Deep AI revolution analysis in cybersecurity

MBAIOSSOUM Bery Leouro*[a], BATOUMA Narkoy[a], FOKOU. K. Géraud[b], ALI Ouchar Cherif[a]
[a]University of Ndjamena, L2MIAS, Chad,
[b]Université de Dschang, École Doctorale, URIFIA, Cameroun

I. Introduction

The integration of Artificial Intelligence (AI) into the domain of cybersecurity represents an undeniable paradigm shift, necessitated by the constant evolution of digital threats and the architectural limitations of conventional defense systems. Faced with an increasingly sophisticated threat landscape, characterized by advanced attack methodologies and an exponential growth in the volume of data requiring protection, traditional security systems, often based on static signatures, have revealed their intrinsic constraints [1].

Traditional security systems, which rely predominantly on signature-based detection, have reached an efficacy ceiling against modern threats, particularly zero-day exploits and highly sophisticated attacks. These methods require prior identification of a threat's fingerprint to recognize it, making them inherently reactive. The sheer volume of security event data—including logs, network telemetry, and alerts generated by Security Information and Event Management (SIEM) solutions—creates a critical dependency on automated analysis. Human security teams are routinely overwhelmed by this data deluge, leading to alert fatigue, inefficient triage, and delayed incident response times.

AI, leveraging advanced capabilities such as Machine Learning (ML), predictive analysis, and rapid decision-making, emerges as a powerful strategic ally to fortify digital defenses. It promises to fundamentally transform how organizations detect, prevent, and respond to cyber threats, enabling a shift from reactive patching to proactive, behavioral defense. AI offers superior predictive modeling and adaptive learning capabilities, which are necessary to identify emerging threats and automate response mechanisms with intelligence [2].

The current integration of AI and security is robust and applied across critical infrastructure globally. In the financial sector, AI is essential for reinforcing fraud detection and regulatory compliance by analyzing vast financial transaction data to identify subtle anomalies and suspicious behaviors at scale [3, 4, 5]. The healthcare industry utilizes AI to protect sensitive patient medical data and secure critical hospital infrastructures against cyberattacks, guaranteeing confidentiality and integrity [6, 7]. Similarly, the energy sector deploys AI to safeguard smart grids from potential intrusions that could disrupt supply [8], while the transportation sector uses it to secure connected vehicle systems and logistics infrastructure against cyber threats, underscoring its essential role in maintaining operational safety and continuity [9, 10]. These examples confirm that AI is now an indispensable component of modern security strategies.

However, The relationship between Artificial Intelligence (AI) and cybersecurity is inherently complex and double-edged. While AI offers undeniable advantages, it also introduces new attack vectors and unprecedented challenges that constitute a significant part of the current threat landscape [11]. On one hand, cybercriminals can now exploit AI to automate and personalize their attacks, such as polymorphic malware or targeted phishing, making detection significantly more difficult [12]. On the other hand, integrating AI into security systems raises fundamental questions. These include the vulnerability of AI models to adversarial attacks [13],

the challenges related to the privacy of data needed to train the algorithms, the potential algorithmic bias, and the critical need for continuous human oversight in the face of the opacity of AI decisions [14, 15].

This article aims to explore in depth the multifaceted impact of AI on data and system security, highlighting both the opportunities it offers to strengthen the defensive posture and the challenges it poses.

This article aims to explore in depth the multifaceted impact of AI on data and system security, highlighting both the opportunities it offers to strengthen the defensive posture and the challenges it poses. To this end, we will adopt the following structure: after this introduction, the next section will detail the methodologies used for this analysis. We will then present the Results and Discussion, structured around the opportunities and advantages of AI in cybersecurity on the one hand, and the challenges and risks associated with AI in cybersecurity on the other. Finally, the article will conclude with a summary of the main findings and perspectives.

II- Methodology

We use a systematic literature review combined with qualitative and conceptual analysis to explore AI's impact on cybersecurity. Our aim is to balance opportunities and challenges using recent research and expert insights.

Data was collected through exhaustive searches in databases like IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus, and Google Scholar. Keywords included "Artificial Intelligence and Cybersecurity," "AI for threat detection," "Adversarial attacks on AI," and their French equivalents. Focus was on the last five years' publications, with foundational works included.

Articles were chosen based on relevance with inclusion criteria covering peer-reviewed journals, conference proceedings, technical reports addressing AI applications in cybersecurity, cybercriminal use of AI, or AI vulnerabilities. Exclusions involved off-topic papers, unreviewed preprints, redundancy, or poor quality. Selection involved initial screening by title and abstract, followed by full reading.

Selected articles underwent thematic analysis on two themes: defensive AI opportunities (intrusion detection, vulnerability analysis, automation) and offensive AI risks (adversarial attacks, malicious AI use, ethical and operational issues). Key arguments, evidence, frameworks, and recommendations were extracted and cross-analyzed to find trends, convergences, divergences, and research gaps.

Limitations include reliance on available publications and rapid evolution of AI and cybersecurity fields, which may quickly outdate findings. Still, this methodology offers a solid base to understand AI-cybersecurity interactions.

III- Results and Discussion

Our study reveals that AI has become a major catalyst for the evolution of cybersecurity, bringing unprecedented capabilities in several key areas. We interess ourselves to AI-Driven Defensive Transformation focusing on opportunities and advanced capabilities, the Adversarial Landscape relating AI-Offensive and systemic Risks and the Ethical, Regulatory, and Governance Challenges.

AI-Driven Defensive Transformation: Opportunities and Advanced Capabilities

AI provides concrete, measurable advantages in reinforcing digital defenses and optimizing security operations, fundamentally altering how organizations manage cyber risk. The value proposition of adopting advanced AI solutions extends from technical prowess to strategic, quantifiable risk reduction tied directly to critical business metrics.

1. Next-Generation Threat Detection: From Signatures to Behavior

AI enables sophisticated detection capabilities that surpass the limitations of traditional signature-based methods.

1.1. Behavioral Anomaly Detection and UEBA

Machine Learning (ML) and Deep Learning (DL) algorithms excel at modeling the statistically "normal" behavior of users and entities within an environment [16, 17, 11]. This capability forms the basis of User and Entity Behavior Analytics (UEBA) solutions [18, 4, 19]. By establishing sophisticated behavioral profiles, AI systems can detect subtle deviations, such as an employee accessing critical files at an unusual time or from an unfamiliar location, even when no specific signature rule has been violated. For instance, solutions like Exabeam Fusion utilize AI to profile activities, flagging minute deviations indicative of compromised credentials or insider threats 1, 17]. This strategic focus shifts detection from merely identifying known malicious files to recognizing suspicious *actions*.

1.2. Predictive Analytics and Automated Threat Intelligence Synthesis

AI is indispensable for analyzing and synthesizing vast volumes of global threat intelligence (TI) sourced from varied domains [20, 21, 15], including the dark web and vulnerability disclosures [22, 23]. This analysis allows AI to move beyond reactive detection to predictive defense, anticipating potential attack vectors and modeling future malicious campaigns. Platforms such as Mandiant Advantage (Google Cloud) utilize AI to provide proactive, contextualized alerts on emerging threats, enabling organizations to fortify defenses before attacks materialize [2].

2. Operational Efficiency and Incident Response Acceleration

AI significantly improves the operational efficacy of security teams, addressing challenges like human resource shortages and alert overload through extensive automation.

2.1. Security Orchestration, Automation, and Response (SOAR): Reducing Time-to-Recovery

Security Orchestration, Automation, and Response (SOAR) platforms are crucial for streamlining incident handling by integrating AI to automate critical, repetitive tasks through integrated workflows. Automation includes the immediate isolation of compromised systems, quarantining of malicious files, and the rapid application of emergency patches.

This automation capability directly impacts the strategic metric known as the Mean Time to Respond (MTTR) [24]. MTTR measures the average time required to achieve system recovery following a failure or cyberattack. AI-driven SOAR dramatically reduces the MTTR, which, in turn, minimizes the financial costs associated with a breach, limits data exposure, and maintains essential business continuity. Tools such as IBM Security QRadar SOAR and Palo Alto Networks Cortex XSOAR exemplify this capacity [25]. The ability to quantify risk reduction using measurable financial and resilience metrics like MTTR allows organizations to move the security conversation from a necessary cost center to a critical risk management function.

2.2. Intelligent Vulnerability Management and Prioritization

AI systems advance beyond simple vulnerability identification by intelligently prioritizing risks. By assessing the likelihood of a vulnerability being actively exploited and calculating the potential impact on an organization's critical assets, AI ensures security teams concentrate their limited human resources on the most relevant and dangerous threats [26]. This functionality serves as a force multiplier, optimizing the deployment of scarce expertise by focusing on threats with the highest probability of immediate exploitation.

3. Harnessing Security Big Data and Adaptive Defense

The ability to process and learn from massive datasets is where AI demonstrates its indispensable nature in modern security operations.

3.1. Advanced Correlation via SIEM and XDR Platforms

Next-generation security platforms require deep AI integration. Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) solutions, such as Google Chronicle Security Operations and Microsoft Sentinel, exploit AI to ingest, normalize, and correlate petabytes of log and telemetry data from diverse sensors. This capability allows for the detection of complex threats dispersed across various systems—endpoints, networks, and cloud environments—that traditional tools could not identify [27].

XDR represents the architectural evolution from Endpoint Detection and Response (EDR), integrating detection and response capabilities across multiple security domains. The pressure on organizations using legacy SIEM platforms, exemplified by the migration faced by QRadar customers toward integrated platforms like Cortex XSIAM, signals a fundamental recognition that comprehensive threat correlation across domains is impractical without native, integrated AI. This market shift validates that the future defense strategy must be platform-centric (XDR), built on a foundation of cross-domain visibility [28].

3.2. Continuous Learning and Adaptive Defense Mechanisms

The core advantage of AI algorithms is their capacity for continuous learning and adaptation to the evolving Tactics, Techniques, and Procedures (TTPs) employed by attackers. This continuous adaptation ensures that defensive measures remain effective and relevant in a perpetually dynamic threat landscape [28].

Table 1 summarizes the critical role of AI within modern security operations platforms:

Table 1: AI Integration and Impact Across Core Security Operations Platforms

Platform Type	**Primary Function**	**AI/ML Role in Modern Implementations**	**Key Metric Impacted (Improvement)**
Security Information and Event Management (SIEM)	Log aggregation, correlation, and real-time monitoring.	Big Data analysis, advanced threat scoring, anomaly detection.	Mean Time to Detect (MTTD)
Security Orchestration, Automation, and Response (SOAR) [1]	Incident workflow automation, playbook execution.	Prioritization, automated response actions (e.g., quarantine, remediation).	Mean Time to Respond (MTTR) [3]

Extended Detection and Response (XDR) [1]	Cross-domain threat visibility (Endpoint, Network, Cloud).	Advanced threat context correlation, behavioral modeling, deep learning analysis.	Containment Speed (MTTC) / System Resilience

The Adversarial Landscape: AI-Offensive and Systemic Risks

The relationship between AI and cybersecurity is inherently dual-use; the same power that fortifies defenses can be weaponized by adversaries. This establishes a true digital arms race, where offensive capabilities leverage automation and personalization to unprecedented degrees.

1. Exploitation of AI by Cybercriminals (AI-Offensive)

Adversaries are now integrating AI to scale and specialize their attacks, increasing both the velocity and sophistication of cyber campaigns.

1.1. Automated Malware Evolution: The Threat of Polymorphic Attacks

AI facilitates the creation of polymorphic malware, malicious software that continuously changes its code and signature with every replication, often utilizing an integrated mutation engine. This dynamic mutation allows the malware to bypass classic, signature-based antivirus solutions, confirming the necessity for defenses focused on behavioral analysis [12].

1.2. Social Engineering at Scale: Deepfakes and Hyper-Personalized Phishing

Generative AI enables the creation of highly convincing deepfakes—realistic audio or video impersonations—which are then used in sophisticated fraud schemes. CEO Fraud (also known as Whaling) is a targeted phishing attack where criminals impersonate high-level executives to manipulate employees into divulging sensitive information or initiating fraudulent financial transactions. The use of AI makes these impersonations hyper-realistic and difficult for humans to detect [29, 30]..

1.3. Large Language Models (LLMs) and Malicious Code Generation

Large Language Models (LLMs), including specialized coding models like GPT-4o-mini, CodeLlama, LLaMA 3.1, CodeT5, and Starcoder [33], can be leveraged by attackers. These tools can generate new, complex, and potentially obfuscated assembly code, significantly lowering the technical skill floor required for advanced cybercrime. This democratization of sophisticated attack generation expands the pool of potential threat actors and accelerates the rate at which novel, evasive attack tools can be created and deployed[34].

2. Direct Attacks Against Defensive AI Models (Adversarial ML)

A significant risk involves direct attacks against the defensive AI models themselves, designed to compromise the system's integrity and reliability. Adversarial AI encompasses techniques that exploit vulnerabilities in the model’s underlying logic through deceptive inputs [34].

2.1. Evasion Attacks (Targeting Inference)

Evasion attacks occur during the inference phase, where attackers introduce subtle, often imperceptible alterations, known as "adversarial examples," into the input data to manipulate the trained model into misclassification. For example, a minor alteration to a file might cause a malware classifier to deem it benign. Adversarial attacks seek to undermine not just the model's functionality but the inherent trust in its output [29].

2.2. Poisoning Attacks (Targeting Training)

Poisoning attacks target the foundational integrity of the model by injecting corrupted or misleading data into the training dataset.[15] This malicious data inclusion undermines the model's overall reliability and introduces biases into its future decision-making. If security analysts cannot trust the AI's classification due to the known risk of adversarial manipulation, the time savings afforded by automation are lost, and human error is reintroduced into the critical security loop [30, 35].

3. Technical and Operational Challenges

The implementation of complex AI defense inherently introduces operational and technical vulnerabilities.

3.1. The Accuracy Paradox: Managing False Positives and False Negatives

The inherent difficulty in calibrating AI models leads to the persistent challenge of managing false positives (excessive false alarms), which contributes to "alert fatigue" among security personnel. Conversely, the occurrence of false negatives (real threats that go undetected) can lead to catastrophic security breaches. Achieving the optimal balance between model sensitivity and precision remains a critical operational challenge [36].

3.2. System Complexity and Reliability

The sophistication required for AI model maintenance, data quality assurance, and integration with existing systems introduces new and complex points of failure. The asymmetry in the AI arms race is pronounced: offensive AI techniques grant the attacker unprecedented scale and personalization, while defenders remain constrained by the high cost of robust testing, compliance, and explainability [35]. This disparity suggests that the rate of new threat emergence will continue to outpace manual defensive capabilities, necessitating automated, shared threat intelligence to maintain parity.

Ethical, Regulatory, and Governance Challenges

The widespread adoption of AI in security introduces profound ethical and legal complexities that directly impact public trust, accountability, and regulatory compliance.

1. The Opacity Problem: Explaining AI Decisions (XAI and the "Black Box")

1.1. The Black Box Limitation

Many advanced Deep Learning algorithms function as "black boxes"; their decisions are the result of complex processes that are difficult or impossible for human architects to interpret or explain. This lack of explicability is a major impediment in a field where the traceability and justification of security actions are vital for auditing, regulatory adherence, and rapid incident resolution[35].

1.2. XAI as an Auditability and Compliance Requirement

Explainable AI (XAI) addresses this by implementing specific techniques to ensure transparency and traceability. XAI is critical not only for compliance but also for system hardening. If a model is opaque, debugging and correcting the source of an adversarial attack becomes impossible. By forcing explainability, XAI enables security teams to trace why a threat was missed or why a system was quarantined, allowing for the rapid identification of the input features that led to misclassification and subsequent patching of the model's logic [36].

1.3. Legal Mandate (GDPR)

The need for XAI is codified in legal frameworks, notably the EU's General Data Protection Regulation (GDPR), which grants individuals the "Right to an Explanation" for decisions significantly affecting them that are made by automated systems. Explainability, facilitated by tools like LIME (Local Interpretable Model-Agnostic Explanations), is therefore a legal necessity, as failure to implement transparent processes creates significant compliance and legal risk [37].

2. Data Privacy, Compliance, and Algorithmic Bias

The development and deployment of robust AI security systems are tightly coupled with sensitive data requirements, raising crucial ethical and compliance concerns.

2.1. Confidentiality of Data and Regulatory Compliance

Effective training of high-performing AI models necessitates access to enormous volumes of sensitive network and often personalized data. This raises major security concerns regarding data handling and compliance with strict privacy regulations like GDPR. The conflict between the need for extensive data to train models and the mandates for data privacy compels innovation toward privacy-preserving methodologies, such as federated learning, to protect sensitive information during the AI training process [6].

2.2. Algorithmic Bias and Equity Concerns

If the datasets used to train security AI systems reflect or embed existing historical or systemic biases, the resulting algorithms will reproduce and potentially amplify these prejudices. In the security context, this can lead to disproportionate surveillance or inequitable security decisions applied to specific user groups. Furthermore, algorithmic bias presents a systemic security vulnerability: an attacker who identifies that an organization's AI is biased against certain network behaviors may deliberately tailor their actions to mimic behaviors that the AI has learned to ignore, creating an easily exploitable blind spot [38].

3. Legal Accountability and Governance Frameworks

The deployment of autonomous AI systems introduces uncertainty regarding legal responsibility and oversight.

3.1. Defining Legal Responsibility

The critical question of legal liability following a catastrophic failure of an autonomous, AI-driven security system remains largely unresolved. This uncertainty about legal accountability can impede the full adoption of fully automated AI solutions in high-sensitivity operational environments [39, 40].

3.2. The Need for Multidisciplinary Governance

Achieving a highly resilient digital infrastructure depends on establishing sophisticated governance frameworks. Effective deployment mandates collaboration among technologists, legal experts, ethicists, and government policymakers to develop harmonized frameworks for testing, certification, and assigning accountability for AI systems.

V. Conclusion

The integration of AI into cybersecurity represents a transformative but highly complex partnership. AI offers essential capabilities for proactive threat detection, predictive analysis, and operational automation, leading to measurable efficiency gains, particularly in reducing the Mean Time to Respond (MTTR). However, AI simultaneously introduces new systemic vulnerabilities, including sophisticated AI-Offensive techniques utilized by adversaries (polymorphic malware, deepfake fraud) and the risk of adversarial attacks launched directly against defensive ML models.

The analysis confirms that strategic investment must move beyond traditional perimeter defense to focus on the integrity, reliability, and trustworthiness of the AI models themselves. The challenges associated with "black box" model opacity, the ethical implications of data privacy and algorithmic bias, and the unresolved issues of legal accountability present significant barriers to responsible, large-scale deployment.

The critical transition from signature-based defenses to behavioral, AI-driven platforms (XDR and SOAR architectures) must accelerate, driven by the measurable efficiency gains in response time and complex threat correlation. To successfully navigate this complex landscape, organizations must strategically address the inherent vulnerabilities introduced by AI, viewing the integrity of their AI models as a primary security pillar.

To realize AI's full defensive potential while mitigating its intrinsic risks, dedicated research efforts must focus on resolving current technological and ethical limitations. Key research directions include:

- Developing Adversarially Robust Models: Research must prioritize designing AI algorithms that are inherently resilient to evasion and poisoning attacks, building upon initial defensive concepts and testing frameworks developed for adversarial machine learning, such as IBM’s CounterFit.
- Enhancing XAI Techniques for Security Applications: Improving the explicability and interpretability of complex Deep Learning models is essential to ensure regulatory compliance, enhance auditability during security incidents, and maintain end-user trust in automated security decisions.[17]
- Advancing Privacy-Preserving AI: Scaling up privacy-centric methods, such as federated learning, is crucial to enable massive-scale threat intelligence collaboration across organizations without compromising sensitive, regulation-protected data.

Achieving a highly resilient digital infrastructure depends fundamentally on a comprehensive strategy that embraces multidisciplinary collaboration. The collective effort of technology developers, legal authorities, ethicists, and policymakers to establish clear ethical standards and effective governance frameworks is essential for realizing AI's full defensive potential while managing its intrinsic risks to society and digital infrastructure.

Références

1- Ferrag, M. A., et al. (2023). Artificial Intelligence for Zero-Day Attack Detection in IoT Networks. IEEE Internet of Things Journal, 10(15), 13320-13333.
2- Shu, S., et al. (2024). AI-powered proactive threat intelligence for enhanced cybersecurity. International Journal of Computer Security, 8(1), 12-28.
3- EL HADDADI, M. (2025). Intelligence Artificielle et FinTechs: Défis et Opportunités pour le secteur financier au Maroc. International Journal of Accounting Finance Auditing Management and Economics, 6(4), 238-256.

4- Khaliq, S., Tariq, Z. U. A., & Masood, A. (2020, October). Role of user and entity behavior analytics in detecting insider attacks. In 2020 International Conference on Cyber Warfare and Security (ICCWS) (pp. 1-6). IEEE.
5- EE - Shashanka, M., Shen, M. Y., & Wang, J. (2016, December). User and entity behavior analytics for enterprise security. In 2016 IEEE International Conference on Big Data (Big Data) (pp. 1867-1874). IEEE.
6- De Saint-Affrique, D. (2022). Intelligence artificielle et médecine: quelles règles éthiques et juridiques pour une IA responsable?. Médecine & Droit, 2022(172), 5-7.
7- Callegarin, D., & Callier, P. (2021). Enjeux du déploiement de l'intelligence artificielle en santé. Actualités Pharmaceutiques, 60(611), 21-24.
8- Fabry, N., & Zeghni, S. (2022). Gouvernance de la smart city et cybersécurité. Cahiers de la sécurité et de la justice, 56(3), 18-26.
9- HANA, M. (2025). Logistique 4.0: Innovations et Stratégies pour une Chaîne d'Approvisionnement Connectée. Revue Internationale de la Recherche Scientifique (Revue-IRS), 3(2), 1400-1413.
10- Paché, G. (2024). Vers une logistique augmentée: le métavers,«nouvelle frontière» du management des flux. Management & Datascience, 8(3).
11- Joseph, A. (2024). AI-driven cloud security: Proactive defense against evolving cyber threats. International Journal of Computer and Information Engineering, 18(5), 261-265.
12- Kim, Y., Hong, S. Y., Park, S., & Kim, H. K. (2025). Reinforcement Learning-Based Generative Security Framework for Host Intrusion Detection. IEEE Access.
13- Liu, Y., & Wang, Q. (2023). Adversarial attacks and defenses in machine learning for cybersecurity. Computers & Security, 125, 103001.
14- [14] Jennifer Tang, Tiffany Saade et Steve Kelly. 2024. The implications of artificial intelligence in cybersecurity : shift- ing the offense-defense balance. https:// securityandtechnology.org/wp-content/uploads/2024/10/The-Implications-of-Artifi- cial Intelligence-in-Cybersecurity.pdf*
15- Haass, J. C. (2022, September). Cyber threat intelligence and machine learning. In 2022 fourth international conference on transdisciplinary AI (TransAI) (pp. 156-159). IEEE.
16- Ahmed, T., Oreshkin, B., & Coates, M. (2007, April). Machine learning approaches to network anomaly detection. In Proceedings of the 2nd USENIX workshop on Tackling computer systems problems with machine learning techniques (pp. 1-6). USENIX Association.
17- Islam, M. A. (2023). Application of artificial intelligence and machine learning in security operations center (Doctoral dissertation, Middle Georgia State University).
18- Khan, M. Z. A., Khan, M. M., & Arshad, J. (2022, December). Anomaly detection and enterprise security using user and entity behavior analytics (UEBA). In 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS) (pp. 1-9). IEEE.
19- EE - Shashanka, M., Shen, M. Y., & Wang, J. (2016, December). User and entity behavior analytics for enterprise security. In 2016 IEEE International Conference on Big Data (Big Data) (pp. 1867-1874). IEEE.
20- Lee, M. (2023). Cyber threat intelligence. John Wiley & Sons.
21- Zhang, S., Chen, P., Bai, G., Wang, S., Zhang, M., Li, S., & Zhao, C. (2022). An automatic assessment method of cyber threat intelligence combined with ATT&CK matrix. Wireless Communications and Mobile Computing, 2022(1), 7875910.
22- Bergman, J., & Popov, O. B. (2023). Exploring dark web crawlers: a systematic literature review of dark web crawlers and their implementation. IEEE Access, 11, 35914-35933.

23- Staley, B., & Montasari, R. (2022). A survey of challenges posed by the dark web. In Artificial intelligence in cyber security: impact and implications: security challenges, technical and ethical issues, forensic investigative challenges (pp. 203-213). Cham: Springer International Publishing.
24- Aramide, O. O. (2025). AI-Driven Automated Incident Response and Remediation in Networks. International Journal of Technology, Management and Humanities, 11(02), 1-9.
25- Obuse, E., Etim, E. D., Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Babatunde, L. A. (2023). AI-powered incident response automation in critical infrastructure protection. International Journal of Advanced Multidisciplinary Research Studies, 3(1), 1156-1171.
26- Chen, L., Wang, Y., & Li, Z. (2023). AI-driven predictive analytics for cybersecurity threat intelligence. Journal of Cybersecurity Research, 5(2), 45-60.
27- Pissanidis, D. L., & Demertzis, K. (2024). Integrating AI/ML in cybersecurity: An analysis of open XDR technology and its application in intrusion detection and system log management.
28- Blangeois, M. (2023). IA générative: révolution ou menace pour les entreprises de services du numérique?. Management & Data Science.
29- Romero-Moreno, F. (2024). Deepfake Fraud Detection: Safeguarding Trust in Generative Ai. Available at SSRN 5031627.
30- Islam, M. R. (2024). Generative AI, cybersecurity, and ethics. John Wiley & Sons.
31- Paidy, P. (2023). Adaptive Application Security Testing With AI Automation. International Journal of AI, BigData, Computational and Management Studies, 4(1), 55-63.
32- Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., ... & Li, K. (2021). Artificial intelligence security: Threats and countermeasures. ACM Computing Surveys (CSUR), 55(1), 1-36.
33- B. L. Mbaiossoum; I. D. A. Mahamat ; N. Batouma, L. Dionlar , B. B. Apollinaire, I. O. Adam, (2025). How to Choose the Best AI LLM: A Guide to Navigating the Diversity of Models. Journal of Information Systems Engineering and Management, 10(34s), DOI : 10.52783/jisem.v10i34s.5790.
34- Mohseni, S., Mohammadi, S., Tilwani, D., Saxena, Y., Ndawula, G. K., Vema, S., Raff, E., & Gaur, M. (2025). Can LLMs Obfuscate Code? A Systematic Analysis of Large Language Models into Assembly Code Obfuscation. Proceedings of the AAAI Conference on Artificial Intelligence, 39(23), 24893-24901. https://doi.org/10.1609/aaai.v39i23.34672
35- Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on Explainable Artificial Intelligence (XAI). IEEE Access, 6, 52138-52160.
36- Nendaz, M. R., & Perrier, A. (2004). Sensibilité, spécificité, valeur prédictive positive et valeur prédictive négative d'un test diagnostique. Revue des maladies respiratoires, 21(2), 390-393.
37- Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). Advances and open problems in federated learning. Foundations and trends® in machine learning, 14(1–2), 1-210.
38- O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown.
39- Ndiaye, M., & Sarr, M. (2024). L'éthique et la gouvernance de l'IA et ses applications au Sénégal. Communication, technologies et développement, (15).
40- Salles, D. (2009). Environnement: la gouvernance par la responsabilité?. VertigO-la revue électronique en sciences de l'environnement, (Hors série 6).