Shadow AI and the Expanding Attack Surface: Risks, Threats, and Countermeasures

Deepak Puthal*, Niranjan Kumar Ray†, and Saraju P. Mohanty‡
* College of IT, United Arab Emirates University, Al Ain, UAE
† School of Computer Engineering, KIIT University, Bhubaneswar, India
‡ Department of Computer Science and Engineering, University of North Texas, Denton, Texas, USA
Email: deepak.puthal@uaeu.ac.ae, niranjan.rayfcs@kiit.ac.in, saraju.mohanty@unt.edu

***Abstract*—The rise of unsanctioned AI models, or Shadow AI, is becoming an information security and governance nightmare. Shadow AI increases attack surfaces without limits and creates uncontrolled systemic risks. Shadow AI models even under governance perimeters can still lead to substantive risks, such as leaking sensitive, ungoverned streams of data and data governance absence. Shadow data leak models can leak sensitive business information to unauthorized recipients, while shadow backdoor models could be engineered to facilitate adversarial attacks. This paper is outlined through a suggested strategic countermeasure of automated AI discovery, inventory, and an advanced governance policy. The most advanced approach, Zero Trust Architecture, views all AI assets as potential threats and requires constant validation and access control of each asset. This approach is demonstrated through a collection of case studies at the end of the section. These studies exemplify how the trustworthiness of AI can be assured.**

***Index Terms*—Pervasive AI, Machine Learning, Edge-AI, Tiny-ML, Security, Privacy and Scalability.**

I. Introduction

The rapid evolution of of new artificial intelligence (AI) and machine learning (ML) tools is changing business paradigms. These new tools promise greater efficiency and innovation. These tools also create new opportunities for competitive advantage. The tools do not seem to be restricted to data science specialists since they are being used by other employees in other divisions like marketing, human resources, and even engineering [1]. This kind of "democratization of technology" however is giving rise to a new phenomenon, named Shadow AI. Shadow AI in a way is a continuation of "Shadow IT" – the deployments of software and hardware infrastructures that central IT does not manage. Shadow AI is the utilization of AI tools without approval, supervision, or documentation [2]. The ungoverned, unmonitored, and unapproved use of Shadow AI poses acute security threats and gaps in the governance of an organization. This paper aims to identify the nature of risks and threats in Shadow AI, and also offer countermeasures that security professionals can employ in their attempts to regain control. The system diagram of the threat landscape and mitigation framework is as shown in Figure 1

A. The AI Revolution

The use of ML in modern enterprises is fundamentally changing as a result of readily available open-source technologies, including PyTorch, TensorFlow, and scikit-learn. Non-experts, including data analysts and engineers, are able to quickly prototype and deploy sophisticated models as a result of ready-made models sits in repositories such as the Hugging Face Hub and the ease of use provided by containerize technologies. This allows them to spin-up inference engines. This technical dexterity allows the circumvention of formal Machine-Learning-Operations (MLOps) frameworks to configure data pipelines and deploy model endpoints. What tends to happen in such cases is that the grassroots innovation occurring is independent from the industry-construct CI/CD pipelines, automated security scans, code formal checks, and even the verification frameworks. What is even more surprising is that the primary drive from swift deployment ignores the primary requirement of strong security, system validation, and other principles, leading to fragmented, undocumented, and scattered portfolios of AI [3].

B. Defining the Shadow AI Problem

The fundamental attributes of Shadow AI is the lack of centralized technical control. Shadow AI is represented by failure to follow primary data governance workflows, the absence of data model integration, and absence of versioning control over training datasets, the model, and metadata. This has observable technical underpinnings, such as the running of models in shadow IT via personal or departmental accounts without oversight, their reliance on unsupported software libraries which possess Common Vulnerabilities and Exposures (CVEs), and, perhaps the most serious, the absence of model management for essential logging of the model's inputs, outputs, and performance metrics. These gaps present a direct challenge to the CIA triad of confidentiality, integrity, and availability. With no model of record, data processing and model usage is a data handle tracing appliance whereby sensitive data is exposed to cross border data flows and gross, unmanaged violations of model governance. The integrity of the models is left unverified which presents a source of unconstrained, and unpredictably negative or purposeful behavior [4] [5].

C. Attack Surface in the Modern Enterprise

Shadow AI shows how the technology used by an organization can trap attackers in a variety of ways. Each unattached AI model, pipeline, or endpoint contains a new area insufficiently protected and unregistered by the organization.

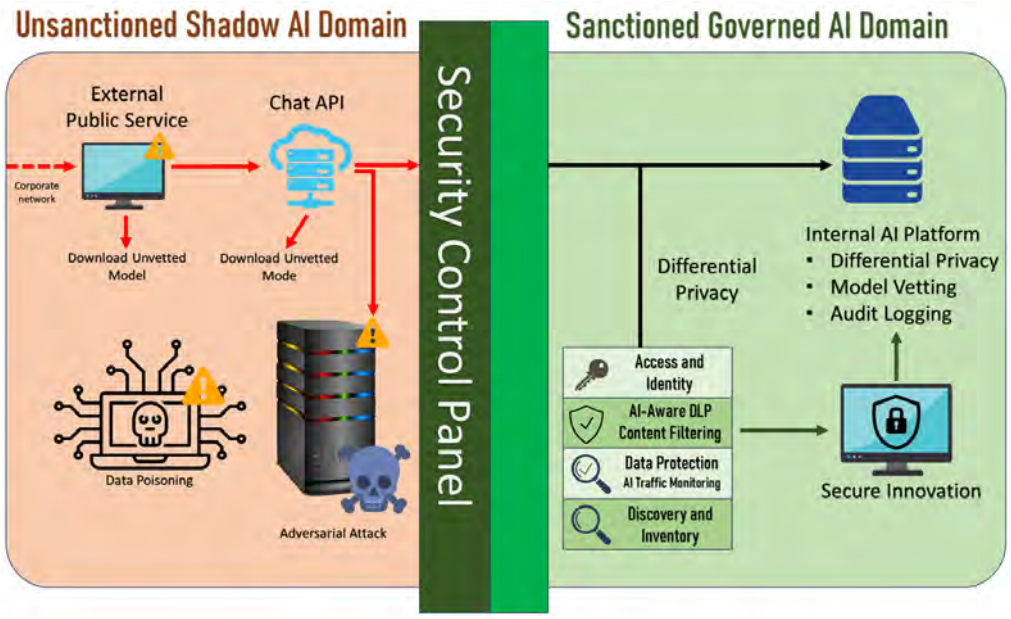

Fig. 1. Shadow AI Threat Landscape and Mitigation Framework

These systems are "soft targets" that have no correlation in the organization's security information and event management (SIEM) and endpoint detection and response (EDR) systems. The attacker needs only to exploit these soft targets to gain the attacker's control [6]. For instance, an image recognition model's API endpoint and exfiltration of sensitive data can trigger vulnerable data pipelines. The unregulated placement of AI with poor control separates the organization's internal perimeter, turning it into a web of delicate and soft systems traditional tools can't scan or protect [7] [8].

D. Article Roadmap

This paper explores potential risks and vulnerabilities that position Shadow AI as a real threat including use cases that can be exploited such as data poisoning, model poisoning, and adversarial attacks. This paper will then lay out a thoughtfully designed set of countermeasures that combine systems of counter automated AI asset discovery, model life cycle management and critical primary shifts in policies and organizational culture. Further, it will examine specific cases of Shadow AI to demonstrate its technical impacts and proactive governance to serve as a motivational model of the need to control more Shadow AI. This paper will finally provide a forecast of the anticipated AI security trend to shift the vision of security practitioners toward more integrated governance and the concept of "AI in the dark" as a defensive design principle.

II. The Risks and Threats of Shadow AI

The unsanctioned advanced AI model deployments pose a range of potential and actual operational failures and risks that can challenge organizational security and compliance. Compared to software, AI models have a distinct attack surface that is a function of the underlying data, the AI algorithms, and the model's operational lifecycle. These risks also transcend traditional problems of access control. Additional concerns include data integrity, model robustness, and the very basis of corporate governance [9].

A. Data Privacy

Having shadows of AI technologies carries major risk to data privacy. Models that are developed on a construction of no formal security are often trained on data sets that have not been de-identified, tokenized, or encrypted. This allows for personally identifiable information (PII), protected health information (PHI), or sensitive data to be processed in the open. The unsanctioned or unapproved use of third-party AI positioned on the cloud carries the serious risk of breaking data residency and data sovereignty laws as the sensitive information is likely moved to and stored in places below the standards of the sensitive data. Besides, these models have no data logging or access logging and, therefore, determining the degree of compliance with regulations like GDPR's "right to be forgotten" or CCPA's consumer data rights is impossible [10]. The compliance officer has no way of showing compliance with data access controls. There is also no way to evaluate the degree to which the organization utilized data for the AI models. The organization is therefore exposed to major legal and financial penalties [11] [12].

B. Intellectual Property

There are distinct threats that stem from deploying uncontrolled AI models, from IP theft to unauthorized data breach. The proprietary data situated within proprietary datasets, from financial documents to email exchanges, can be breaches quite easily if reconstructive models are employed with minimum

TABLE I
SHADOW AI RISKS & THREATS.

Threat Category	Core Risk	Technical Impact
Data Privacy Violations	Uncontrolled data processing	PII exposure, regulatory non-compliance
IP Theft & Exfiltration	Unmonitored data leakage	Model inversion, unauthorized data transfer
Vulnerabilities & Backdoors	Unpatched software & libraries	Remote code execution, hidden access
Adversarial AI Attacks	Subversion of model logic	Data poisoning, model evasion

cyber protections. When AI models are deployed on unprotected cyber infrastructures, there is a distinct possibility that bad actors may employ untethered exploits to obtain access to critical AI training datasets. However, situations that involve model-inversion attacks may be of a greater threat, where an attacker may try to use the model as an oracle, thus extracting sensitive information from the dereferenced training data. Data exfiltration can be safely described as a covert operation. An example to demonstrate this point would be how outputs generated by the AI model may be seen as a direct prompt, sensitive data may be manipulated to be showcased as the model, ever so cleverly, leaking proprietary information without being tethered to the core data [2]. In this case, the model is the data extraction tool, and the resulting model output is the disguised exfiltration method.

C. Security Vulnerabilities

Shadow AI capabilities carry associated security risks that can be weaponized. Different shadow models and their dependencies frequently and to a greater degree than approved enterprise software, are overlooked during the patch and vulnerability scanning cycles. This leaves them exposed to the known CVEs in their libraries and frameworks. In addition, during these lapses, unchecked models may include self-contained backdoors. A hostile internal member or a compromised external vendor can stealthily deploy C2 (command and control) systems, models that are corrupted, or triggers that are damaged and designed to be 'poisoned' during C2 systems to control networked devices. This backdoor can be configured to respond to specified conditions such as certain triggers or inputs, and under such circumstances, an attacker can gain 'privileged' access' to the network, establish 'persistence' and utilize other hostile means [13]. Operating these models are devoid of an organization's security observability tools, and as a result, any malicious behavior that is perpetrated is likely to remain uncovered until the situation runs amok.

D. Adversarial AI Attacks

Besides the classic security concerns, Shadow AI has specific vulnerabilities to Adversarial AI attacks, which pivot on the ML model's intrinsic characteristics and functionalities. One critical attack vector is the data poisoning attack in which an adversarial character attempts to poison the training pipeline and modify the model's behavior by injecting false or corrupted data. A ghost in the network could poison the shadow AI model's data stream and it is plausible that this data is used for network traffic analysis [14]. Therefore, it is possible to cause the model to misclassify hostile traffic as benign. Another formidable attack is model evasion in which an adversary is able to gain access by crafting a specific sort of malevolent input that is targeted for misclassification by the model. The system architecture of threat landscape and mitigation framework is as shown in Figure 1. In this manner, an adversarial user can circumvent the AI-controlled security. Shadow AI's absence of stringent monitoring and orthodox validation exposes these frameworks to these highly sophisticated attacks. Although the model's outputs cannot be authenticated, the absence of core validation concerning the model's deficiencies is perhaps the gravest concern. The Shadow AI core risks and impacts are classified as in Table I.

III. FRAMEWORK FOR COUNTERMEASURES

The mitigation of the possible risks from Shadow AI 's requires the deep and multi-sided governance combined with automated system of security. Transforming the security from a reactive Incident Response approach to a proactive Risk Management approach is the goal. Doing so will achieve the desired outcomes if all AI assets, regardless of approval status, work seamlessly with a security framework. This framework must address every aspect of AI model, their creation. deploying, then supervising and even till their possible withdrawal from the system, with the necessary security and compliance as the first priority. The architecture diagram of the defense architecture against the Shadow AI is shown in Figure 2.

A. AI Governance and Policy

Governance pertaining to AI is how the first tier of a security strategy is defined, effective as the base layer of any security strategy. From a technical viewpoint, an effective governance AI strategy translates into the policies that govern Acceptable use (AU), data handling, model validation, and the deployment of an AI system being made policy 'machine readable'. A pivotal tier is the Centralized AI Model Registry defined as a single source of truth for all the models in an enterprise. This model manifesto should capture the model within an enterprise's domain, its 'lineage', the 'training data' assets, the 'dependencies', and the 'intended use'. The policy system should be able to 'audit' the deployment of the model on the policy 'walled' objectives which checks the model for security and compliance. It is paramount that these policies within the policy system should be executed within closed loop automated pipelines or integrated security policy tools to which the users do not have any manual toggle controls that can forcibly override these processes [15].

TABLE II
A STRATEGIC FRAMEWORK FOR COUNTERMEASURES.

Countermeasure	Core Strategy	Technical Outcome
Governance & Policy	Centralized AI Model Registry	Auditable trail, automated compliance
Discovery & Inventory	Automated asset detection	Comprehensive visibility, real-time flagging
Behavioral & Cultural	Secure innovation platforms	Channeling unsanctioned models
Zero-Trust Integration	Continuous verification	Granular access control, threat isolation

B. Technological Countermeasures

Policy execution requires complete understanding of all AI assets within an organization. For this purpose, an organization must deploy and integrate a robust AI asset discovery and inventory system. These systems use network traffic, endpoint detection and response systems, cloud service provider application programming interfaces, and other systems to locate training and inference activities of certain models. This involves the ability to monitor API calls to ML frameworks like TensorFlow and PyTorch, detect certain model training, monitor binary data transfers, and identify specific models and proprietary files and binaries within endpoint devices. All of the model discovery should automatically flow into a central AI model registry, and unsanctioned models should be flagged for prompt action. This technology captures even the most brief instances of shadow AI, permitting complete visibility and better governance of the organization's AI activities.

C. Behavioral and Cultural Countermeasures

The tools required to maintain the framework can indeed be enabled by technology but a secure culture is required to sustain the tools. To move the culture from 'security versus innovation' to 'secure innovation' requires a mindset shift. This is achieved in practice by offering developers secure, pre-approved and frictionless platforms for AI experimentation. These platforms, typically made available in the form of boxes, secure sandboxes or isolated development environments, are security engineered with security policies, approved libraries and automated SC systems. Organizations can incentivize shift from a 'bring your own model' culture to a 'use our secure environment' culture by offering a secure path of least resistance. This approach redirects unauthorized innovation to secure and controlled innovation pathways and thereby lowers the benefits of going outside the framework [16].

D. Integrating Shadow AI into a Zero-Trust Architecture

The integration of AI capabilities into a zero-trust security framework is the single most effective countermeasure. In this framework, no AI model, be it sanctioned or shadow, is assumed to be trusted. Each model and its accompanying data inputs and outputs must be continuously verified. Access to data, computing resources, and other network services must be granted according to data and network resource access authentication controls. This implies that sophisticated identity and access management (IAM) systems need to be applied to AI models as separating the model from IAM systems will not scale, thus treating the AI models as first class citizens in the IAM ecosystem. Model shadowing is also important, in that centralized models are kept unsanctioned to prevent unsanctioned models from lateral movement [17]. Continuous and real-time threat detection and neutralization is accomplished by monitoring model behavior for anomalies such as unsanctioned network activity, obtaining or generating data outputs outside of the expected inputs, or requesting data beyond the sanctioned scope. Through imposition of stringent and granular verification and access control, the zero-trust model will be capable of mitigating the effects of a shadow AI instance, regardless of the initial detection failure [18]. The strategic countermeasure and technical outcome are listed in Table II.

IV. CASE STUDIES AND REAL-WORLD EXAMPLES

To fully address the risks associated with Shadow AI, it is mostly useful to conduct a narrowed analysis on a few practical examples [14]. The subsequent, anonymized case studies highlight the risks posed by unattended AI resources, as well as the value associated with the implementation of a proactive security infrastructure.

A. Data Privacy Breach

A large financial services corporation employed a cross-functional data science team to construct an unsupervised learning model designed to capture and predict various customer transaction activity and provide covert and strategic business intelligence. The model was trained on a replicated dataset derived from a production database containing raw PII data that was not properly de-identified due to a lack of proper oversight from governance and cybersecurity teams. The developed model, which was trained on a data-devoid PII production database, was trained on a development server modelously separated from the corporate security perimeter and was left exposed to an open API endpoint protected by a weak cryptographic key. This was discovered and exploited by an adversary during reconnaissance as part of a broader surveillance program. The adversary successfully performed a model inversion attack which involved constructing new PII data based on user-provided parameters. This ethically concerning data privacy breach, which was unauthorized and properly monetized, was discovered by an internal compliance audit with a significant time difference from the reinitialization performed by the adversary. This emphasizes the lack of oversight concerning the use of this model and access to the ungoverned AI asset.

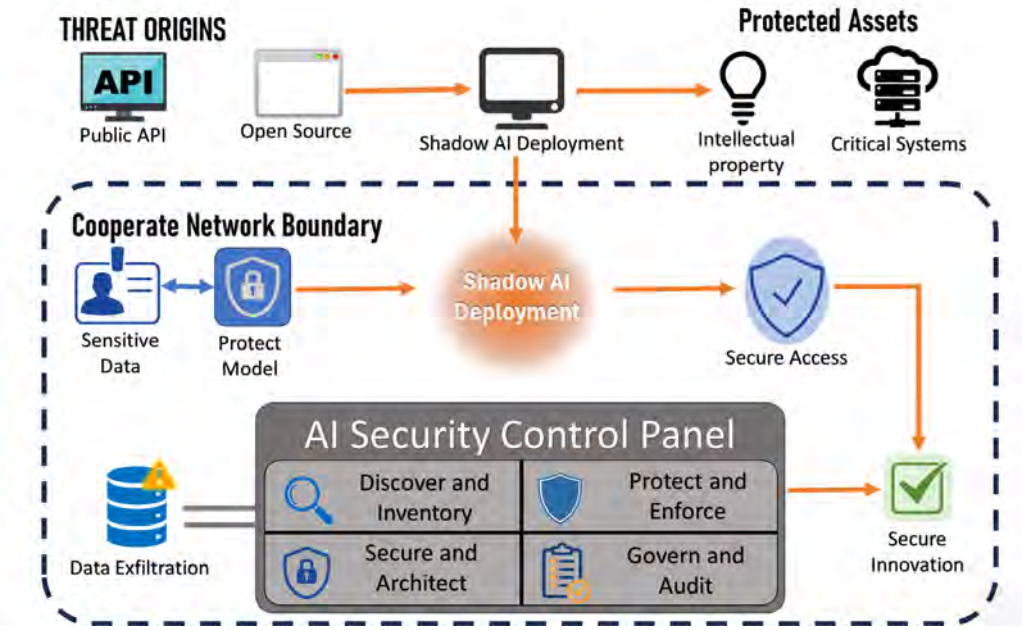

Fig. 2. Defense-in-dept Architecture against Shadow AI

B. Vulnerability Exploitation

A team of software engineers at a tech company implemented an open-source Large Language Model (LLM) for automatic code documentation. The model was deployed in a team-managed standalone containerized environment. The LLM's container image was pulled from a non-validated public repository, which concealed an unpatched flaw from an epochal library within an ancient artifact. An attacker was able to exploit this vulnerability, achieving remote shell access to the container, and then laterally moving through the internal network by pivoting onto the host machine using improper permissions. The LLM, which was supposed to provide basic productivity enhancements, became the organization's network's primary attack surface [19]. It illustrates the supply chain risk of unsupervised AI. One unassessed element in the infrastructure components can jeopardize the whole protective architecture.

C. Proactive Governance

Within a large-scale manufacturing firm, the security unit executed a complex AI Control Framework. The automated AI asset discovery platform within the company's network monitoring system and cloud API logs was a key element of the Control Framework. When a factory quality control engineer attempted to deploy a private, unapproved computer vision model to an edge device, the platform instantly flagged the activity. It 's a case when the unique API calls to an external model repository and the data transfer patterns associated with training on the factory floor were identified. Thereafter, the security automation workflow executed a set of predetermined actions: the device was autonomously quarantined from the broader network, the security operations center (SOC) was alerted, and a formal risk assessment was initiated. The security team was able to coordinate with the engineer, conduct a security and compliance review of the model, and transfer it to a controlled ventilation system within 24 hours. This model was contained, preventing it from becoming a shadow asset. It also guaranteed that the model was protected securely so that it could be used without exploitation. The summary of the case studies, threat types, and technical impact classification is as shown in Figure III.

V. Conclusion & Future Steps

Unsupervised deployment of AI technologies in an organization is called "Shadow AI." This is concerning as it has been recognized as one of the primaries means by which organizations expand their digital attack surfaces. The practice of shadow innovation is problematic because it triggers extreme technological risks such as loss of sensitive-privacy data, uncontrolled model exfiltration, unintentional damage through unmonitored backdoors, and masked breaches in unmonitored AI. The provided case studies demonstrate these risks using concrete, verifiable security incidents. The optimal way to mitigate these incidents is through a holistic strategic framework that synchronizes self-regulating policy automation, tech governance, and a zero-trust framework. This is illustrated in our paper by the automated retrieval scenario post-incident in which an automated discovery process halts an ongoing breach. The highly reactive governance that prevails in the field is in stark contrast to this. The field of AI security is poised for a dramatic change as the availability of generative and multimodal models becomes commonplace. Now, prediction models must also account for data-centric attack vectors, including advanced counter-metric fabrication

TABLE III
SHADOW AI CASE STUDIES.

Case Study	Threat Type	Technical Outcome
Unapproved Analytics	Data Privacy Breach	Model inversion led to PII exfiltration
Rogue LLM	Supply Chain Attack	Vulnerability exploited for network access
Proactive Governance	Unsanctioned Deployment	Automated discovery prevented full breach

and hidden payloads, as well as counter-metric concealed models.

The focus must shift to the outcomes, making it imperative to establish model trust frameworks, at a minimum, digital attestations and real-time integrity monitoring for lineage models during the AI operational lifecycle.

Moreover, the domain of Explainable AI (XAI) focusing on security analytics will be instrumental as it helps security analysts explain the why and the how of an AI model's decision and the additional benefits during threats hunting and incident response [20]. AI governance frameworks will have to dynamically decentralize and automate predictively and, at the granular level, the behavioural analytics to anticipate and thwart the use and deployment of sanctioned models unsanctioned and Restrained Before Substantial Risks [21]. However, Shadow AI will shift the operational security framework of the admins. Merely guarding the network and endpoint perimeter restrictions is insufficient. The new narrative is that every AI model, every dataset, and every inference pipeline requires protection as a top tier asset, and high security must be meticulously in place.

The implementation of autonomous and continuous passive AI systems is highly encouraged as these systems can automatically create and maintain dynamic inventories of all AI assets. Visibility constraints will remain, and a zero-trust approach will ensure that no AI component is deemed fully trustworthy, necessitating verification of every interaction. The next focus should be on protecting safe innovation. AI systems will need to be designed securely to protect developers and platform-appropriate vetting procedures from validation tailspin as compliance burdens are shifted to developers and away from protective regulation designed to capture innovation.

ACKNOWLEDGMENT

The authors acknowledge the use of artificial intelligence-based tools to assist with language editing and clarity improvement of the manuscript.

REFERENCES

[1] N. Kühl, M. Schemmer, M. Goutier, and G. Satzger, "Artificial intelligence and machine learning," *Electronic Markets*, vol. 32, no. 4, pp. 2235–2244, 2022.

[2] D. Puthal, A. K. Mishra, S. P. Mohanty, A. Longo, and C. Y. Yeun, "Shadow ai: Cyber security implications, opportunities and challenges in the unseen frontier," *SN Computer Science*, vol. 6, no. 5, p. 405, 2025.

[3] T. Chin, Q. Li, F. Mirone, and A. Papa, "Conflicting impacts of shadow ai usage on knowledge leakage in metaverse-based business models: A yin-yang paradox framing," *Technology in Society*, vol. 81, p. 102793, 2025.

[4] E. Yilmaz and O. Can, "Unveiling shadows: Harnessing artificial intelligence for insider threat detection," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13 341–13 346, 2024.

[5] K. Michael, R. Abbas, and G. Roussos, "Ai in cybersecurity: The paradox," *IEEE Transactions on Technology and Society*, vol. 4, no. 2, pp. 104–109, 2023.

[6] N. Poehlmann, K. M. Caramancion, I. Tatar, Y. Li, M. Barati, and T. Merz, "The organizational cybersecurity success factors: an exhaustive literature review," *Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20*, pp. 377–395, 2021.

[7] T. O. Abrahams, S. K. Ewuga, S. Kaggwa, P. U. Uwaoma, A. O. Hassan, and S. O. Dawodu, "Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 120–140, 2024.

[8] S. Shrestha, C. Banda, A. K. Mishra, F. Djebbar, and D. Puthal, "Investigation of cybersecurity bottlenecks of ai agents in industrial automation," *Computers*, vol. 14, no. 11, p. 456, 2025.

[9] D. Puthal and S. P. Mohanty, "Cybersecurity issues in ai," *IEEE Consumer Electronics Magazine*, vol. 10, no. 4, pp. 33–35, 2021.

[10] A. Said, A. Yahyaoui, and T. Abdellatif, "Hipaa and gdpr compliance in iot healthcare systems," in *International conference on model and data engineering*. Springer, 2023, pp. 198–209.

[11] N. Khalid, A. Qayyum, M. Bilal, A. Al-Fuqaha, and J. Qadir, "Privacy-preserving artificial intelligence in healthcare: Techniques and applications," *Computers in Biology and Medicine*, vol. 158, p. 106848, 2023.

[12] N. K. Ray, D. Puthal, and D. Ghai, "Federated learning," *IEEE Consumer Electronics Magazine*, vol. 10, no. 6, pp. 106–107, 2021.

[13] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, p. 101804, 2023.

[14] A. O. Ugwu, X. Gao, J. O. Ugwu, and V. Chang, "Ethical implications of ai in healthcare data: a case study using healthcare data breaches from the us department of health and human services breach portal between 2009-2021," in *2022 International Conference on Industrial IoT, Big Data and Supply Chain (IIoTBDSC)*. IEEE, 2022, pp. 343–349.

[15] S. Yusif and A. Hafeez-Baig, "Cybersecurity policy compliance in higher education: a theoretical framework," *Journal of Applied Security Research*, vol. 18, no. 2, pp. 267–288, 2023.

[16] A. Habbal, M. K. Ali, and M. A. Abuzaraida, "Artificial intelligence trust, risk and security management (ai trism): Frameworks, applications, challenges and future research directions," *Expert Systems with Applications*, vol. 240, p. 122442, 2024.

[17] C. Singh, R. Thakkar, and J. Warraich, "Iam identity access management—importance in maintaining security systems within organizations," *European Journal of Engineering and Technology Research*, vol. 8, no. 4, pp. 30–38, 2023.

[18] K. Spanaki, E. Karafili, and S. Despoudi, "Ai applications of data sharing in agriculture 4.0: A framework for role-based data access control," *International Journal of Information Management*, vol. 59, p. 102350, 2021.

[19] B. C. Das, M. H. Amini, and Y. Wu, "Security and privacy challenges of large language models: A survey," *ACM Computing Surveys*, vol. 57, no. 6, pp. 1–39, 2025.

[20] R. Machlev, L. Heistrene, M. Perl, K. Y. Levy, J. Belikov, S. Mannor, and Y. Levron, "Explainable artificial intelligence (xai) techniques for energy and power systems: Review, challenges and opportunities," *Energy and AI*, vol. 9, p. 100169, 2022.

[21] D. Puthal, S. P. Mohanty, E. Kougianos, and G. Das, "When do we need the blockchain?" *IEEE Consumer Electronics Magazine*, vol. 10, no. 2, pp. 53–56, 2020.