

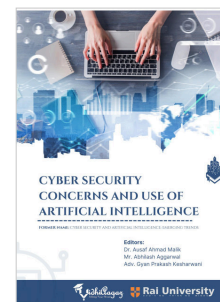
CHAPTER 22

AI-Driven Robotics: Navigating Cyber Security Concerns and the Rise of Cybercrimes

Shubha M.

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 188–194

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Shubha M., *AI-Driven Robotics: Navigating Cyber Security Concerns and the Rise of Cybercrimes*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 188 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Shubha M., ‘AI-Driven Robotics: Navigating Cyber Security Concerns and the Rise of Cybercrimes’ in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 188.

CHICAGO (17TH ED.)

Shubha, M. “AI-Driven Robotics: Navigating Cyber Security Concerns and the Rise of Cybercrimes.” In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 188–194. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-22/>.

APA (7TH ED.)

Shubha, M. (2024). AI-driven robotics: Navigating cyber security concerns and the rise of cybercrimes. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 188–194). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-22/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-22/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

AI-DRIVEN ROBOTICS: NAVIGATING CYBER SECURITY CONCERNS AND THE RISE OF CYBERCRIMES

Shubha M.²⁹

ABSTRACT

Robotics' use of artificial intelligence (AI) has transformed several sectors by increasing productivity and creativity. But this has brought up serious cybersecurity issues. As AI becomes more and more used, vulnerabilities are revealed that can be used by bad actors to commit cybercrimes. This study examines the relationship between cyber security and robots driven by AI, revealing both new risks and possible advantages. Healthcare, manufacturing, autonomous cars, and military are just a few of the areas that are using AI-driven robots more and more. However, these machines also come with security dangers, such as ransomware attacks, data breaches, and remote manipulation. The difficulty of guaranteeing system security and integrity is made worse by the absence of legal frameworks and the quick development of technology. This study investigates the cyber security of AI-driven robots, emphasizing the ways in which risks are changing, cybercriminal techniques, and the consequences for both persons and companies. The main issues that need to be addressed are data manipulation, control over robotic systems, and illegal access, all of which present threats to personal safety, security, and privacy. In order to defend AI-powered robotic systems from cyberattacks, the report highlights the necessity of proactive cyber security measures, such as strong encryption, frequent software upgrades, safe network setups, and AI-driven threat detection techniques. It also emphasizes how important it is for researchers, industry executives, and legislators to work together to create moral guidelines and laws governing the use of AI in robots. AI-driven robots have a lot of promise, but realizing that potential will require resolving cyber security issues. Society can take use of the advantages of robots driven by AI while preventing cybercrimes by recognizing and reducing risks.

Keywords: robotics, cybersecurity, cybercrimes, legal frameworks, privacy, measures

INTRODUCTION

Artificial Intelligence and robotics are changing our daily lives and various sectors such as healthcare, defence, manufacturing, logistics and transportation. The AI-driven robots can perform complex tasks and it does not require any human intervention as a result of which it is capable of making its own decisions. But one does not know how a man-made machine is able to function on its own. While this is termed as 'black box' being present in the AI system, it is unclear about the inside mechanism. From courtroom robots to autonomous vehicles, the growth of artificial intelligence has shaped the human lives by impacting the way we live, work and interact. This rapid advancement poses threats especially in the area of cybersecurity.

As robots are interconnected to networks and rely on large data, it makes them highly vulnerable to cyber threats. This means that the security risks are changing beyond hacking. Various cybercrimes are being committed by these AI-driven systems by exploiting people around the world. The AI systems in robots can be influenced to perform dangerous acts. While AI is being incorporated within cybersecurity to combat cyber threats, today it stands as a dangerous concern in the realm of digital world. This issue

²⁹ Student at Christ Academy Institute of Law, Bengaluru, India.

demands urgent attention to ensure public safety. The major difficulty lies in the formulation of a legal framework to govern the AI-driven cybercrimes or threats. While it is problematic and involves various hurdles in doing so, but it is possible to hold the person accountable if an effective legislation is passed. AI driven methodologies are recently becomes highly upgrading the industrial robotic system and its easier for factories and industries to implement the robotic system easily and inexpensive.

METHODOLOGY

This paper uses a comprehensive methodology the analyse the role of AI-driven robotics in cybersecurity which comprises of relevant literature, case studies and reports. This methodology focuses to examine the growing cyberthreats and incident response as well. The below mentioned steps are included in the methodology of this paper.

1. Case Studies:

This study examines real-world case studies and use cases showcasing AI deployment in cybersecurity, analysing successful implementations, challenges, and lessons learned from AI-driven solutions.

2. Data Collection and Analysis:

The study compiles data sources related to AI-driven cybersecurity research and applications, using statistical analysis and data visualization techniques to gain insights and trends on the effectiveness and impact of AI in cybersecurity.

3. Framework Evaluation:

The study evaluates existing frameworks and methodologies for integrating AI into cybersecurity practices, conducting a SWOT analysis to identify best practices and areas for improvement in AI-driven cybersecurity approaches.

THE ROLE OF AI-DRIVEN ROBOTICS IN MODERN CYBER SYSTEM

Robotics powered by AI is transforming technology and improving the capabilities of contemporary cyber systems in a variety of sectors. These days, these robots are essential to digital ecosystems that depend on autonomous behaviour, data processing, and decision-making. But there are additional difficulties brought forth by this merging, especially in cybersecurity. Managing risks and benefits in contemporary cyber systems requires an understanding of the role played by AI-driven robots. As AI advances to a higher intelligence level, more human service employees and human intelligence (HI) at the intelligence levels lower than that level should be used less.

Definition

AI-driven robots carry out tasks either fully or partially on its own by utilizing AI methods such as computer vision, deep learning, and machine learning. These robots are able to sense their surroundings, make judgments in real time, and adjust to changes by using data. To carry out intricate operations in the cyber environment, they communicate with digital systems such as sensors and cloud platforms. Self-driving automobiles, robotic industrial arms, and autonomous drones are a few examples. These

systems are essential parts of contemporary cyber ecosystems since they depend on safe cyber infrastructures for data processing, communication, and job execution.

The Role of AI in strengthening Cybersecurity

By creating sophisticated Intrusion Detection Systems (IDS) that continuously scan networks for anomalous activity or threats, artificial intelligence (AI) can improve cybersecurity. Without human assistance, AI-driven systems are capable of automatic patching, which finds and fixes flaws in robotic software. By examining historical attack trends, AI can also forecast future cyberthreats, allowing for proactive protection measures.

Major Applications and their Role in Cyber Systems

Patient care is being revolutionized by AI-powered surgical robots, robotic nurses, and diagnostic gadgets that rely on real-time data sharing between sensors, AI algorithms, and medical records. Examples of AI-driven robotics in cyber systems include self-driving automobiles, autonomous vehicles, and autonomous drones and ground vehicles. To traverse roadways, communicate with other cars, and avoid obstacles, these systems make use of sensors, cameras, and artificial intelligence algorithms. Because defence robots depend on secure communication links and real-time AI decision-making, they are both strong and susceptible. Robots that can learn and adjust to changing settings are expanding automation in factories and supply chains, increasing productivity and decreasing human error.

CYBERSECURITY THREATS IN AI-DRIVEN ROBOTICS

Many cybersecurity experts believe that malware is the key choice of weapon to carry out malicious intends to breach cybersecurity efforts in the cyberspace. AI-driven robots are rapidly being incorporated into a variety of industries, including manufacturing, healthcare, transportation, and defence. This brings with it both potential and hazards. These robots are appealing targets for hackers because of their reliance on AI algorithms, networked systems, and large volumes of data, which makes them susceptible to cybersecurity attacks.

- **Malware and Ransomware Attacks**

Robotic systems are susceptible to ransomware and virus assaults, which can seriously impair their functionality. Hackers can take control of functionality, steal data, and initiate other attacks by infecting software using malware. Particularly, ransomware is becoming a more serious menace as hackers target vital systems in hopes of making big profits. For example, hackers might interrupt robotic manufacturing processes and lock down software in autonomous cars, resulting in large financial losses.

- **Supply Chain Attacks**

Supply chain assaults are a new hazard to AI-driven robotics. During production or transportation, cybercriminals may target robot hardware or software, creating backdoors that let them gain access to operations. Because these assaults are hard to identify and happen before the robot enters its operating environment, it is essential for businesses to make sure their supply chains are secure.

- **Data Breaches and Privacy Concerns**

AI-driven robots, particularly in healthcare and finance, handle sensitive data, which can be accessed, stolen, or manipulated by hackers. This data can lead to identity theft, corporate espionage, or reputational damage. The real-time data collected by these robots increases the attack surface. Inadequate encryption, insecure storage, and weak access control mechanisms can contribute to data breaches in AI-driven robotics.

- **Network and IoT Vulnerabilities**

Due to flaws in IoT devices, AI-driven robots—which are frequently incorporated into broader cyber-physical systems and IoT networks—can be subject to cyberattacks. Attackers may use these flaws, such as out-of-date software, unprotected communication protocols, or a lack of encryption, to access the robot's system. The Mirai botnet assault emphasizes how crucial it is to give network and Internet of Things security top priority in order to stop illegal access or control of AI-driven robots.

LEGAL, ETHICAL AND REGULATORY IMPLICATIONS

Legal, ethical, and regulatory issues like as responsibility, data privacy, safety, and justice are brought about by the development of AI-driven robotics. Frameworks that safeguard users, reduce risks, and promote innovation are being developed by governments, regulatory agencies, and businesses. Ensuring data privacy, encouraging accountability, and protecting data privacy in crucial areas are important legal, ethical, and regulatory ramifications.

Legal Accountability and Liability

Determining responsibility and liability in the event of damage or failure is one of the legal difficulties in the field of AI-driven robots. The topic of who is at fault for mishaps is brought up by autonomous robots, which make choices without human input. The complicated decision-making processes of AI systems are difficult for current legal systems to manage, and the arrival of robots with different degrees of autonomy makes things even more difficult. Legal frameworks must change to clearly define accountability and responsibility in cases involving AI-driven robots. This includes constructing insurance mechanisms to cover damages brought on by robotic systems and establishing liability for particular actors involved in robot design, programming, and deployment.

Ethical Concerns in Decision Making and Bias

Due to biases in their training data, AI-driven robots that rely on machine learning algorithms may provide immoral results. This may lead to law enforcement robots unfairly targeting particular populations or healthcare robots giving some people worse than ideal treatment because of their gender or colour. Particularly in delicate fields like criminal justice, healthcare, and recruiting procedures, ethical considerations are crucial. In order to guarantee ethical AI, developers should give fairness in models top priority, check training data for bias, increase decision-making transparency, and set up explicit procedures for human supervision and decision-making process intervention.

Regulatory Frameworks for Safety and Certification

Given their growing usage in the industrial, transportation, and healthcare sectors, the safety of AI-driven robots is a critical regulatory concern. Regulatory bodies must set strict safety requirements and

certification procedures for these robots, including controlling the AI models, hardware, and software, in order to prevent injury. To avoid regulatory fragmentation and provide uniform safety and security standards, governments and international organizations must also harmonize rules across countries.

STRATEGIES AND SOLUTIONS FOR SECURING AI-DRIVEN ROBOTICS

i. Implementation of Strong Encryption and Data Protection

AI-driven robots' extensive data production, transmission, and processing capabilities make them susceptible to data theft and manipulation. Both data at rest and data in transit should use robust encryption algorithms to guard against unwanted access or manipulation with sensitive data. The robotic system operates with safe data encryption thanks to encryption techniques like AES and TLS. By limiting access to vital systems and data, access control techniques like multi-factor authentication (MFA) can lower the risk of insider threats and illegal access.

ii. Securing AI Models Against Adverse Attacks

When coming up with the long run analysis, development and application of AI ways in Cyber Security, one needs to distinguish between the immediate goals and long views. Robotic AI models are vulnerable to adversarial assaults, in which adversaries alter input data to trick the AI's judgment. By identifying and fending off hostile inputs, methods such as adversarial training can increase AI resilience. By increasing the transparency of AI decision-making, explainable AI (XAI) enables engineers to see anomalous behaviour that might indicate an attack and take preventative measures. Both techniques aid in defending AI systems from possible dangers.

iii. Regular Software Updates and Patching

Robots powered by AI depend on complex software, which may have flaws. Patching and regular updates are essential for addressing these vulnerabilities. Rapid device deployment of security updates using automated patch management systems reduces vulnerability to possible attacks, particularly in IoT networks where unpatched vulnerabilities might be widely exploited.

iv. Intrusion Detection Systems (IDS) and Real-Time Monitoring

AI-based intrusion detection systems (IDS), which continually analyse network traffic and identify questionable activities, are essential for protecting AI-driven robots. These systems can evolve over time to enhance detecting skills when paired with machine learning. Robotic systems that are monitored in real time can also identify behavioural abnormalities, enabling operators to make necessary corrections before serious harm is done. These systems can improve their detection skills by learning from previous attacks.

v. Establishing Regulatory Standards and Governance

Both technological advancements and legislative frameworks are necessary for the safe use of AI-driven robotics. In order to help businesses adopt best practices like safe coding, ethical AI use, and GDPR compliance, governments and industry associations should create cybersecurity guidelines for AI and

robots. Organizations may reduce cyber threats and ensure legal and regulatory compliance by using frameworks such as the Risk Management Frameworks (RMF), which assist in identifying, evaluating, and mitigating cybersecurity risks related to AI-driven robots.

vi. **Human-Robot Collaboration in Cybersecurity**

AI-driven robotics cybersecurity should be seen as a human-robot partnership, with human operators being essential in system monitoring, alarm response, and decision-making during security events. Good training initiatives may raise staff members' knowledge of cyberthreats and get them ready for security lapses. Specialists must work with AI and keep striving for its appropriate and optimal use, and not become complacent or over-reliant on third party ML-based solutions.

FUTURE TRENDS AND EMERGING RISKS

The next trend in AI-driven robotics is towards completely autonomous robots with advanced self-learning capabilities. Without human assistance, these robots are capable of making intricate judgments, learning from data in real time, and adjusting to their surroundings. But this independence makes cybersecurity more vulnerable. Cybercriminals may target robots to alter their behaviour or obtain illegal access since they interface with other networks and systems. Attackers could take advantage of flaws in AI models, which could have unexpected and harmful consequences. It is anticipated that essential infrastructure industries including energy, transportation, healthcare, and military will increasingly rely on AI-driven robots. They will carry out military operations, surgeries, and power grid management. Swarm robotics, in which several robots collaborate to accomplish complicated tasks, has promise for military operations, agriculture, and disaster relief. But there are new cybersecurity issues with this technology. Adversarial assaults are getting more complex, and machine learning algorithms for decision-making rely significantly on these techniques. Strong cybersecurity frameworks, cutting-edge AI security research, and international cooperation are required to reduce these dangers. This will assist in defending robotic systems powered by AI against changing threats.

The consequences of these emerging AI-driven cyberattacks could be life-threatening and highly destructive. By undermining data confidentiality and integrity, highly sophisticated and stealthy attacks will erode trust in organizations and perhaps result in systemic failures.

CONCLUSION

By increasing automation and efficiency, AI-driven robotics is transforming sectors including healthcare, manufacturing, transportation, and military. However, a number of cybersecurity issues are brought about by this convergence with cyber systems. Robots are particularly vulnerable to cyberattacks, such as ransomware, malware, and data breaches, since they depend on linked networks like the Internet of Things and cloud services. The research paper draws attention to certain cybersecurity issues, such as hostile assaults on AI models and flaws in data integrity and real-time communication. Case studies demonstrate how cyberattacks on industrial systems, medical robotics, and driverless cars have practical repercussions that impact both human safety and financial interests.

A comprehensive strategy is required to safeguard AI-driven robotics from cyberattacks. This covers governance strategies like modernized legislative frameworks and global cybersecurity standards in addition to technological solutions like encryption and machine learning algorithms. To create effective defences, cooperation between researchers, commercial companies, and governments is essential. To maintain the safe and efficient operation of these systems in a world that is becoming more and more digital, a proactive and cooperative approach is required. By embracing the principles of collaboration, innovation, and adaptability, organizations can stay ahead of cyber adversaries and safeguard their digital infrastructure in an increasingly interconnected and digitized world.
