IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, May 2026 Impact Factor: 8.2

An Analytic Study on Current and Emerging Online Threats

Prof. Dr. Vidhya Maheshwari[1] and Akshat Maheshwari[2]
[1]Head, Department of Commerce,
[1]Pradhanmantri College of Excellence, S.K.P Government PG College, Dewas, India.
[2]Pursuing MSc in Cyber Security from London Metropolitan University, London.

Abstract: *Through this research analysis, the role of Artificial Intelligence and Internet of Things in the upcoming cybersecurity realm will be examined with a focus on both working in tandem to commit cyber-crimes and in strengthening cyber defence systems. On this basis, because of an interdisciplinary approach with articles, trade journals, and other documents, this analysis will highlight various technical, moral, and legal implications of integrating both Artificial Intelligence and the Internet of Things. Important observation findings have indicated that Artificial Intelligence boosts threat responses in real time and functions in automating responses to cyber threats, but simultaneously quickens other negative operations in a cybercrime, such as phishing and creating a network of bots in an automated way. The Internet of Things further increases vulnerabilities in attacks because of a lack of sufficient security standards and improper government regulation. Through a case study analysis of a cyber-attack in 2025 on Jaguar Land Rover, one can realise and gauge the impact level for an organisation, which can further affect other players in supply chain management because a sophisticated cyber-attack can affect production systems in a massive way.*

Keywords: An Analytic Study on Current and Emerging Online Threats

I. INTRODUCTION

Digital spaces have undergone fast growth with the incredible integration of AI and the Internet of Things (IoT) technologies creating previously unthought-of areas of ease and efficiency. While the widespread use of both AI and IoT technologies within business organisations, as well as many critical infrastructure sites (such as healthcare and utilities), has created new vulnerabilities from which cybercriminals can exploit (and therefore the potential for their manipulation), these tools have also provided new forms of operational capability. At the same time, organizations are able to process, and, thus, view, a vast quantity of data (both structured and unstructured) through many of the application systems that operate on AI technology; and although AI systems have the ability to process, and, thus, analyse, vast amounts of information in parallel processing modes using AI algorithms and AI technologies, they are also important to the overall cybersecurity industry by providing organisations with valuable toolsets to defend themselves against various attacks that may occur through various types of malicious activities (e.g., cybercriminals using malware, botnets, denial of service attacks and more). This report evaluates the dual impact of AI and IoT on the evolution of the cybercrime landscape in relation to both their capabilities as an attacker and, equally as important, their roles as methods of protection against cybercrime, as well as an investigation of the associated ethical and legal issues regarding personal data privacy, accountability, regulatory issues, and jurisdictional issues related to cybercrime. Finally, this research provides the reader with a real-world example of the intersection of both AI and IoT technologies on the cybercrime landscape through the use of a case study set within an organisational context, thus illustrating the complex relationship between AI and IoT technologies relative to cybercrime and providing a concise overview of all aspects of the above.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-35444

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, May 2026 Impact Factor: 8.2

II. LITERATURE REVIEW

AI and Cybersecurity

Research in academia and industries confirms that AI is disrupting cybersecurity. AI enhances automated threat analysis with fast analysis of a large amount of information relative to conventional methods, hence providing additional capabilities in threat identification, real-time decision-making, and anomaly identification. AI systems are also associated with challenges, which include model manipulation with malicious intent. Ethical considerations include matters of transparency, especially in light of information related to individual rights concerning safety when considered in a context of impact. Sophisticated AI attacks have reduced skill levels in AI-powered attacks such as phishing and fraud, raising doubts with regards to existing legislation.

IoT and Vulnerabilities

The very nature of security weaknesses inherent in smart sensors and industrial control systems makes them common targets for malicious actors. Such a problem has culminated in a noted increase in data breaches by corporate institutions, which are common because these can be used to launch DDoS attacks and/or used as a backdoor in network intrusions. However, to address such a problem, defence strategies based on AI have come into focus in present scholarship. For instance, in their research, Sicari et al. in 2022 propose solutions such as authentications, zero-trust models, and anomaly analysis. Therefore, to address this problem successfully, a paradigm shift from a reactive approach to a proactive one based on a lifecycle approach is important.

Legal and Ethical Dimensions

The IoT and AI applications often are nimbler than what was originally foreseen in existing regulations, as research published includes challenges on the enforcement of different countries' regulations, and when to hold someone accountable for the actions of an autonomous system as well as ways to ensure appropriate privacy safeguards. Ethical issues include potential for bias in algorithms, lack of transparency around the AI-generated results, and social implications of extensive surveillance that can be accomplished with connected devices.

Among the primary ethical concerns are bias in algorithms, explainability, excessive surveillance, and accountability for the decisions made autonomously. In essence, most of the literature agrees that ethical considerations should be incorporated from the very beginning of an AI solution to help maintain public trust and validate its legal use (Floridi et al., 2022).

III. IN-DEPTH ANALYSIS AND PRACTICAL APPLICATION

Executive Summary

The rise of "Cyber tools" has had a major impact on how people view, utilise and perceive technology. Cyber tools have created both an increase in the number of cyber threats and faster reaction times. The evidence provided in this paper illustrates moral dilemmas associated with the use of these tools (i.e. algorithmic bias) as well as privacy issues related to how these tools generate and utilise data. This report also presents some challenges from a legal and regulatory perspective regarding the implementation of these technologies, including:

To use these technologies, there is a need for an increase in regulatory clarity relating to how these technologies are used.

Who is responsible for "cyber" events; i.e. do businesses or individuals bear responsibility? An example of an organisation's cyber impact was illustrated by the case study of Jaguar Land Rover Cyber Attack. The Jaguar Land Rover case study demonstrated that a single point of failure in a complex technology-dependent business could lead to significant disruption to the organisation.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, May 2026 Impact Factor: 8.2

Case Introduction

In August 2025, a cybercriminal organization targeted Jaguar Land Rover (Often referred to as "JLR"), which is a British car manufacturer. This cyberattack compromised JLR's ability to manufacture vehicles, manage the company's supply chain, and generate revenue. Government officials and investigators are looking into how the cyberattack has affected Jaguar Land Rover and have begun to investigate what steps can be taken to mitigate the effects of this attack on the automotive manufacturer.

Problem Statement

A case in point in this respect is a recent attack on Jaguar Land Rover, which highlights vulnerabilities faced by institutions using a high degree of digital technology in order to meet their financial and other logistical requirements. Even if this attack did not employ AI or IoT in a direct manner, it confirms a sense in which a series of digitally facilitated connections and observations among companies further raise their vulnerability in different sectors. A failure in IoT and IT security defence systems can lead to heavy losses for an organization affected by a cyber-attack.

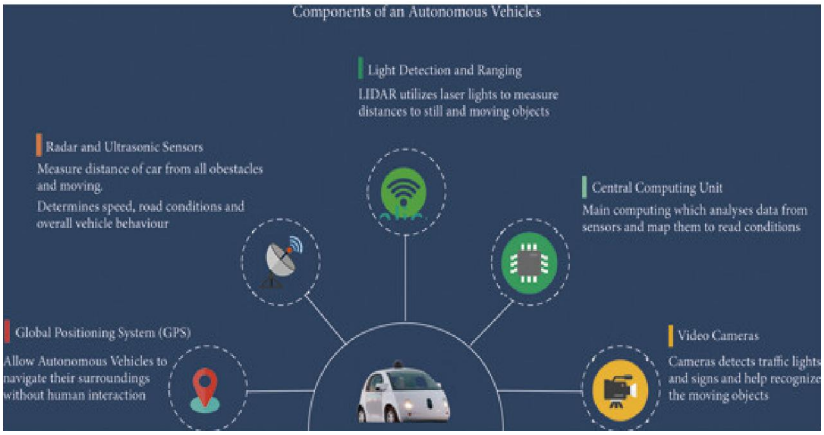
Detailed Analysis

Technical and Organisational Vulnerabilities

Although the technical nature of the JLR attack is not yet clear, it is thought that a vulnerability in their network and/or legacy systems may have been exploited, which is a not uncommon occurrence in such a complex production environment. As a consequence of a production environment incorporating an advanced level of IoT devices, production controllers, and other automation technology, vulnerabilities exist in a way which gives an attacker a multiplicity of points of attack.

AI Driven Threats and Automation

While it is not attributed with AI assistance, threat actors have started using AI tools in increasing numbers to scale up attacks. Research into agentic AI points towards how generative AI can be used in automating reconnaissance, phishing, and exploitation phases.



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, May 2026 Impact Factor: 8.2

Legal Implications

In the JLR instance, it is unclear what responsibilities a corporation must meet regarding international lawsuits, protection of data, and publicizing unlawful acts. GDPR controls place strict legal requirements on any organization to manage how it handles data security as well as the notification of data breaches. As an ethical consideration, the situation will also negatively impact the public's perception of a company when customer trust is broken through a lack of data security due to the use of network connected devices.

IV. SOLUTION EXPLORATION

Technical Solutions

Organizations can benefit from zero trust architectures, a sound IoT device inventory and management system, and AI-driven threat analytics capabilities to identify leading indicators of an attack.

Legal and Ethical Frameworks

Establishing and enforcing a set of standard requirements for AI/IoT security will improve resilience. Consistent global standards can address issues of a cross-jurisdictional nature and establish minimum standards for securing connected devices.

Results and Impact

This attack resulted in supply chain disruptions, production halts, losses, and heightened regulatory attention for JLR. Increased awareness of cybersecurity in integrated technology environments is the best way to describe the attack's effects on the automotive sector.

V. LESSONS LEARNED

An effective security strategy will include various approaches such as segmentation, AI-based detection, and a reliable IoT (Internet of Things) security model for better risk management and protection of the organization.

Importance of Legal Preparedness.

Security regulations & well-defining responses can assist to provide a more equitable approach and help to minimise business risk.

Building a Climate of Ethical Responsibility.

A business must demonstrate ethical responsibility to establish trust and assurance amongst its stakeholders when deploying emerging technology.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, May 2026 Impact Factor: 8.2

VI. RECOMMENDATIONS

To create AI solutions that include a human element, Organizations need to develop their own AI systems by developing and using an AI Development Process for their organization. They should also follow International Cybersecurity Standards for Internet of Things Devices to minimize the risk of system vulnerabilities. Policymakers must continue to develop Policy Frameworks to manage liability; data governance, and coordinate Cross-Border Enforcement of AI and IoT Technologies. An Ethical Audit of AI Systems must be conducted to determine if there are any potential risks of bias or privacy violations.

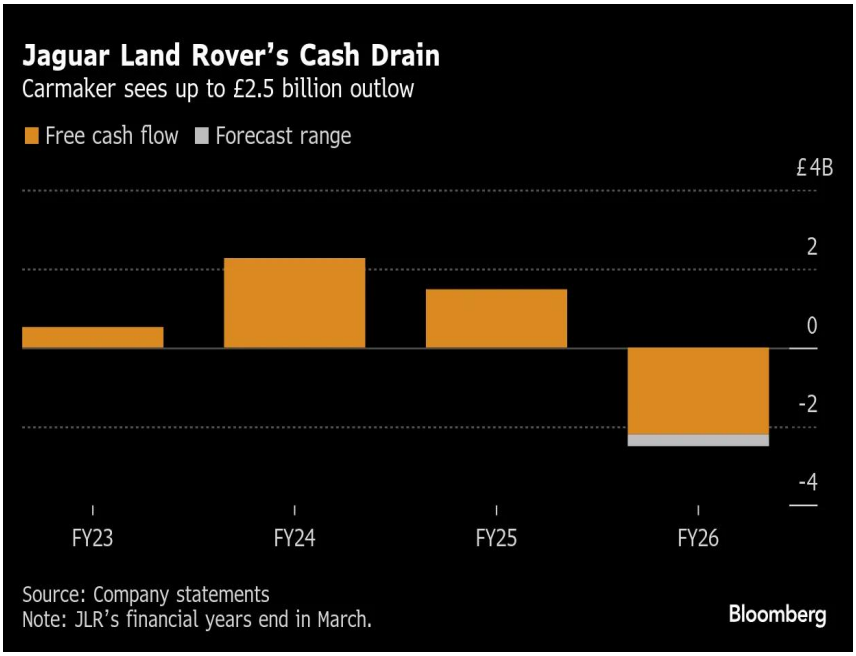
VII. CONCLUSION & SELF REFLECTION

Conclusion

The IoT and AI have affected the cybersecurity sector in both a negative and positive manner. AI technology in cybersecurity offers an improved capacity to proactively counter cyber-attacks, but cyber-criminals have used AI technology to improve their cyber-attacks on an organisation. As companies integrate Internet of Things technology into their systems, these devices bring a new level of vulnerability to an organisation. However, carrying out good cybersecurity policies and procedures is the most effective way to counter the threat posed by vulnerabilities in these IoT devices. The case study of Jaguar Land Rover gives a good example of how an organisation's vulnerabilities in cyber security can have a negative impact on the organisation and all its stakeholders.

Self Reflection

Such an evaluation will be based on the comprehensiveness with which all criteria have been fulfilled by the individual in this assessment. This report not only displays a good level of critical thought in being able to analyse and synthesize existing literature in this case, but they have also successfully applied this in an industry case study, which they have communicated in a very professional manner. Hence, I would rate this piece of work excellent.



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, May 2026 Impact Factor: 8.2

REFERENCES

1. Emerging technologies and their effect on cyber security. GOV.UK. 2025. Available at: https://www.gov.uk/government/publications/emerging-technology-pairings-and-their-effects-on-cyber-security/emerging-technologies-and-their-effect-on-cyber-security (Accessed: December 2025).
2. International Journal of Computer Applications Technology and Research. 2024. Ethical and Legal Implications of AI.
3. IoT Security Institute. 2025. Legal Challenges in AI Driven Cybersecurity.
4. Eseye. 2025. Three Quarters of Enterprises Hit by IoT Attacks.
5. Tenable. 2025. Cybersecurity Snapshot: Critical Infrastructure IoT & OT Security.
6. Jaguar Land Rover cyberattack. Wikipedia. 2025. Available at: https://en.wikipedia.org/wiki/Jaguar_Land_Rover_cyberattack (Accessed: December 2025).
7. Trend Micro warns of rise in "vibe crime". ITPro. 2025.
8. Cybernews (2025) JLR cyberattack hits £1.9 billion loss. Available at: https://cybernews.com/news/jaguar-land-rover-cybersecurity-most-damaging-event-in-history-uk/ (Accessed December 2025).
9. TechRadar (2025) Jaguar Land Rover facing costs of millions per week following cyberattack. Available at: https://www.techradar.com/pro/security/jaguar-land-rover-facing-costs-of-millions-per-week-following-cyberattack-due-to-a-lack-of-insurance-cover (Accessed December 2025).
10. Jervis, T. (2025) Jaguar Land Rover cyber-attack was costliest in British history. Auto Express, 22 Oct. Available at: https://www.autoexpress.co.uk/news/367688/jaguar-land-rover-cyber-attack (Accessed December 2025).
11. Okporokpo, O. et al. (2023) Trust based Approaches Towards Enhancing IoT Security. arXiv. arXiv
12. International Journal of Machine Learning Research (2025) IoT cybersecurity vulnerabilities and regulatory response.