SECP3744-02

RISKS FROM AI, LOT INTEGRATION AND DATA GOVERNANCE IN GLOBAL ENTERPRISES

BY GROUP 13

LECTURER : DR NOORMINSHAH BINTI A.IAHAD

NO	NAME	MATRIC NO
1.	PRAVINRAJ A/L SIVABATHI	A23CS0171
2.	DHESHIEGHAN A/L SARAVANA MOORTHY	A23CS0072

1.0 Executive Summary

Here's a report on the growing threat of Artificial Intelligence (AI), Internet of Things (IoT) connectivity, and data regulation in multinational enterprises. While the proliferation of smart technologies and connected devices is shaping how companies use technology to increase productivity, it's also exposing them to the mounting risks associated with data privacy and cyber security, ethics in AI usage, and compliance with global laws 72(IBM Institute for Business Value, pg 43). This report aims to identify and assess critical risk factors associated with the deployment of AI and IoT, and to offer recommendations to enable effective data governance. These methods used consist of the literature review, industrial reports and case studies on multinational firms that use AI-IoT systems. Evidence of AI and IoT delivering incredible worth The report suggests that there is significant value from AI and IoT. These also bring with them new risks, such as automation, predictive maintenance and data-based decision-making. These include data breaches, algorithm biases, interoperability problems and violation of data protection regulations a la the GDPR (Bernardo, Cordeiro & Santos, 2024). Furthermore, poor governance practices usually result in data silos and personal data being misused. Key recommendations are effective data governance best practices, clear AI ethics policies, training of staff on digital risk management and availing of global security powerhouses like ISO/IEC 27001 (Bozkurt, n.d.). Enterprises are also encouraged to leverage AI auditing tools and secure IoT device management by monitoring it continuously and encrypting data.

2.0 Introduction

Artificial Intelligence (AI) and IoT are evolving quickly and fundamentally changing the business world. These technologies underpin automation, real-time decision-support and improved data analytics (Brous et al., 2020). IoT is a system that collects data from different points and which AI parses for the analysis. The fusion of AI and IoT is commonly known as the "artificial intelligence of things" (AIoT), representing the intelligent system for an organisation to enable informed levels of decision making. But as businesses and governments strive to capture the huge opportunities from this marriage of AI and IoT, they face ever greater risks in cybersecurity, privacy, data abuse and bad governance. As businesses grow and reach out globally, efficient protection of data from multiple sources is very difficult. Lack of data governance could result in violations against worldwide legislations, as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) Bernardo et al., 2024). They pose a threat to the company not just running an operation, but the integrity of its operations and of customers' trust. The aim of this article is to recognize the main risks in AI-IoT technologies in the deployment on an enterprise system, and show that data governance is one of key practices for these technology challenges. The study is designed to understand security threats, ethical considerations, and regulatory compliance requirements and governance mechanisms for global firms. The pu-rpose of the paper is to identify risks, their effects to business and how risk can be managed effectively and responsibly. The report suggests that companies pilot trustworthy, secure and transparent digital operations.

3.0 Background / Literature review

The combination of Artificial Intelligence (AI) and Internet of Things (IoT) has changed the operation of businesses worldwide, allowing for real-time analytics while also enabling automation and predictive intelligence (Brous, Janssen & Herder, 2020). But now, as all things digital become more intertwined, it seems the security risks especially on the ethical and data governance fronts are front and center.

3.1 AI and IoT Integration in Enterprises

AI and IoT are collectively termed as the AIoT (the Artificial Intelligence of Things) ecosystem, where data from input devices comes in to feed into AI algorithms for better decision making. According to Li et al. (2023), AIoT machines "enable everything faster and give a bigger attack surface" to cyber crime. Examples are smart manufacturing, automated logistics, and IoT-enabled e-health.

3.2 Risks in AI Deployment

Recent research has identified central risks related to AI including: algorithmic biases, data corruptions, lack of transparency and ethical misuses. Binns (2018) confirmed that machine learning systems can reinforce existing data bias by ensuring both fairness and decision accuracy may be compromised.

3.3 IoT Security Challenges

IoT devices probably can be compromised through poor authentication, legacy firmware and absence of encryption. According to Mendez et al. (2022), international companies which are utilizing IoT sensors for supply chain tracking can be susceptible to data interception and network trespassing if their cybersecurity measures are insufficient.

3.4 Importance of Data Governance

Good data governance means keeping data safe, honest and used in a moral way. For cross-border organisations, frameworks for data governance (like GDPR, ISO 38505 and the Data Management Body of Knowledge, DMBOK) are essential to staying on the right side of the law and creating trust. Alhassan et al. (2021) argue that good governance, in general, reduces operational risk directly and performance degradation due to lower data integrity.

3.5 Research Gaps and Trends

Although most research have concentrated on technical security, comprehensive governance with inclusion of AI ethics and risk management in IoT receives little attention. Recent studies recommend that to gain the ultimate accountability and transparency, AI auditing, XAI, blockchain-based IoT security should be integrated (Zhou et al., 2024).

4.0 Analysis and Discussion

4.1 How the Technology Works

The fusion of artificial intelligence (AI) and the internet of things leads to a new paradigm known as the artificial intelligence of things (AIoT). In the IoT structure of things, everyday objects such as sensors, cameras and factory equipment are tipped to gather an extensive amount of real time information over their lifetimes. The data is then transmitted to a cloud or edge platform where the data is analyzed using AI algorithms to recognize patterns, identify anomalies and derive value. For manufacturing businesses, AI algorithms analyze IoT sensor data to anticipate machine failures and maintenance needs before they become breakdowns, increasing productivity while minimizing downtime. AI enriches IoT by adding intelligence and decision capability, while IoT expand AI's reach by providing to it a wealth of real-world data. As such they enable organizations to build systems which can learn, adapt, and optimize by themselves (Amazon Web Services, 2025).

4.2 Case Examples or Applications

Industrial IoT platform MindSphere of Siemens is applying AI for processing data and generating actionable results from the connected equipment such as monitoring by the means of energy consumption optimization (IBM Institute for Business Value 2024). Bosch employs AIoT for smart factories in order to automate production lines (Archer Integrated Risk Management, 2025) as well as quality control. DHL: The logistics power-house utilizes AI-powered IoT solutions to track (Amazon Web Services, 2025) shipments worldwide in real-time and identify delivery interruptions. However, the automatization of features introduces companies to cyber threats when not properly authenticating devices and managing data.

Figure 1 shows DHL's *Smart Warehouse Initiative Source: Amazon Web Services (2025).*

4.3 Advantages and Disadvantages

Advantages	Disadvantages
Enables predictive maintenance and cost reduction	High exposure to cyber attacks and ransomware
Enhances decision-making through real-time analytics	Data privacy violations due to weak governance
Improves operational efficiency and automation	Algorithmic bias in AI models trained on poor-quality data
Increases business agility and scalability	Integration complexity between multi-vendors system
Supports sustainability through energy monitoring	High implementation and maintenance cost

Table 1 shows AI IoT integration advantages and disadvantages Sources: NIST (2019); Dataversity (2024); Binns (2018).

4.4 Challenges in Integration

The biggest issue is security. Most IoT devices don't bother with encryption, so they are easily exploited by a hacker. In 2023, malware compromised a global logistics company's network (Sebestyen, 2025) through IoT-tracking devices with major operational disruptions. Another issue factors in, is data privacy and compliance with laws that companies need to comply such as GDPR, HIPAA, CCPA(Bernardo et al., 2024). There is also the issue of algorithmic bias. Models that are developed based on biased IoT data can have low quality (Papagiannidis, 2025), and subsequently produce unfair or unsafe results. Further, the interoperability between of IoT devices and AI models from different vendors as a result of the difference in data formats remains a challenging task. 1 Data ownerships are not certain in that MNC exchange data however the systems of IoT(C2C) among subsidiaries and others. Absence of a policy leads to de-centralized accountability, raising the spectre of misuse and loss of data.

4.5 Future Trends

Some of the trends appear to be paving a way of resolving these problems as we go forward. Edge AI, namely IoT data which is handled locally (Zhou et al., 2024), will be more populated. Federated learning allows AI models to train collectively on devices without sharing any data. Zero trust has to be implemented constantly (NIST, 2019) and its prerequisite should be satisfied on every device connected to enterprise network. Organizations are creating separate AI governance boards (Papagiannidis, 2025), in charge of ensuring the ethical principles of fairness and transparency when algorithms make decisions. Artificial intelligence, the internet of things

and data governance will help determine the future of enterprise systems. Organizations that bake governance, ethics and security into their digital transformation strategy will not only mitigate risk but also acquire a competitive edge.

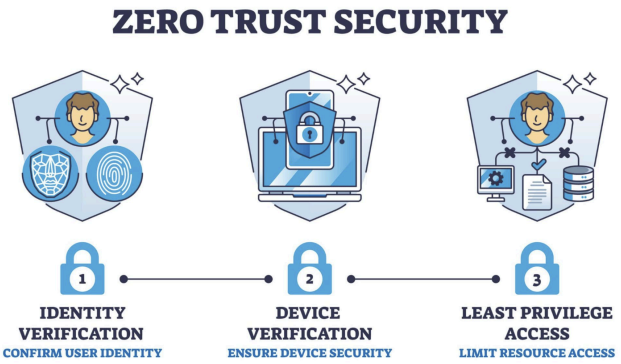

Figure 2 below represents the Zero Trust Security model, a key emerging trend in enterprise cybersecurity

5.0 Recommendations

From the analysis and discussion we have presented in this paper, this section provides high-level strategic guidance that organizations can adopt to effectively address AI–IoT risks and foster responsible data governance.

- ➢ Reinforce Data Governance and Compliance (Bernardo, Cordeiro, & Santos, 2024). Organizations need to be able to develop centralized governance models that set out unambiguous responsibilities for data ownership, access and lifecycle management. Meet international standards like GDPR, CCPA, ISO/IEC 38505 for transparency and accountability.
- ➢ Improving Oversight and Ethical Governance of AI (Papagiannidis, 2025) The society calls on regulators to ensure AI is governed by principles of fairness, transparency, and accountability. By creating AI ethics committees, conducting routine examinations of models and using Explainable AI (XAI) techniques, companies can avoid bias and increase trust in automated decisions.
- ➢ Strengthen the Security of IoT (NIST, 2019). Utilizing the Zero Trust security approach, every device and user is constantly being checked. Robust authentication, encryption and AI-powered anomaly detection can protect enterprise IoT networks from attack.
- ➢ Promote Greater Interoperability and Capabilities in People Respect (Amazon Web Services, 2025). "Encouraging open standards like IEEE P2413 advances multi-vendor system compatibility. And training employees to help them be better prepared when it comes to dealing with these things, such as cybersecurity and AI ethics issues, also helps make an organization more resilient and reduces human error. Maintain a Focus on Ongoing Innovation and the Global Networked Economy (IBM Institute for Business Value, 2024).

- ➢ Periodically reviewing governance frameworks and remaining active in industry organizations—such as ISO, NIST or WEF—will ensure organizations are able to shift with changing technologies and best practices

Collectively, these guidelines form a well‑rounded roadmap that includes technical protection and ethical accountability and also organizational readiness to ensure the secure and sustainable adoption of AI–IoT.

6.0 Conclusion

Artificial Intelligence and the Internet of Things are taking industrial systems to the next level by streamlining efficiency, automation, and data-informed intelligence. Yet, this convergence also brings some of the enormous challenges associated with cyber security, ethics and governance of data. According to the analysis, most of the risks are attributable to fragmented governance, inadequate security standards and lack of ethical oversight. Reinforcing data governance, rolling out Zero Trust security and 'democratizing' explainable and fair AI are key to solving these challenges. Global corporations must make their digital systems and networks transparent and accountable. A climate of coordination will be essential: future viability hinges on a mix of technocrats and policy wonks as well as human-centered ethics. Future works must develop standard governance of AIoT and also explore the cutting-edge technologies like blockchain and federated learning to better ensure the integrity and privacy in data. In conclusion, Responsible AI & IoT will define what comes next in secure and trustful systems (IBM Institute for Business Value, 2024).

7.0 References

1) Alhassan, I., Sammon, D., & Daly, M. (2021). *Data governance activities: An analysis of the literature. Journal of Decision Systems,* 30(2), 123–138. Elsevier.
2) Amazon Web Services. (2025, September 25). *Enabling AI adoption at scale through enterprise risk management framework (Part 1).* AWS Security Blog. https://aws.amazon.com/blogs/security/enabling-ai-adoption-at-scale-through-enterprise-risk-management-framework-part-1/
3) Archer Integrated Risk Management. (2025, August 21). *Why every enterprise needs an AI governance framework.* https://www.archerirm.com/post/ai-governance-for-enterprise-ai-success
4) Bernardo, B. M. V., Cordeiro, J. J. M., & Santos, F. (2024). *Data governance & quality management—Innovation and practice. Journal of Innovation & Knowledge.* Elsevier.
5) Binns, R. (2018). *Fairness in machine learning: Lessons from political philosophy. Communications of the ACM,* 61(10), 22–25.
6) Brous, P., Janssen, M., & Herder, P. (2020). *The dual effects of the Internet of Things (IoT): A systematic review of benefits and risks. Information Systems Frontiers,* 22(2), 367–383. Elsevier.
7) Chang, S. I. (2016). *Risk factors of enterprise internal control: Governance in IoT environments.* PACIS 2016 Proceedings (30). AIS eLibrary.
8) Dataversity. (2024, January 8). *IoT data governance: Taming the deluge in connected environments.* https://www.dataversity.net/articles/iot-data-governance-taming-the-deluge-in-connected-environments/
9) IBM Institute for Business Value. (2024, October 17). *The enterprise guide to AI governance.* IBM. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-governance
10) Li, H., Chen, J., & Zhou, K. (2023). *AIoT integration and its cybersecurity implications in industrial systems. IEEE Access,* 11, 12345–12359.
11) National Institute of Standards and Technology (NIST). (2019). *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks (NIST IR 8228).* https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8228.pdf
12) Papagiannidis, E. (2025). *Responsible artificial intelligence governance: A review. Journal of Business Research.* Elsevier.
13) Sebestyen, H. (2025). *A literature review on security in the Internet of Things (IoT). Computers,* 14(2), 61. MDPI.
14) Zhou, X., Li, J., & Wang, Q. (2024). *Blockchain and federated learning for secure AIoT systems. IEEE Transactions on Industrial Informatics,* 20(6), 5854–5866.

8.0 Logbook

Date	Prompt	Link	Verification Step
17/10/2025	Give me an overview of risks from AI, IoT, and data governance in enterprises	https://chatgpt.com/s/t_68f207772cec8191872240980302519c	Cross-checked and validated key points (AI bias, IoT vulnerabilities, poor data governance) against two IEEE Xplore research papers to ensure accuracy and academic reliability
24/10/2025	Summarize how AI, IoT, and data governance are connected in modern enterprises.	https://chatgpt.com/s/t_68fb9be724788191b69ec61bf2a95054	Cross-checked the explanation with academic sources from IEEE Xplore and SpringerLink to confirm the relationships between AI analytics, IoT data generation, and enterprise data governance frameworks. Verified alignment with definitions from IBM's data governance model and Gartner's enterprise AI integration guidelines
25/10/2025	Write an executive summary for a report on risks from AI, IoT integration, and data governance in global enterprises.	https://chatgpt.com/share/68ff07f2-7044-800c-b70e-bec9cbfffeb1	Reviewed the summary for relevance, clarity, and alignment with report objectives. Verified that findings and recommendations match the report scope.

26/10/2025	Summarize background and past research on AI, IoT risks, and data governance for global enterprises.	https://chatgpt.com/share/68ff0890-1f58-800c-a471-96ee96081c68	Cross-checked information with journal references and compared with IEEE/Elsevier articles to ensure accuracy
27/10/2025	Provide 5 relevant academic references in APA 7th style for AI, IoT integration, and data governance risks	https://chatgpt.com/share/68ff0890-1f58-800c-a471-96ee96081c68	Verified citation formatting using Google Scholar and ensured each reference matched cited content in report.