4EP0Zqx0Ag&ved=0ahUKEwiQwLeX79r7AhVayzgGHVFNDIoQ4dUDCBA&uact=5&oq=how+the+government+taken+various+action+on+cyber+security+crimes&gs_lcp=Cgxnd3Mtd2l6LXNlcnAQAzoKCAAQRxDWBBCwAzoFCAAQgAQ6BAgAEEM6BggAEBYQHjoICAAQgAQQsQM6BQguEIAEOgsIABCABBCxAxCDAToHCAAQgAQQDToKCAAQgAQQsQMQDToGCAAQBxAeOggIABAIEAcQHjoKCAAQCBAHEB4QDzoICAAQCBAeEA86BggAEAgQHjoECCEQCjoFCAAQogQ6BwgAEB4QogQ6CgghEMMEEAoQoAE6CAghEMMEEKABOgcIIRCgARAKSgQIQRgASgQIRhgAUKUdWPavB2DfqQhoA3ABeACAAbECiHXpIBCTAuNTUuMTYuMZgBAKABAcgBCMABAQ&sclient=gws-wiz-serp.
[11] https://en.wikipedia.org/wiki/Cybercrime.
[12] https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html.
[13] https://www.businesstoday.in/technology/news/story/cyber-security-incidents-double-till-august-this-year-273707-2020-09-23.
[14] https://en.wikipedia.org/wiki/Web_server. 1.*Nancy J. Yeager; Robert E. McGrath (1996). Web Server Technology. ISBN 1-55860-376-X. Retrieved 22 January 2021.* 2.^ *William Nelson; Arvind Srinivasan; Murthy Chintalapati (2009). Sun Web Server: The Essential Guide. ISBN 978-0-13-712892-1. Retrieved 14*
[15] https://www.google.com/search?client=avast-a-1&q=CLOUD+COMPUTING&oq=CLOUD+COMPUTING&aqs=avast..69i57j0l6j69i61.8914j0j1&ie=UTF-8.
[16] https://www.cisco.com/c/en/us/solutions/ipv6/overview.html.

