International Journal of Emerging Engineering and Technology (IJEET)
ISSN (e): 2958-3764
Volume: 4, Number: 2, Pages: 71- 76, Year: 2025

AI, Cybersecurity and Growing Ethical Dilemma: A Survey

Amna Iftikhar, Irshad Ahmed Sumra, Bilal Gillani, and Uneeb Raziq Khan

School of Systems and Technology, University of Management & Technology, Lahore, 54000, Pakistan
Corresponding author Amna Iftikhar (Email: amna.iftikhar1036@gmail.com)

Received: 12/02/2025, Revised: 23/05/2025, Accepted: 19/06/2025

***Abstract*— This survey paper examines the work of various researchers. It states that cybersecurity threats are increasing rapidly and becoming harder to prevent. A new subject, 'Artificial Intelligence,' has entered this space as a means for specialists to combat evolving cybersecurity threats and attacks. Utilising techniques such as threat identification and automated responses can help organisations protect sensitive and confidential data, ensuring security across corporations in a highly unsafe environment. This paper discusses the ethical use of AI in cybersecurity and demonstrates the need to ensure that new technologies are developed and used fairly, ethically, and responsibly.**

***Index Terms*—Artificial intelligence, cybersecurity, machine learning, internet of things (IoT), ethical AI, data privacy, cyber-physical systems.**

I. Introduction

Today artificial intelligence (AI) is widely used everywhere, from logic in online chess to finding trends in financial markets [1-8]. It provides people with information they might otherwise miss. Technology is advancing faster than laws, and this speed can lead to practices that are ethically corrupt and even harmful. Even though AI is used to defend systems against threats and attacks, "bad actors" might use it to attack vulnerable victims and systems [4, 9-11]. Moreover, private citizens who lack the resources to defend themselves are more likely to be attacked online, which is why government guidance in this regard is essential to protecting and ensuring their safety [12-20]. With the advent of more advanced AI tools, online threats have become a serious issue as hackers misuse AI to attack and exploit weaknesses. This urges companies to remain alert and protect themselves by taking preventive measures. This paper examines how AI use affects our digital safety and focuses on its ethical use for safety and security.

The following sections provide a comprehensive analysis:

- Basic Concept of AI and Cybersecurity: Analyzes AI foundations, ML techniques and their application in identifying and mitigating cyber threats;
- Use of machine learning in cybersecurity to strengthen protective measures: Gives a quick review of machine learning and cybersecurity and emphasizes their importance together
- IoT Security and Ethical Considerations: Discusses the integration of interconnected devices, the necessity of privacy-by-design and ethical engineering principles;
- Legal Compliance and Ethical Standards: Examines legal liabilities in AI decision systems, job displacement concerns and the importance of ethical management;
- Regulatory Policies and Conclusion: Reviews EU and US regulatory frameworks for AI governance and synthesizes the balance between innovation and safety.

II. Basic Concept of AI and Cybersecurity

Artificial Intelligence has become an essential part of our everyday activities, with its evident applications in email filtering, conversational agents, and interactive entertainment. [8, 21-26]. As compared to traditional programming, which uses fixed rules and data structures and can't be used for solving complex problems on a daily basis, AI is much more flexible and an adaptable solution for handling multiple tasks per day simultaneously and fills the gap of traditional programming failing by learning and analyzing historical events [27-35]. It can derive logical conclusions that might have been overlooked by humans, thereby removing the risk of human error and providing highly precise, verifiable data and results [36]. Fig. 1 illustrates how ML techniques are applied within an AI-powered cybersecurity framework to identify and neutralize threats in real time.

III. Use of Machine Learning in Cybersecurity to Strengthen Protective Measures

A. Quick Description of Machine Learning

Machine learning refers to a computer's ability to learn from data without human consciousness [19]. There are multiple examples for machine learning, such as teaching a program to read handwriting by feeding it millions of writing samples until it starts recognizing characters and symbols accurately [16]. The more data we feed a machine learning program, the better its outputs become as it learns from the data provided [15].

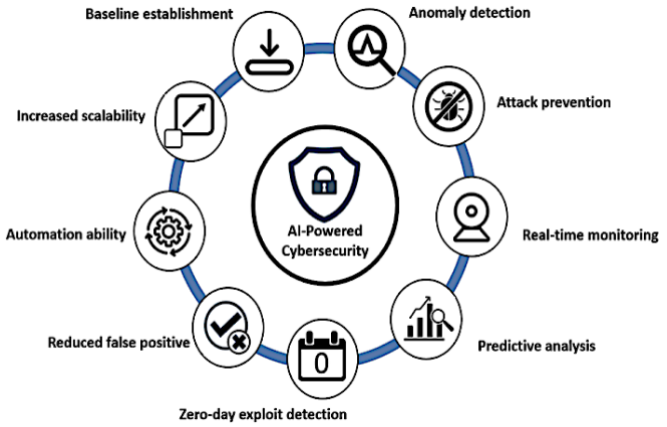

Fig. 1. AI-powered cybersecurity framework showing ML-based threat detection.

B. *Quick Description of Cybersecurity*

Cybersecurity (Fig. 1), a widely used term, encompasses all tools, techniques, software, policies, and hardware interfaces used to protect the integrity of a network and all information contained in and transmitted through it [4]. On a global scale, a data breach costs an average of $ 4 million, and this amount doubles to $ 8 million in the United States [36-38]. Companies that fail to secure their data, such as social security numbers, are prone to losing their clients and are at the risk of facing lawsuits [33, 39].

C. *Use of Machine Learning in Cybersecurity*

Machine learning plays a pivotal role in cybersecurity for securing sensitive data and information [5]. Machine learning programs analyze network traffic to find and identify patterns and create rules to stop security breaches [17]. These programs use 'clustering' to group similar traffic patterns and detect anomalies, 'classification' to label network requests as benign or malicious, and 'regression' to predict and quantify the likelihood of future threats [21]. These programs can detect and remove viruses or ransomware before they are noticed by humans [20]. For example, the 'Deep Learning' solution for Face ID was developed by Apple so that facial recognition happens on the phone instead of external software to protect the privacy of individuals [3].

IV. IoT SECURITY AND ETHICAL CONSIDERATIONS

Internet of Things devices include all devices we encounter regularly, such as smartwatches, temperature-controlling thermostats, and many more [13]. To make these devices work smoothly for humans, security specialists use a theory known as 'Cyber-Physical Systems Theory'. As shown in Fig. 2, IoT devices such as wearables, thermostats, and cameras form an interconnected ecosystem that, while convenient, significantly expands the cybersecurity attack surface. IoT devices are always at a risk of getting attacked since they always collect and rely on data and thus create multiple opportunities for attackers to exploit sensitive information [23]. And so, to keep this data safe from malicious attackers, companies must ensure high protective measures in their networks [22].

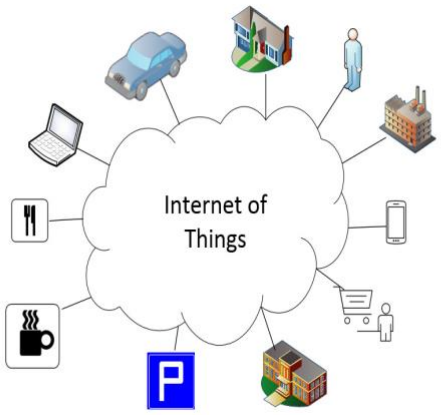

Fig. 2. IoT ecosystem illustrating interconnected smart devices and attack surface.

The principle 'Privacy by Design' supports the development of IoT devices and their associated software with privacy in mind [24][40]. It means building devices keeping privacy as a priority, needing it not be incorporated later on via any patch methods after the device has been built [14]. This demonstrates how safety is a core feature for IoT devices. The point to note is that these devices should not only be safe and secure against external threats but also operate as intended [13]. For example, if a smoke alarm or nuclear power plant fails to work as supposed, it could cause a mass catastrophe.

Along with the safety of these devices, it is also very important to consider the ethics of their use [14]. Ethics is the final principle which is to be considered for IoT devices and it takes an ethical team of engineers to ensure technology is being used for a good cause [7].

V. LEGAL COMPLIANCE AND ETHICAL STANDARDS

With AI so prominently advancing, it is a growing concern that millions of jobs would be replaced by AI in the near future, especially in the manufacturing and software development market [29]. A major question regarding the future of these displaced workers and their source of income arises. But meanwhile, there is an urgent need to address any fatal or illegal consequences that may arise due to the introduction of AI in every field as a decision-making system [6]. An obvious example is the advent of self-driving cars [1]. If such an AI-controlled car accidentally kills someone, it is difficult to decide who is legally responsible for the unfortunate incident. If an accident is caused by a person driving a car himself, it is evident that he will be blamed and punished for it, but an accident caused by a self-driving car raises questions [25]. Another possibility for accidents involving such cars is denial-of-service attacks launched by an attacker [4]. In this scenario, it is the sole duty of legal systems to enact laws, clarifying whether the manufacturer is to be held accountable for failing to develop a more secure network or the attacker [30].

There are endless ethical concerns to consider when talking about artificial intelligence [9]. But some recent research and published papers prove that such ethical concerns are often treated as irrelevant or low-priority by managers and corporate management, as they don't contribute to profit [10]. It is obvious that if upper-level management doesn't prioritize ethical considerations and treat them as the topmost priority, the developers who are writing the AI code would also not prioritize them either [31]. This creates a complete circle of teams who fail to use artificial intelligence in a true, ethical manner. This is why the IEEE suggests that AI should be used ethically across all management levels, whether it is used by developers or leaders [7]. The focus should completely be on ethical use of artificial intelligence. Figure 3 presents a summary of current AI ethics and governance frameworks, illustrating how EU guidelines, the US Executive Order, and IEEE standards collectively balance innovation with safety.

Fig. 3. AI ethics and governance frameworks balancing innovation and safety.

VI. REGULATORY POLICIES BY THE EU

The guidelines by the European Union regarding the use of AI in an ethical manner ensure that AI is safe for all citizens [11]. It provides complete directions on how to deploy and monitor AI so that the implementation is secure for all.

The guideline describes that even though AI should assist humans, humans should always be involved to verify AI findings and accuracy [11]. AI systems must be built such that they are secure and accurate with built-in failsafes to prevent any failures [32]. Furthermore, data secured must be reliable and accessible to authorized persons [30]. Users must be told when they are using AI and an AI system should always explain its decisions to humans in easy and simple words [11]. Developers should always include all groups when developing new AI systems to ensure no bias, helping everyone get acquainted with the working of the system [10]. AI systems should be sustainable, causing no harm to the environment, and there must be a clear person or party responsible for the decisions that an AI system makes [7].

The United States does not have specific laws regarding AI policies, but it has an executive order that provides guidance for government and corporate entities [12]. This order states that AI policies should be clear and easy to understand and should be achieved through constant testing and review [12]. To promote growth in AI industries and to make them accessible, the government will invest in them, helping those most in need [29]. Moreover, the government will also train citizens for this industry for the protection of civil rights [12]. Companies must also protect users, especially in areas like healthcare, education, and housing [2]. They must also use every tool available to protect users' sensitive and personal data and prevent it from being compromised [30]. Lastly, the United States must ensure these ethical principles are taken care of at all times to establish a standard as a leader [12].

VII. RESEARCH GAPS, EMERGING CHALLENGES, AND FUTURE DIRECTIONS

A. Research Gaps

Despite the growing body of literature on AI-driven cybersecurity, several significant research gaps persist. First, the majority of published studies evaluate ML-based intrusion detection and threat classification models in controlled laboratory settings using benchmark datasets such as NSL-KDD or CICIDS. These datasets do not fully reflect the diversity and unpredictability of real-world network traffic, which limits the generalizability of findings. Real-world deployment of such models, particularly in resource-constrained IoT environments, remains largely unaddressed in the current literature [17] [21].

Second, while ethical frameworks such as the EU AI Ethics Guidelines and IEEE Standard 7000-2021 provide high-level principles, there is a notable absence of operationalized, enforceable standards that developers can apply during the software development lifecycle. The gap between policy and practice in ethical AI implementation remains wide, especially for small and medium-sized organizations that lack dedicated AI governance teams [10][7].

Third, the literature on legal accountability for AI-caused harm remains underdeveloped. While incidents such as autonomous vehicle accidents and AI-controlled infrastructure failures raise clear questions of liability, no internationally agreed-upon legal standard currently exists to determine responsibility among manufacturers, developers, and deploying organizations [25][30], [40]. This legal ambiguity poses a risk to both industry adoption and public trust.

B. Emerging Challenges

The rapid advancement of AI introduces several emerging challenges that existing cybersecurity frameworks are not yet equipped to address. One of the most pressing is the rise of adversarial attacks, in which malicious actors deliberately manipulate input data to deceive AI models into making incorrect classifications or predictions. Such attacks pose a direct threat to the reliability of AI-driven intrusion detection systems [9].

The proliferation of deepfakes and AI-generated synthetic media presents another significant challenge, particularly for identity verification systems and the integrity of digital

communications [34]. As generative AI tools become increasingly accessible, the potential for large-scale disinformation campaigns and social engineering attacks grows considerably. Current detection mechanisms lag behind the pace of deepfake generation technology, representing a critical vulnerability.

Additionally, the increasing integration of AI into critical infrastructure including power grids, healthcare systems, and financial networks expands the attack surface and raises the stakes of potential failures. AI systems in these domains must balance automation efficiency with robust fail-safe mechanisms, yet current standards for AI safety in critical infrastructure remain fragmented across jurisdictions [32][12].

C. Future Directions

To address the gaps and challenges identified above, future research should pursue several key directions. First, there is a strong need for the development and adoption of privacy-preserving machine learning techniques, such as federated learning and differential privacy, which enable AI models to be trained across distributed datasets without exposing sensitive user data. These approaches are particularly relevant for cybersecurity applications in healthcare, finance, and government sectors [22].

Second, the establishment of internationally harmonized regulatory frameworks is essential. Current AI governance efforts such as the EU AI Act and the US Executive Order on AI operate largely within their respective jurisdictions, creating compliance inconsistencies for multinational organizations. Future policy work should focus on interoperability between these frameworks and the development of common standards for AI auditing, transparency reporting, and liability assignment [11] [12].

Third, bias detection and fairness auditing in AI-driven cybersecurity systems must receive greater attention. AI models trained on historically biased data may disproportionately flag certain user groups as threats, raising serious civil rights and equity concerns. Research should focus on developing fairness-aware training pipelines and evaluation metrics specific to security classification tasks [10].

Finally, the advancement of Explainable AI (XAI) tailored to cybersecurity contexts is a critical priority. Current AI threat detection systems often function as black boxes, producing decisions that security analysts cannot easily interpret or verify. Developing XAI tools that provide human-understandable explanations for AI-driven security alerts will be essential for building practitioner trust, satisfying regulatory transparency requirements, and enabling faster and more accurate incident response [9].

VIII. CONCLUSION

There is no doubt in the fact that AI offers various benefits, but the dangers and vulnerabilities associated with it cannot be overlooked. AI is also responsible for introducing harmful attacks that threat corporate integrity. Government regulation & ethical companies are necessary for the protection of those at risk. This survey highlights that technological advancement without ethical oversight is dangerous and with the use of cybersecurity in the age of AI, a safe culture's formation is possible. The goal is to find a balance between technological progress and responsible practices that prioritize human safety.

FUNDING STATEMENT

The authors received no specific funding for this study.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

All authors contributed to the conception, literature review, drafting, and critical revision of this manuscript and approved the final version for submission.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

REFERENCES

[1] Tesla, "AI & Robotics." [Online]. Available: https://www.tesla.com/AI. [Accessed: 2024].

[2] R. Al-Shabandar, G. Lightbody, F. Browne, J. Liu, H. Wang, and H. Zheng, "The application of artificial intelligence in financial compliance management," in *Proc. 2019 Int. Conf. Artificial Intelligence and Advanced Manufacturing*, 2019. doi: 10.1145/3358331.3358339.

[3] Apple, "An on-device deep neural network for face detection," *Apple Machine Learning Research*, Nov. 2017. [Online]. Available: https://machinelearning.apple.com/research/face-detection.

[4] D. Ghelani, "Cyber security, cyber threats, implications and future perspectives: A review," *American Journal of Science, Engineering and Technology*, 2022. doi: 10.22541/au.166385207.73483369/v1.

[5] D. Ghillani, "Deep learning and artificial intelligence framework to improve the cyber security," *Authorea Preprints*, 2022. doi: 10.22541/au.166379475.54266021/v1.

[6] H. Lin, Z. Yu, S. Peng, and B. Bian, "Security issues in commercial application of artificial intelligence," in *Proc. 2021 3rd Int. Conf. Artificial Intelligence and Advanced Manufacture*, 2021. doi: 10.1145/3495018.3495359.

[7] J. I. Olszewska and IEEE Systems and Software Engineering Standards Committee, "*IEEE Standard Model Process for Addressing Ethical Concerns During System Design: IEEE Standard 7000-2021*", IEEE, 2021. doi: 10.1109/IEEESTD.2021.9536679.

[8] J. D. Rodríguez-García, J. Moreno-León, M. Román-González, and G. Robles, "Introducing artificial intelligence fundamentals with LearningML: Artificial intelligence made easy," in *Proc. 8th Int. Conf. Technological Ecosystems for Enhancing Multiculturality*, 2021. doi: 10.1145/3434780.3436705.

[9] G. Srivastava et al., "XAI for cybersecurity: State of the art, challenges, open issues and future directions," *arXiv preprint*, arXiv:2206.03585, 2022. doi: 10.48550/arXiv.2206.03585.

[10] M. Agbese, R. Mohanani, A. Khan, and P. Abrahamsson, "Implementing AI ethics: Making sense of the ethical requirements," in *Proc. 27th Int. Conf. Evaluation and Assessment in Software Engineering*, 2023. doi: 10.1145/3593434.3593453.

[11] European Commission, "Ethics guidelines for trustworthy AI," *Shaping Europe's Digital Future*. [Online]. Available: https://digitalstrategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. [Accessed: 2024].

[12] The White House, "Executive order on the safe, secure, and trustworthy development and use of artificial intelligence," *The United States Government*, Oct. 30, 2023. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[13] D. E. Johnson and M. Ketel, "IoT: Application protocols and security," *International Journal of Computer Network and Information Security*, vol. 11, no. 4, pp. 1–8, 2019. doi: 10.5815/ijcnis.2019.04.01.

[14] H. F. Atlam and G. B. Wills, "IoT security, privacy, safety and ethics," in *Internet of Things*, Springer, 2019. doi: 10.1007/978-3-030-18732-3_8.

[15] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[16] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015. doi: 10.1038/nature14539.

[17] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016. doi: 10.1109/COMST.2015.2494502.

[18] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009, pp. 1–6.

[19] P. Louridas and C. Ebert, "Machine learning," *IEEE Software*, vol. 33, no. 5, pp. 110–115, 2016. doi: 10.1109/MS.2016.114.

[20] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019. doi: 10.1109/ACCESS.2019.2895334.

[21] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, 2019. doi: 10.1186/s42400-019-0038-7.

[22] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine learning for security and the internet of things: The good, the bad, and the ugly," *IEEE Access*, vol. 7, pp. 158126–158147, 2019. doi: 10.1109/ACCESS.2019.2948912.

[23] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015. doi: 10.1016/j.comnet.2014.11.008.

[24] A. Cavoukian, "Privacy by design: The 7 foundational principles," *Information and Privacy Commissioner of Ontario, Canada, Tech. Rep.*, 2009.

[25] F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA, USA: Harvard University Press, 2015.

[26] V. Mnih et al., "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, 2015. doi: 10.1038/nature14236.

[27] R. S. Michalski, J. G. Carbonell, and T. M. Mitchell, *Machine Learning: An Artificial Intelligence Approach*. Berlin, Germany: Springer, 2013.

[28] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Networks*, vol. 61, pp. 85–117, 2015. doi: 10.1016/j.neunet.2014.09.003.

[29] K. Schwab, *The Fourth Industrial Revolution*. Geneva, Switzerland: World Economic Forum, 2016.

[30] P. Voigt and A. Von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, Switzerland: Springer, 2017.

[31] M. Brundage et al., "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation," *arXiv preprint arXiv:1802.07228*, 2018.

[32] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issues and challenges," in *Proc. 2010 24th IEEE Int. Conf. Advanced Information Networking and Applications*, 2010, pp. 27–33. doi: 10.1109/AINA.2010.187.

[33] B. Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. New York, NY, USA: W. W. Norton & Company, 2018.

[34] N. Chesney and D. Citron, "Deep fakes: A looming challenge for privacy, democracy, and national security," *California Law Review*, vol. 107, no. 6, pp. 1753–1820, 2019.

[35] J. McCarthy, M. L. Minsky, N. Rochester, and C. E. Shannon, "A proposal for the Dartmouth summer research project on artificial intelligence," *AI Magazine*, vol. 27, no. 4, pp. 12–14, 2006.

[36] A. Turing, "Computing machinery and intelligence," *Mind*, vol. 59, no. 236, pp. 433–460, 1950. doi: 10.1093/mind/LIX.236.433.

[37] D. Silver et al., "Mastering the game of Go with deep neural networks and tree search," *Nature*, vol. 529, no. 7587, pp. 484–489, 2016. doi: 10.1038/nature16961.

[38] IBM Security, "Cost of a data breach report 2023," *IBM Corp.*, Armonk, NY, USA, Tech. Rep., 2023. [Online]. Available: https://www.ibm.com/reports/data-breach.

[39] Sumra, I.A., Hasbullah, H., Ab Manan, J.-L.: Effects of attackers and attacks on availability requirement in vehicular network: a survey. In: International Conference on Computer and Information Sciences (ICCOINS2014), Malaysia, 3–5 June 2014.

[40] Sumra, I.A., Hasbullah, H.B., AbManan, Jl.B. (2015). Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey. In: Laouiti, A., Qayyum, A., Mohamad Saad, M. (eds) Vehicular Ad-hoc Networks for Smart Cities. Advances in Intelligent Systems and Computing, vol 306. Springer.

TABLE I: SUMMARY OF THE PAPER

Topic / Area	**Key Concept**	**Main Benefit / Role**
AI Definition	Flexible, adaptive computing beyond fixed rules	Automates complex tasks; reduces human error
AI vs Traditional Programming	Learns from historical data dynamically	Handles multitasking and pattern recognition
AI Applications	Spam filters, chatbots, video games, finance	Improves daily life and business processes
Supervised Learning	Classification, regression, clustering of data	Identifies and labels cybersecurity threats
Deep Learning	Multi-layer neural networks (e.g., Face ID)	High-accuracy threat detection and recognition
Intrusion Detection	Real-time network traffic analysis	Detects viruses and ransomware automatically
XAI for Cybersecurity	Explainable AI for transparent decisions	Builds trust; explains AI-driven security actions
IoT Devices	Smartwatches, thermostats, cameras, etc.	Convenience expands attack surface
Cyber-Physical Systems	Theory linking digital and physical systems	Ensures safe operation of critical devices
Privacy by Design	Privacy built into devices from the ground up	Eliminates need for post-deployment patches
IoT Attack Risks	Data collection creates exploitation opportunities	Requires strong network protective measures
IEEE Standard 7000-2021	Model for ethical AI system design	Embeds ethics at every management level
EU AI Ethics Guidelines	7 principles: oversight, transparency, fairness, etc.	Ensures safe, trustworthy AI for all EU citizens
US Executive Order (2023)	Federal guidance for safe AI deployment	Protects civil rights; promotes responsible growth
AI Legal Liability	Accountability for AI-caused harm (e.g., self-driving)	Drives need for clear legal responsibility laws
Data Privacy (GDPR)	Regulation of personal data processing in EU	Protects user data; enforces compliance
Job Displacement	AI replacing manufacturing and software roles	Requires workforce retraining and social policy
Malicious Use of AI	Deepfakes, adversarial attacks, cyber weapons	Demands proactive defence and regulation
Denial-of-Service Attacks	Attackers disabling AI-controlled systems	Highlights need for resilient AI infrastructure
Ethical AI Development	Involving all stakeholders; avoiding bias	Produces fair, inclusive, responsible AI systems