Cybersecurity Technologies and Solutions
Hassan Saad Fadhil

IT Engineer, Department of Computer Engineering, Mosul University, IRAQ

Email: computer.eng.hassan@gmail.com

**Abstract:** *Nowadays, the majority of transactions are carried out online, necessitating high-quality security for an efficient and completely secure concern. A very high level of security was also required for some of the most recent innovations, such as cloud computing, internet banking, and mobile technology. Because these solutions store users' private information, protecting it is crucial. In this paper, we reviewed the most prominent* *solutions for Cybersecurity issues and the most trending technologies that are used.*

**Keywords:** *Cybersecurity, information security, Deep Learning, Machine Learning.*

1. **INTRODUCTION**

Over the past few years, a lot has been written and said about advanced persistent threats in cyberspace and their potential and actual impact on the nation's information infrastructure. Digital dangers represent a mission confirmation challenge, whether mission affirmation is understood fundamentally as a day-to-day existence cycle framework designing interaction or as an issue space that incorporates framework strength, vigor, survivability, congruity of tasks (COOP), or business progression - especially zeroing in on mission fundamental capabilities, and business process reengineering. The intent and sophistication of cyber threats vary, and their effects on the system or network they target can also vary widely. One constant is that the majority of advanced cyber attacks simply cannot be stopped by the cyber defenses that are currently in use [1]. In today's cyberspace, the world is expanding rapidly. People with malicious intentions are given opportunities by the extraordinary growth in information access. Protecting systems and technologies from unusual activities is a pressing necessity. Maintaining an organization's computing assets' Integrity, Confidentiality, and Availability (ICA) or their ability to connect to the network of another organization is referred to as cyber security. Numerous researchers believed and advocated for educating the younger generation about cyber-security concepts in light of the evolution and growth of cyber threats. [2].

 The safety of data is a major concern for any government, and more and more information is now handled digitally or through cyberspace. Additionally, many social media platforms provide a safe environment where users can connect with others from around the world. Social media is the primary target of the crimes discussed for evaluating unauthorized information. Crime is on the rise as a result of people's inability to safeguard sensitive information as a result of technological advancements [3].

1. CYBER SECURITY CHALLENGES

The process of digitization in every facet of human life, including education, business, healthcare, and other areas, has resulted in the gradual storage of all types of data, including sensitive data. The process of safeguarding digital information from theft or physical damage while maintaining its confidentiality and availability is known as security. However, as technology advances rapidly, the rate of cybercrime also rises in both number and complexity. Technical attackers create more potent attack tools to investigate the target's weaknesses and thus attack the victim. As a result, numerous novel and challenging-to-detect variants of attacks are emerging[4].
Cyber security also protects against traditional crimes that are carried out over the Internet as well as those that involve computers and networks[5]. Organizations are becoming more aware of information and related technologies in almost every function, particularly in driving innovation and generating competitive advantage. Corporate information and technology services are vulnerable to various security risks in today's information environment (Figure 1), including the leakage of sensitive data and prolonged disruptions in email and internet access, all of which significantly impact business continuity[6].

As opposed to the more conventional method of detecting malicious signatures, the focus of cybersecurity has recently shifted to monitoring network and Internet traffic for the detection of malicious actions. Particularly, traditional cybersecurity focuses on catching malware by examining incoming traffic for malware signatures that only detect limited-scope threats that have previously been encountered. Additionally, the development of signatures lags significantly behind that of cyber attack strategies[7]. The typical practice of putting in place security measures across the entire organization, such as firewalls and anti-virus software, is only the very beginning of cyber security management in today's complex and interconnected business environment [8].



*Figure 1 Relationship Between Cybersecurity and Other Security Domains* [9]

2.1 Security Modeling Criteria

It is common knowledge that exploiting vulnerabilities can compromise a system's security by introducing unwanted changes to one of the system's three properties—Availability, Integrity, or Confidentiality. Through the creation of policy rules and their implementation, the majority of the currently available security models attempt to address only one system property at a time. In this instance, none of the three aspects can be compromised because they are all extremely crucial to the mission [10].

* + 1. High-Level Security Requirements

Cyber security of the systems is one of the biggest obstacles to smart grid deployment, according to the Electric Power Research Institute (EPRI) [19]. The EPRI Report says that cyber security is a big problem because this important industry is more likely to be hit by cyberattacks and incidents as it gets more connected. Inadvertent compromises of the information infrastructure as a result of user errors, equipment failures, and natural disasters are all examples of deliberate attacks that must be addressed by cyber security. An attacker may be able to exploit vulnerabilities to gain access to control software, penetrate a network, and alter load conditions, resulting in unpredictable grid destabilization. Various organizations conduct the high-level requirements for smart grid communication security and the corresponding standards in detail[11].

1. MACHINE LEARNING AND CYBER SECURITY

 The transfer of data across the network between nodes is the Internet's primary function. The Internet is a worldwide network of millions of distinct computers, networks, and other devices. The number of people using the Internet has skyrocketed as a result of advancements in mobile devices, networks, and computer systems. As a result, adversaries and cybercriminals have turned their attention to the Internet[12].

 The machine learning (ML) technique is being used in cyber security more and more than ever before. ML is one of the promising solutions that have the potential to be effective against zero-day threats, starting with the classification of IP traffic and filtering malicious traffic for intrusion detection. A few ML techniques and how they can be used in cyber security are discussed. The paper provides a set of comparison criteria for the ML method and makes recommendations for the best approach based on the characteristics of the cyber security issues. In ML methods, data is very important. Before performing any kind of analysis, a machine learning researcher must have a thorough understanding of the data set. Second, the ML analysis cannot directly utilize raw data like NetFlow, packet capture, and other network data.[13].

1. DEEP LEARNING TECHNIQUES FOR CYBER SECURITY

The Critical National Infrastructure (CNI) of a nation, which uses and relies on Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) to manage their production, is the primary target of cyberattacks. Examples of CNI include water, gas, electricity, and hospitals. The protection of CNIs becomes an important consideration. There is a variety of legal, technical, organizational, capacity-building, and cooperation aspects that are used to classify the currently available protective measures. In addition to policies and regulations that can be used to combat cyberattacks against CNIs, specific practical steps must be taken for these regulations to be effective[14].

1. IOT AND CYBER-SECURITY

In the past, just mobiles and PCs were associated with the web yet in the new time with the appearance of new advancements different things like surveillance cameras, microwaves, vehicles, and modern hardware are presently associated with the web This organization of things is known as the web of things. There are currently 6 billion internet-connected devices, and this number is expected to rise to 20 billion in a few years. Software security solutions exist for the majority of attacks on PCs and mobile devices, but similar security solutions do not exist for the rest of the internet of things[15]. The Internet of Things (IoT) has been widely used in industries, smart cities, and healthcare. Homes, workplaces, and public transportation are where people spend the most time [16].

1. CONCLUSION AND FUTURE DIRECTION

 The well-being of any modern organization is the responsibility of the executive management. Information Security plays a crucial role in an organization's well-being because most, if not all, organizations are entirely dependent on the confidentiality, integrity, and availability of their information assets; Consequently, the majority of businesses utilize Cyber Space for essential business procedures; likewise, the Internet has emerged as an essential link in contemporary information systems.

It is now possible to delve deeper into the development of these technologies and move forward to improve the security of our environment and our work after we reviewed the most important technologies used in cybersecurity and discussed their future and the possibilities or security criteria that they offer.

**REFERENCES**

[1] D. J. Bodeau, R. Graubart, and J. Fabius-Greene, “Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels,” *Proc. - Soc. 2010 2nd IEEE Int. Conf. Soc. Comput. PASSAT 2010 2nd IEEE Int. Conf. Privacy, Secur. Risk Trust*, pp. 1147–1152, 2010, doi: 10.1109/SocialCom.2010.170.

[2] J. Kaur and K. R. Ramkumar, “The recent trends in cyber security: A review,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5766–5781, 2022, doi: 10.1016/j.jksuci.2021.01.018.

[3] M. L. Ali, K. Thakur, and B. Atobatele, “Challenges of cyber security and the emerging trends,” *BSCI 2019 - Proc. 2019 ACM Int. Symp. Blockchain Secur. Crit. Infrastructure, co-located with AsiaCCS 2019*, pp. 107–111, 2019, doi: 10.1145/3327960.3332393.

[4] K. M. Rajasekharaiah, C. S. Dule, and E. Sudarshan, “Cyber Security Challenges and its Emerging Trends on Latest Technologies,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 981, no. 2, 2020, doi: 10.1088/1757-899X/981/2/022062.

[5] A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood, “Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications,” *Proc. - 2013 11th Int. Symp. Auton. Decentralized Syst. ISADS 2013*, 2013, doi: 10.1109/ISADS.2013.6513420.

[6] D. Ghelani, “Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review,” *Authorea Prepr.*, vol. 8345, no. X, 2022, doi: 10.11648/j.XXXX.2022XXXX.XX.

[7] T. Mahmood and U. Afzal, “Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools,” *Conf. Proc. - 2013 2nd Natl. Conf. Inf. Assur. NCIA 2013*, pp. 129–134, 2013, doi: 10.1109/NCIA.2013.6725337.

[8] Y. S. Chen, P. Pete Chong, and B. Zhang, “Cyber security management and e-government,” *Electron. Gov.*, vol. 1, no. 3, pp. 316–327, 2004, doi: 10.1504/EG.2004.005555.

[9] B. Von Solms and R. von Solms, “Information & Computer Security Article information : Cyber Security and Information Security – What goes where ?,” *Inf. Comput. Secur.*, 2018.

[10] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, “Cyber security threat analysis and modeling of an unmanned aerial vehicle system,” *2012 IEEE Int. Conf. Technol. Homel. Secur. HST 2012*, pp. 585–590, 2012, doi: 10.1109/THS.2012.6459914.

[11] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on cyber security for smart grid communications,” *IEEE Commun. Surv. Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012, doi: 10.1109/SURV.2012.010912.00035.

[12] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, “A Survey on Machine Learning Techniques for Cyber Security in the Last Decade,” *IEEE Access*, vol. 8, pp. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[13] R. Das and T. H. Morris, “Machine learning and cyber security,” *2017 Int. Conf. Comput. Electr. Commun. Eng. ICCECE 2017*, 2018, doi: 10.1109/ICCECE.2017.8526232.

[14] M. A. Ferrag, L. A. Maglaras, H. Janicke, and R. Smith, “Deep Learning Techniques for Cyber Security Intrusion Detection : A Detailed Analysis,” pp. 126–136, 2019, doi: 10.14236/ewic/icscsr19.16.

[15] S. Naik and V. Maral, “Cyber security - IoT,” *RTEICT 2017 - 2nd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. Proc.*, vol. 2018-January, pp. 764–767, 2017, doi: 10.1109/RTEICT.2017.8256700.

[16] A. Alnasser, H. Sun, and J. Jiang, “Cyber security challenges and solutions for V2X communications: A survey,” *Comput. Networks*, vol. 151, pp. 52–67, 2019, doi: 10.1016/j.comnet.2018.12.018.

**Author's Biography (Mandatory)**

**Hassan S. Fadhil,** is a student of Computer Engineering at the College of the Engineering/ University of Mosul. He completed his M.Sc. in the department of Electrical and Computer Engineering/ ECE at Istanbul Altinbas University. His research interests are Cybersecurity, Smart Cities, Data Security, Data Hiding, and Social Engineering.



**Cite this paper:**

Hassan S. Fadhil, “Cybersecurity Technologies and Solutions”, Vol. xx, No. xx, pp. xx-xx, June 2022.