# Current Technological Advancements and Emerging Trends Pose Challenges for Cybersecurity

Nikeeta[1], Shristi[2], Ms. Shreya Sharma [3], Dr. Anil Kumar Lamba[4], Ms. Aarti Maan[5]

[1]Student (UG), CSE Department, Geeta Engineering College, Panipat
[2]Student (UG), CSE Department, Geeta Engineering College, Panipat
[3]Assistant Professor, CSE Department, Geeta University, Panipat
[4] Professor, CSE Department, Geeta University, Panipat
[5]Assistant Professor, CSE Department, Geeta University, Panipat
nikkimalik55@gmail.com , jaglanshristi@gmail.com , shreya.cse@geetauniversity.edu.in , dranil.cse@geetauniversity.edu.in ,cse.ap2@geetauniversity.edu.in

**Abstract:** In the current digital era, cyber security has become a critical concern for organizations worldwide. With the increasing use of advanced technologies such as cloud computing, the Internet of Things (IoT), and artificial intelligence, new cyber security challenges have emerged. This study aims to examine the challenges faced by cyber security professionals in keeping up with the latest technologies and trends. Additionally, the study will explore emerging technologies and their potential impact on cyber security. Information technology has emerged as one of the most important growth drivers for long-term economic development. More specifically, cyber security has emerged as a critical factor in ensuring global sustainable development. When we think of cyber security, the first thing that comes to mind is 'cyber-crimes', which are increasing at an alarming rate. Various governments and businesses are taking numerous steps to combat cybercrime. Aside from various measures, cyber security remains a major concern for many people. This paper focuses on the challenges of cyber security on the most recent technologies. It also focuses on the most recent cyber security techniques, ethics, and trends that are changing the face of cyber security.

**Keywords:** Cyber security, cyber-crime, cyber ethics, social media, cloud computing,

## Introduction:

Moment, a person can shoot and admit any type of data via dispatch, audio, or videotape with the simple press of a button, but has he ever considered how securely his data is being delivered to the other person without any information being blurted ? Cyber security has the result. The structure of ultramodern living that's rising the fastest is the internet. Because further than 60 of total marketable deals are now done online, this field needed a high position of security for transparent and stylish deals. As a result, cyber security has surfaced as a hot content. The compass of cyber security extends beyond securing information in the IT assiduity to colorful other fields similar as cyber space, etc. Even slice- edge technologies similar as pall computing, mobile computing, E-commerce, and net banking bear a high position of security. Because these technologies contain sensitive information about a person, their security has come critical. Perfecting cyber security and securing critical information structure are critical to each country's security and profitable well- being. Making the Internet safer (and guarding Internet druggies) has come an essential element of the development of new services as well as government policy. Numerous nations and governments are now administering strict cyber security laws in order to help the loss of critical information. Every existent must be trained in cyber security in order to cover themselves from the growing number of cyber-crimes.

### 1. Cyber Crime:

Any illicit action that uses a computer as its main tool for commission and theft is referred to as cybercrime. The concept of "cybercrime" as used by the U.S. Department of Justice has been broadened to include any criminal action that keeps evidence on a computer. Crimes that have been made possible by computers, like network intrusions and the spread of computer viruses, as well as computer-based variations of already-common crimes, like identity theft, stalking, bullying, and terrorism, which have become major problems for people and nations, are all included in the growing list of cybercrimes.

## 2. Cyber Security:

Data security and sequestration are always the top security preventives that any establishment takes. In the world we presently inhabit, all information is kept in digital or cyber form. Druggies can engage with musketeers and family in a safe terrain on social networking spots. Cybercriminals will continue to target social media spots in the case of home druggies in order to steal particular information [2]. A person must take all necessary security preventives during bank deals as well as when using social networking spots.

## 4. Trends Changing Cyber Security:

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

### 4.1. Mobile Networks:

We have instant access to everyone, anywhere in the globe. Even so, these mobile networks continue to take security very seriously. As more people use devices like tablets, phones, Computers, and other similar devices—all of which require additional security measures in addition to those built into the programs being used—firewalls and other security measures are currently becoming more accessible. Always take into account how secure these mobile networks are. Extreme vigilance must be used in the event of any security issues because mobile networks are relatively susceptible to these cybercrimes.

#### 4.1.1. Cloud Computing:

Now days slowly but surely, small, medium, and large organizations are promoting pall services. To put it another way, the earth is gradually encroaching on the shadows. This most recent trend poses a serious threat to cyber security since it allows businesses to avoid traditional sources of scrutiny [1]. In order to help the loss of essential data, policy controls for online operations and pall services will also need to adapt as the number of operations available in the pall rises. Security enterprises remain a big problem even while most services are developing their

own strategies. Although the pall may have many advantages, it's crucial to remember that as it grows, security issues also do.

### 4.2. Web Servers:

Online application attacks that seek to steal data or spread malicious code remain dangerous. Cybercriminals spread their harmful malware by using legitimate web servers that they have hacked. Yet, attacks that steal data also pose a serious threat and are frequently reported in the media. Now, we must concentrate more on protecting web servers and web applications. Web servers are particularly effective platforms for these thieves to steal data. One needs to use a safer browser all the time, especially while doing important transactions, to prevent falling prey to these frauds.

### 4.3. Code Encryption:

Encryption is the process of encrypting communications (or information) to prevent hackers or eavesdroppers from reading them. An encryption approach converts the message or information into an unreadable cipher text using an encryption algorithm. Usually, this is done using an encryption key, which specifies how the message will be encoded. At its most fundamental level, encryption protects the confidentiality and integrity of data. Yet growing encryption use brings even more cyber security issues.

### 4.4. IPv6: New Internet protocol:

The new IPv6 protocol is taking the role of the outdated IPv4 protocol, which served as the basis for both our networks and the Internet in general. To defend IPv6, more is required than only moving IPv4 capabilities. Although IPv6 completely replaces IPv4 in terms of increasing the number of IP addresses available, security policy still needs to account for certain fairly fundamental changes to the protocol. To reduce the risks connected with cybercrime, it is therefore always desirable to switch to IPv6 as soon as is practical

### 4.5. APT's and Targeted Attacks

A new type of malicious malware known as “APT" (Advanced Persistent Threat). For years, detecting such targeted assaults has relied heavily on network security techniques like web filtering and intrusion prevention systems (IPS) (mostly after the initial compromise). Network security needs to integrate with other security services to identify attacks as they happen since attackers are becoming more daring and using shadier methods. Thus, we must strengthen our security protocols to prevent the emergence of fresh hazards in the future.

Hence, the aforementioned are some of the developments that are altering the global landscape of cyber security.

The top network threats are listed in Fig. -1 below.

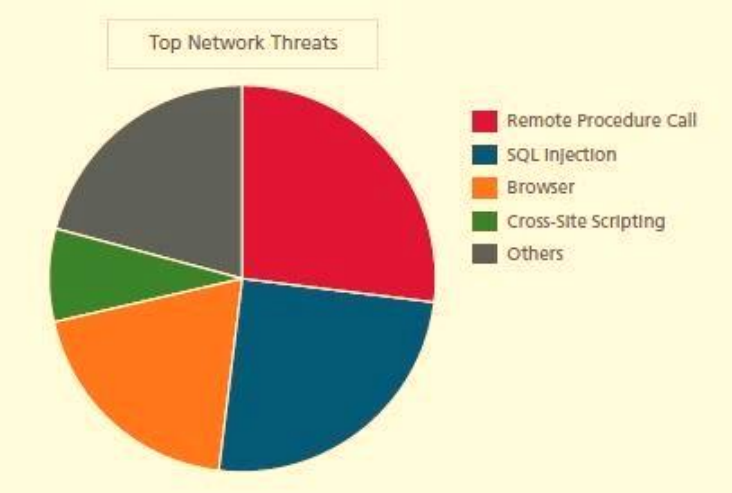


**Figure 1The Pie Graphic up top illustrates the main dangers to networks and online safety.**

## 5. Social Media's Part in Cyber Security:

Companies must discover inventive methods to protect client information in a world that is getting more social and connected. Social media is essential to cyber security and will significantly affect individual cyber threats. Companies are using social media more and more, just like there could be an assault [3]. Due to the fact that the majority of people use social networking sites virtually daily, social media has grown to be a significant platform for hackers to access personal data and steal important information.

Businesses cannot afford to stop using social media since it is so important for building brand awareness, even though it can be exploited for cybercrime [5]. They need solutions that will draw their attention to the issue so they can deal with it before any real harm is done. But, organizations should be aware of this, understand the relevance of information analysis, particularly in social conversations, and provide appropriate security measures in order to minimize risks. Social media management requires the use of the proper tools and techniques.

## 6. Cyber Security Techniques:

6.1. **Authentication of Data:** The papers we get must always be validated before downloading, which entails checking to make sure they are authentic and haven't been altered. Usually, these documents are verified using antivirus software that is installed on the machines [4]. To protect the devices from infections, a dependable anti-virus program is required.

6.2. **Access Control and Password Security:** User names and passwords have long been given top priority in information security. This might be one of the first cyber security measures.

6.3. **Firewalls:** A firewall is a piece of hardware or software that helps prevent viruses, worms, and hackers from trying to access your computer via the Internet. Every message that enters or leaves the internet is examined by the installed firewall, and those that do not follow the set security standards are blocked. Firewalls are therefore essential for the identification of malware.

6.4. **Anti-Virus Software:** Antivirus software is a type of computer program that seeks out, prevents, and eliminates harmful software programs like viruses and worms. Most antivirus programs offer an automatic update feature that allows the program to obtain profiles of new infections so that it can scan for them as soon as they are discovered. As a basic requirement, anti-virus software must be installed on every system.

6.5. **Malware Scanners:** Typically, this software scans every file and document on the computer for dangerous viruses or malicious code [6]. Trojan horses, worms, and viruses are examples of harmful software, which is referred to as malware.

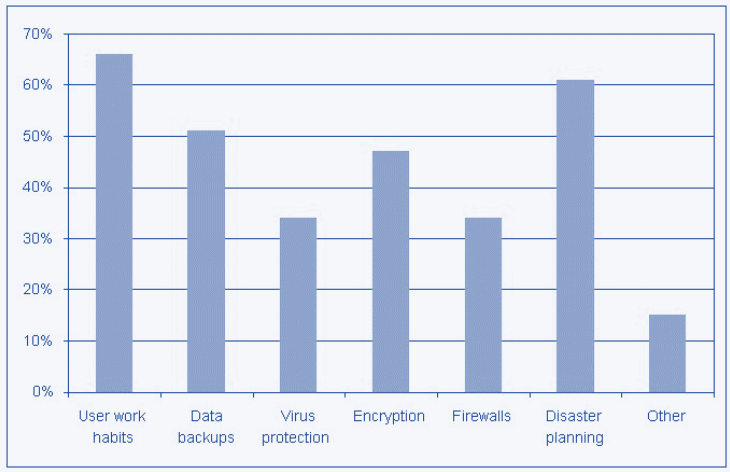


**Figure 2 Techniques of cyber security**

## 7. Conclusion

Networks are utilized to carry out essential operations; therefore, computer security is a broad subject that is becoming more important as the world becomes more connected. When each New Year comes and goes, cybercrime and information security both continue to evolve in new ways. Enterprises are being put to the test by the newest and most cutting-edge technology in terms of how they protect their infrastructure and how they use new platforms and intelligence to do so, in addition to the new cyber tools and threats that emerge every day. If we wish to have a safe and secure future in cyberspace, cybercrimes cannot be totally abolished, but we should do everything in our ability to limit them.

## 8. Future Work

Cyber ethics are the foundation of the internet's code. If we put these cyber ethics into practice, there is a good chance that we will utilize the internet ethically and safely [7]. The following is a list of a few of them.

- With information available on any topic imaginable, the Internet is recognized as the largest library in the world. So, it is always essential to use this information sensibly and lawfully.
- Refrain of internet bullying. Don't insult someone, make up a story about them, email them embarrassing pictures of themselves, or do anything else that could cause them harm.
- Never access someone else's account using their password.
- Never try to deliver malware to other people's computers to corrupt them.
- Always abide by any copyright instructions, and only download authorized videos or games.
- Avoid trying to impersonate someone online or making bogus profiles for them because doing so could land you and the impersonator in hot water.
- Avoid trying to impersonate someone online or making bogus profiles for them because doing so could land you and the impersonator in hot water.

Some cyber-ethics that one should follow when using the internet include those described above. We were always taught the right rules when we were very young, and the same is true in cyberspace.

**REFERENCES**

[1] 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 " by G.Nikhita Reddy, G.J.Ugander Reddy.

[2] CIO Asia, September 3rd, H1 2013: Cyber security in Malaysia by Avanthi Kumar.

[3] Computer Security Practices in Non-Profit Organizations – A Net Action Report by Audrie Krause.

[4] A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.

[5] IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

[6] Cyber Security: Understanding Cyber Crimes- SunitBelapure Nina Godbole.

[7] A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.