iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.47844

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XII Dec 2022- Available at www.ijraset.com

Cyber Security Challenges with Latest Technologies

Aman Kumar[1], Anand Pandey[2], Ashutosh Sangam[3], Manjot Kaur Bhatia[4]
[1, 2, 3, 4] *Jagan Institute of Management Studies, Rohini Sector-5, New Delhi*

Abstract: ***A crucial element of information technology is cyber security. Cyber security is the process of defending sensitive information and crucial systems against online assaults. When we think of cyber security, the first thing that comes to mind is cybercrimes, which are on the rise every day. Governments and other businesses are taking a lot of measures to stop these cybercrimes. Maintaining cyber security continues to be a very challenging task for us despite many attempts.***

I. INTRODUCTION

Internet usage is currently the most common form of infrastructure. Many modern technologies are changing the way people look in today's world. But because of these new technologies, we are unable to effectively protect our private information, which is why cybercrime is on the rise right now. Today, more than 70% of transactions take place online; hence this industry needed robust security for open and honest dealings. Even the most cutting-edge technology, such as cloud computing, online shopping, net banking, etc., require a high level of security. Since these technologies contain some of a person's most important information, their security has become essential. Each country's security and economic growth depend on improving cyber security and safeguarding vital information infrastructure. It is now crucial for both the creation of new services and public policy that the Internet be made safer (and users of the Internet are protected). A thorough and safer strategy is required to combat cybercrime. In order to avoid the loss of critical information, many countries and governments today have severe rules against cybercrime. Everyone must receive training in cyber security so they can defend themselves against online crimes.

II. CYBER CRIME

Cybercrime is any illicit conduct involving a computer, network, or other networked device. While the majority of cybercrimes are committed to make money for the perpetrators, others are committed against computers or other technology to cause financial or psychological harm to the target.

III. CYBER SECURITY

The process of defending our systems and sensitive data against online threats is known as cyber security. Cyber security is intended to counter attacks against networked systems and applications from both inside and outside of a business.

IV. TRENDS CHANGING CYBER SECURITY

Some of the trends that are significantly affecting cyber security are listed below.

1) *Web Servers:* Attacks to harvest data or spread harmful code are still a possibility against web applications. Through genuine web servers they have infiltrated, cybercriminals disseminate their malicious code. However, attacks that steal data also pose a serious threat and are frequently reported in the media. The protection of web servers and web applications must now take center stage. Web servers provide these thieves with very effective platforms for data theft. In order to avoid becoming a victim of these scams, one must constantly use a safer browser, especially during critical transactions.
2) *Cloud Computing And Its Services:* These days, all small, medium-sized, and large businesses are gradually embracing cloud services. In other words, the earth is gradually encroaching upon the clouds. This most recent trend is problematic for cyber security since it allows traffic to avoid traditional ports of inspection. With an expansion in the number of cloud-based apps, policy controls for web applications and cloud services will also need to adapt in order to prevent the loss of crucial data. Security issues are always a top worry, even though cloud providers are developing their own models. Although the cloud may offer tremendous benefits, it is important to remember that as the cloud develops, security problems also do.
3) *APTS And Targeted Attacks:* An entirely new class of cybercrime software is known as an APT (Advanced Persistent Threat).

For years, network security tools like web filtering and intrusion prevention systems (IPS) have been crucial in spotting such targeted attacks (mostly after the initial compromise). As attackers grow more daring and employ shadier strategies, network security must collaborate with other security services to identify attacks. Therefore, we must enhance our security measures to stop new risks from emerging in the future.

4) *Mobile Networks:* We can now communicate with anyone, anywhere in the world. Security, however, is a very serious worry for these mobile networks. As more people utilize devices like tablets, phones, PCs, and other such devices—all of which again require additional security protections beyond those included in the applications used—firewalls and other security mechanisms are becoming permeable. We must always consider how secure these mobile networks are. Additionally, mobile networks are quite vulnerable to these cybercrimes, thus extreme caution must be used in the event of any security difficulties.
5) *IPv6: New internet protocol:* The new Internet protocol, IPv6, is replacing IPv4 (the previous version), which served as the foundation of both our networks and the Internet as a whole. It takes more than simply migrating IPv4 capabilities to protect IPv6. While IPv6 is a complete replacement that increases the number of available IP addresses, there are several very basic modifications to the protocol that will greatly increase the risk of personal cyber threats. The use of social media by employees is surging, just like the attack threat. Since the majority of people use social media or social networking sites virtually daily, it has developed into a significant platform for cybercriminals to get into personal data and steal vital information.

V. COMMON CYBER THREATS

Although cyber security experts put a lot of effort into closing security gaps, attackers are constantly looking for novel ways to avoid IT detection, get around defenses, and take advantage of developing weaknesses. The most recent cyber security risks are reinventing "existing" risks by utilizing work-from-home settings, remote access technologies, and new cloud services. Among these rising threats are:

A. Malware

Malicious software that gives unauthorised access to or harms a computer, such as worms, viruses, Trojan horses, and spyware, is referred to as "malware." Attacks by malware are becoming more "fileless" and are made to avoid common detection techniques, including antivirus software that checks for harmful file attachments.

B. Ransomware

Ransomware is a sort of virus that encrypts files, data, or systems and demands a ransom payment from the cybercriminals who attacked the system in order to unlock it. If the ransom is not paid, the data may be erased, destroyed, or made public. State and local governments have been the target of recent ransomware attacks because they are easier to hack than organizations and are under pressure to pay ransoms in order to restore the websites and programmes that citizens depend on.

C. Phishing / Social Engineering

Phishing, a form of social engineering, is the activity of deceiving users into divulging their own PII or sensitive information. In phishing scams, emails or text messages that seem to be from a reliable company seek for private information, including login credentials or credit card information. The rise of remote employment has been linked to an increase in pandemic-related phishing, according to the FBI.

D. Insider Threats

If they misuse their access privileges, current or former employees, business partners, contractors, or anybody else who has accessed systems or networks in the past can be regarded as an insider threat. Traditional security measures that concentrate on external threats, such as firewalls and intrusion detection systems, may not be able to detect insider threats.

E. Distributed Denial-Of-Service (DDOS) Attacks

DDoS assaults often involve flooding a server, website, or network with traffic from numerous synchronised systems in an effort to bring them down.

DDoS assaults bring down enterprise networks by using the simple network management protocol (SNMP), which is utilised by modems, printers, switches, routers, and servers.

F. Advanced Persistent Threats (APTS)

APTs happen when a hacker or group of hackers compromises a system and goes for a long period of time without being discovered. The invader ignores networks and systems in order to monitor business activity and gather crucial data without activating defensive countermeasures. The most recent Solar Winds intrusion into US federal networks serves as an example of an APT.

G. Man-In-The-Middle Attacks

An eavesdropping technique known as "man-in-the-middle" involves a cybercriminal intercepting and relaying messages between two parties in order to steal data. An attacker may, for instance, collect data passing between a visitor's device and an insecure Wi-Fi network.

VI. CYBER SECURITY TECHNIQUES

1) *Access Control And Password Security:* The user ID and password are a fundamental method of safeguarding our information. This is the initial step in implementing cyber security.
2) *Authentication of Data:* Before downloading a document, we must always verify that it came from a reputable and trustworthy website. Anti-virus software checks these documents for viruses. So, protecting the gadgets from viruses also requires having strong anti-virus software.
3) *Malware Scanners:* This software scans all the papers and files on the computer to look for viruses and malicious code. Malicious software, also referred to as malware, includes things like viruses, worms, and Trojan horses.
4) *Firewalls:* A firewall is a piece of hardware or software that aids in blocking hackers, viruses, and worms from trying to access your computer through the Internet. Every message sent or received must travel through the firewall, which examines each one and prevents any that don't meet the security requirements.
5) *Anti-virus software:* A computer application known as antivirus software works to identify, stop, and take action against dangerous software programs like viruses and worms. In order to scan for new viruses as soon as they are identified, the majority of antivirus products have an auto-update capability that allows the programe to download profiles of new viruses. Every system must have anti-virus software as a fundamental requirement.

VII. CYBER ETHICS

The internet's code is nothing more than cyber ethics. There is a good possibility that we will use the internet in a proper and safe manner if we put these cyber ethics into practice. Several of them are listed below:

1) USE THE INTERNET TO CONNECT WITH PEOPLE AND COMMUNICATE. It's simple to remain in touch with friends and family, talk to coworkers, and share ideas and information with people nearby or halfway around the world thanks to email and instant messaging.
2) Avoid being a bully online. Don't hurt someone by calling them names, making up stories about them, sending embarrassing images of them, or doing anything else.
3) The Internet is regarded as the world's largest library, offering information on every subject imaginable. As a result, it is always crucial to use this information responsibly and legally.
4) Avoid using other people's credentials to access their accounts.
5) Never attempt to corrupt other people's systems by sending malware to them.
6) Never give out your personal information to anyone because there's a chance that someone will misuse it and get you into trouble.
7) Never put up a false front when communicating online, and avoid creating fictitious identities of other people because doing so could get you and them both into trouble.

• Always respect copyrighted information, and only download legal games or videos. The aforementioned are a few cyber-ethics that one should adhere to when utilizing the internet. Since we were very young, we have always been taught the correct rules, and the same is true in cyberspace.

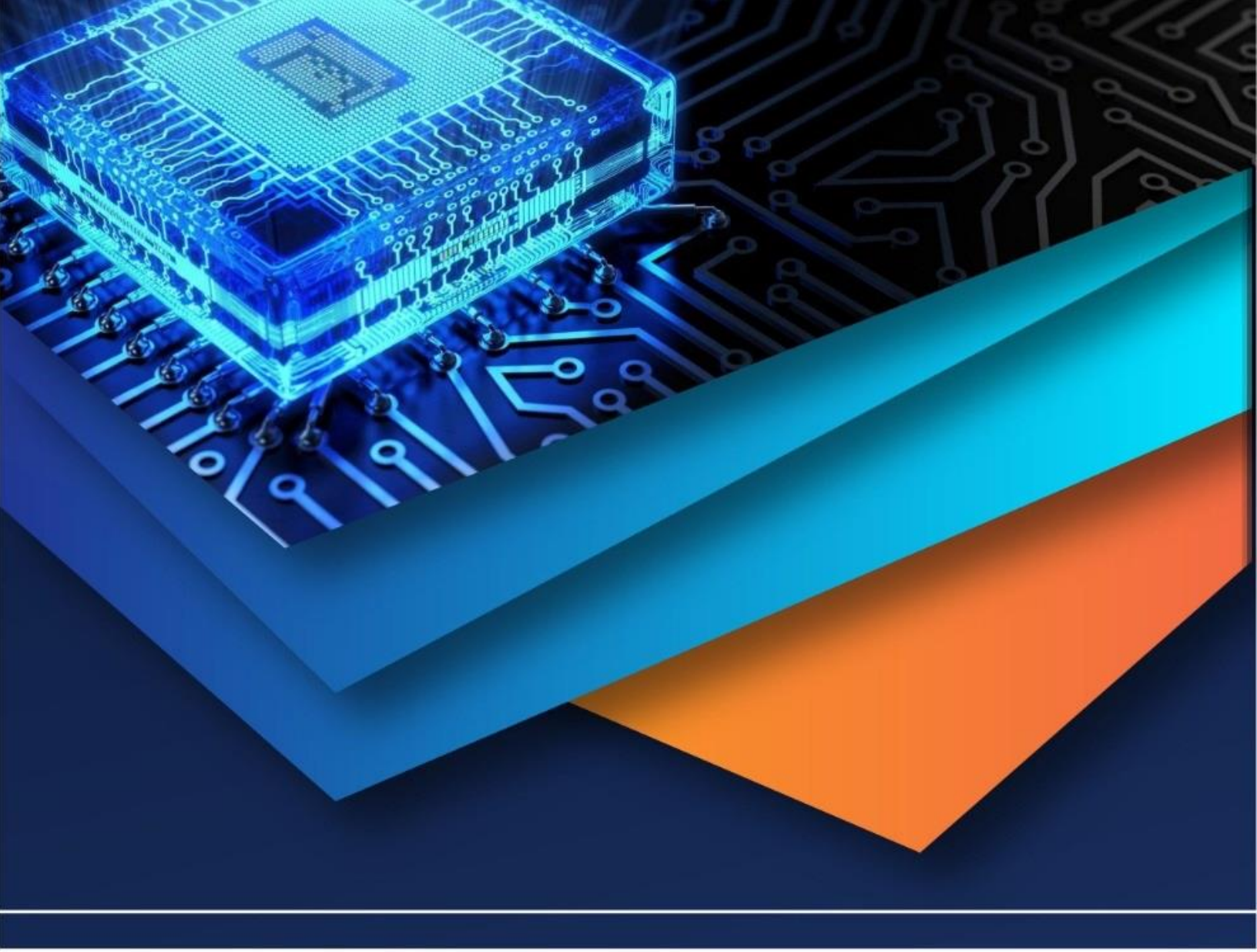
VIII. CONCLUSION

Because the world is getting increasingly interconnected and relies on networks to conduct crucial transactions, the broad topic of cyber security is becoming more crucial.

As time goes on, cybercrime continues to take numerous routes while still protecting the data. Enterprises are being put to the test by the newest and most innovative technologies in terms of how they protect their infrastructure and how they require new platforms has enough wisdom to do so. The day-to-day emergence of new cyber tools and threats. In order to have a safe and secure future in cyberspace, we should do our best to reduce cybercrimes. However, there is no ideal answer to this problem.

REFERENCES

[1] Understanding cybercrime and cyber security - Sunit Belapure N. Godbole
[2] Audrie Krause's report for NetAction, Computer Security Practices in Nonprofit Organizations
[3] James Lyne's article for Sophos, dated April 12, 2014, titled "Eight Trends Shaping Network Security."
[4] A Review of Cyber Security 2012 by Luis Corrons of Panda Labs
[5] "Study of Cloud Computing in the HealthCare Industry," by G.Nikhita Reddy and G.J. Ugander Reddy, appeared in the September 2013 issue of the International Journal of Scientific & Engineering Research, volume 4, issue 9.
[6] Safety Critical Systems - Next Generation, IEEECS, July/August 2013, IEEE Security and Privacy Magazine.
[7] CIO Asia, September 3, H1 2013, by Avanthi Kumar, "Cyber security in Asia."



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY