IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125147

# CYBER SECURITY AND ITS EMERGING TREND ON THE LATEST TECHNOLOGIES

**Parmeshwar R. Kumare[1], Lowlesh N. Yadav[2], Vijay M. Rakhade[3]**

Student, Shri sai college of Engineering and Technology, Bhadrawati, India[1]

Head of the Department, Computer Science and Engineering, Shri sai college of Engineering and Technology, Bhadrawati, India [2]

Assistant Professor, Computer Science and Engineering, Shri sai College of Engineering and Technology, Bhadrawati , India [3]

**Abstract**: The term "cybersecurity" refers to the practice of protecting electronic information by reducing information risks and vulnerabilities. Data threats can be caused by a variety of factors, including intentional attacks (such as hacking) or unintentional events (such as power outages). Cyber security includes measures to prevent unauthorized access to electronic information and systems and prevent hijacking of information and systems. Some of the latest artificial intelligence (AI) developments have implications for cybersecurity. For example, machine learning techniques can be used to identify malware and natural language processing can be used to decrypt large volumes of text for security-related information. Artificial intelligence can also be used to create new approaches to endpoint security, network security, and user authentication.

**Keywords:** cybersecurity, hacking, artificial intelligence, malware.

## I. INTRODUCTION

As the world becomes increasingly digital, so too does the need for cybersecurity. In today's connected world, sensitive information is stored online and easy to hack. Cybersecurity is the practice of protecting computers and networks from unauthorized access or theft. In recent years, there has been a growing interest in using artificial intelligence (AI) for cybersecurity purposes. AI can be used for a variety of tasks, including detecting malicious activity, developing new attack strategies, and accelerating responses to cyber incidents. This includes measures to prevent unauthorized persons from accessing or stealing information. Cybersecurity is often confused with information security.

•Cybersecurity aims to protect computer systems from unauthorized access or other damage or inaccessibility.
•Information security is a broad category that protects all information assets, whether in physical or digital form.

Managing cybersecurity in a changing threat landscape is a challenge for every organization. The traditional approach of focusing resources on protecting systems against the most well-known threats and not protecting less severe ones is not a smart idea. Keeping up with security changes requires additional protection and flexibility.

## II. OVERVIEW AND CONCEPTS OF CYBERSECURITY

There are many important concepts related to cybersecurity. It is important to understand these concepts to effectively defend against cyber-attacks.

*Data. Data is the most important asset of any organization. Essential to running our business and providing services. Protecting data from unauthorized access or theft is an important aspect of cybersecurity.
*Virus-A is a type of malware designed to damage or disable your computer. Viruses can spread quickly and wreak havoc on networks.
*Malicious software. Malicious software is any software designed to damage or disable your computer. May contain viruses, spyware, and trojan horses.
*A firewall is a system designed to block unauthorized access to a computer network. Firewalls can be hardware or software.
*Intrusion Detection Systems - Intrusion detection systems are tools for detecting and responding to attacks on computer networks.

DOI: 10.17148/IJARCCE.2023.125147

*Encryption - Encryption is the process of changing data so that it cannot be read by unauthorized persons. Encryption is an important part of network security.

Cybersecurity can be a broad field spanning many disciplines. It is divided into 7 main pillars:

1. Network security: Most attacks originate from networks, and network security solutions are designed to detect and protect against them. These solutions include information and management such as Data Loss Management (DLP), Identity Access Management (IAM), Network Access Control Council (NACA), and Next Generation Firewall (NGFW) application management to ensure the safe use of the Internet. Advanced layered cyber threat prevention system including Intrusion Prevention System (IPS), Next Generation Anti-Virus (NGAV), Sandboxing, and Content Disarmament and Restructuring (CDR). Network analysis, threat detection, and automated Security Orchestration and Response (SOAR) technologies are also required.

2. Cloud security: As more and more organizations adopt cloud computing; cloud security is becoming a top priority. A cloud security strategy includes cybersecurity solutions, controls, policies, and services that help protect an organization's cloud infrastructure (applications, data, infrastructure, etc.) from attacks. Many cloud service providers offer security solutions, but these solutions often do not provide enterprise-grade security in the cloud. Protect against known intrusions and attack schemes by adding third-party solutions in your cloud environment.

3. Endpoint security: The Zero Trust security model is based on micro-segmentation based on localization. Any technology that attempts to do this to mobile workers falls prey to endpoint security. End-to-end security allows businesses to manage information and network security, protect against threats such as anti-phishing and ransomware protection, and protect end users such as desktops and laptops through forensic technologies such as endpoint detection and response (EDR). Answers.

4. Mobile Security: Most unlabelled mobile devices such as tablets and smartphones can access corporate information and expose organizations to threats from malicious apps, zero-day exploits, phishing, and IM (instant messaging) attacks. Mobile security guards against these attacks and protects functions and devices from hacking and jailbreaking. When the AN MDM (Mobile Device Management) solution is connected, businesses can ensure that only compatible mobile devices can access assets.

5. IoT security: Internet of Things (IoT) devices are effective, but they also expose organizations to new cyber threats. Criminals threaten to attack malicious devices that cannot connect to your network for nefarious purposes, such as access to your company's business or other grubs around the world. IoT security protects vulnerable IoT devices from discovery and classification of connected devices, automatic deployment to manage network operations, and IPS-based victim sandboxing to block attacks on critical IoT devices. In some cases, limited agents may be used to optimize your device's computer system to prevent exploits and attacks.

6. Application security: Like anything directly connected to the internet, web applications are subject to threats. Since 2007, OWASP has been monitoring 10 major Internet application security threats, including injections, authentication failures, misconfigurations, and scripts. OWASP Prime 10 attacks are blocked by security applications. The security app also prevents caterpillar attacks and blocks all interactions between the app and the bees. Through continuous learning, applications can be maintained when DevOps releases new content.

7. Zero Trust: Archaic security structure around the perimeter that creates a fortress-like wall around the organization's assets. However, this approach has many problems, such as the threat it can pose to business leaders, which causes the network perimeter to disappear quickly. As assets circulate off-premises as a part of cloud adoption and faraway operations, a brand-new method to safety is required. Zero Trust takes a complementary approach to the security and protection of personal assets by combining micro-segmentation, monitoring, and social governance with responsible access control.

## III. IMPORTANCE OF NETWORK SECURITY

The importance of network security relates to the use of information by unknown or unauthorized users. This is done with special attacks called cyberattacks. Good? A cyber-attack is an external or internal threat or attempt by an attacker to exploit and compromise the confidentiality, integrity, and availability of an organization's plans or personal information. Cyber attackers use illegal methods, tools, and techniques to damage, disrupt or gain access to computers, devices, networks, applications, and illegal information. There are many different types of cyber-attacks, and the following list shows some of the main attacks that criminals and attackers use to exploit the software:

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125147

- Malware
- Ransomware
- Injection prevention (e.g. cross-site scripting, SQL injection, security injection)
- Control and middleman attacks
- phishing
- denial of service
- privilege escalation
- unpatched/vulnerable software
- remote code execution
- brute force

We must use network security to prevent such attacks. Not just cyber security, but information security and privacy, etc. Everything that leads to it must be implemented. As time goes on, new attacks are used and we become more vulnerable to them, so technologies such as machine learning and AI (artificial intelligence) need to be used in conjunction with cybersecurity to improve the site.

To solve many of these problems, it is necessary to develop a self-learning AI-based cybersecurity incident management system. Modern technologies can teach self-learning processes without collecting all business data. It then analyses information that doesn't need to create a social structure, from millions of symbols to billions of symbols related to the fight for the economy. The result is a new level of knowledge of the human community in various categories of cybersecurity, including IT plus products. Get the complete product, the product you want, and the users and applications accessing your data. Distribution and market evaluation also play an important role in sales.

Threat Revealing - Hackers follow similar patterns as others, so today's hackers change frequently. AI-based cybersecurity systems will provide global and industry-specific threat information to help you make critical decisions not only about what will attack your business but also to support those that cannot attack your business.

Managing Productivity - Understanding the impact of the various security tools and processes you use is critical to effectively managing security. AI will help you understand where your information security is strong and where there are gaps.

Crime - IT Reporting In addition to Inventory, Risk Reporting, and Operations Management, AI-based systems will already predict how and where a crime will occur, but you will be able to focus on weak areas with resources and energy distribution. The guidance provided by AI analytics can help improve an organization's cyber resilience by integrating and improving controls and processes. incident response.

AI-powered systems respond to rich context and security alerts, respond quickly to incidents, and identify root causes to mitigate adverse effects and prevent future issues.

## IV. ADVANTAGES

Benefits Prevent data leakage. Prevent network attacks. User policy.

## V. NO LIMITATIONS EXTENSION POLICY

Unsecured network. Unsecured communication channel. unknown error. Legacy system. Maintenance not found. IoT and more connected content.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125147

## VI. CONCLUSION

As more and more organizations use these analytical tools, there is no limit to what they can do. Machine learning can help organizations not only detect threats but eliminate them before they impact operations. The future of cybersecurity depends on artificial intelligence or machine learning.

## REFERENCES

1. Technologies in Cybersecurity" by SANS Institute:
   Link: https://www.sans.org/reading-room/whitepapers/application/emerging-technologies-cyber-security-36620
2. "Emerging Trends and Technologies in Cyber Security" by International Journal of Science and Research (IJSR):
   Link: https://www.ijsr.net/archive/v5i2/NOV161463.pdf
3. "Emerging Trends in Cybersecurity and Data Privacy" by Infosecurity Magazine:
   Link: https://www.infosecurity-magazine.com/magazine-features/emerging-trends-cybersecurity/
4. "The Future of Cybersecurity: Trends to Watch" by Security Intelligence:
   Link: https://securityintelligence.com/posts/future-cybersecurity-trends-watch/
5. "Emerging Trends in Cybersecurity for 2021 and Beyond" by HelpSystems:
   Link: https://www.helpsystems.com/resources/articles/emerging-trends-cybersecurity-2021
6. "Emerging Trends in Cybersecurity: Challenges and Solutions" by ScienceDirect:
   Link: https://www.sciencedirect.com/science/article/pii/S1877050920323493
7. "Emerging Cybersecurity Trends and Technologies" by Government Technology:
   Link: https://www.govtech.com/security/emerging-cybersecurity-trends-and-technologies.html
8. "Emerging Technologies in Cybersecurity: Industry Report 2021" by CyberDB:
   Link: https://cyberdb.co/cybersecurity-industry-report-2021/
9. "Cybersecurity Trends: 2021 and Beyond" by IBM Security: Link: https://www.ibm.com/security/digital-assets/cybersecurity-trends-2021.pdf
10. "Emerging Trends in Cybersecurity 2021" by Hitachi Systems Security:
    Link: https://hitachi-systems-security.com/wp-content/uploads/2021/05/Emerging-Trends-in-Cybersecurity-2021-1.pdf
11. "Top 10 Cybersecurity Trends to Watch in 2021" by CSO Online: Link:
    https://www.csoonline.com/article/3605758/top-10-cybersecurity-trends-to-watch-in-2021.html
12. "Emerging Trends in Cybersecurity: A Review" by International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE):
    Link: http://ijarcsse.com/Before_August_2017/docs/papers/Volume_8/June2018/V8I6-0155.pdf
13. "Emerging Trends in Cybersecurity 2021" by Mimecast: Link:
    https://www.mimecast.com/globalassets/documents/mimecast-research/emerging-trends-in-cybersecurity-2021-4.pdf
14. "Emerging Trends in Cybersecurity" by NortonLifeLock:
    Link: https://us.norton.com/internetsecurity-emerging-trends-in-cybersecurity.html
15. "Emerging Trends in Cybersecurity" by Oxford Academic:
    Link: https://academic.oup.com/cybersecurity/article/5/1/tyaa011/6203515
16. "Emerging Trends in Cybersecurity for 2021 and Beyond" by Security Magazine:
    Link: https://www.securitymagazine.com/articles/94912-emerging-trends-in-cybersecurity-for-2021-and-beyond
17. "Emerging Trends and Technologies in Cybersecurity" by Security Intelligence:
    Link: https://securityintelligence.com/posts/emerging-trends-and-technologies-in-cybersecurity/
18. "Emerging Technologies in Cybersecurity: A Comprehensive Review" by International Journal of Advanced Computer Science and Applications (IJACSA) Link: https://thesai.org/Downloads/Volume11No3/Paper_39-Emerging_Technologies_in_Cybersecurity.pdf