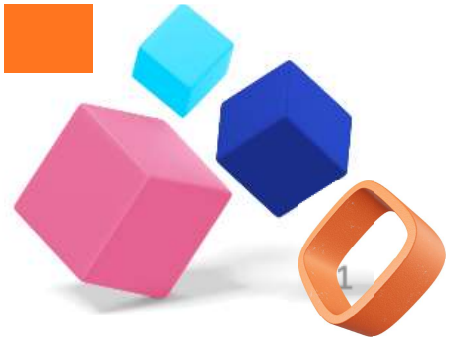
UNIVERSITI TEKNOLOGI MARA

ICT TRENDS THAT MATTER

Shamsatun Nahar Ahmad
Noor Azrin Zainuddin
Basri Badyalina
Nur Azlina Mat Noor
Muhammad Zulqarnain Hakim Abd. Jalal
Faten Elina Kamaruddin
Nurul Huda Md Yatim



FAKULTI SAINS KOMPUTER DAN MATEMATIK
UNIVERSITI TEKNOLOGI MARA
CAWANGAN JOHOR

Terbitan Edisi 2025

e ISBN: 978-629-7647-05-0

Diterbitkan oleh:
Universiti Teknologi MARA Cawangan Johor
Jalan Universiti Off KM 12 Jalan Muar ,

85000 Segamat, Johor .
Tel: 07-9352000
Fax: 07-9352716
https://johor .uitm.edu.my

EDITORIAL BOARD

TABLE OF CONTENTS

PREFACE

Praise be to Allah SWT, with His will, this eBook, ICT Trends that Matter, has been successfully compiled to capture some of the most relevant and transformative discussions in the world of Information and Communication Technology (ICT).

The work is a compilation of various views of the different practitioners, scholars, and professionals who have contributed their ideas and thoughts regarding the emerging technologies and their influence. The chapters provide just a few examples of how cybersecurity, big data harmonisation, artificial intelligence, novel learning tools, and social media analytics demonstrate the extent to which ICT has permeated our everyday worlds, our classrooms, workplaces, and communities.

ICT Trends that Matter offers readers a comprehensive exploration of 14 contemporary ICT themes that are shaping education, industry, and society. The eBook covers a wide spectrum of topics such as Big Data & AI, Digital Learning & Tools, Practical ICT Applications, Social Media & Communication and Smart Campus Initiatives highlighting UiTM Johor's experience in developing a data-driven digital ecosystem.

This eBook is informative and inspirational, with contributions that combine theory, research, and practical work. It makes the readers consider the existing ICT issues and opportunities and provides practical knowledge on personal, educational, and professional development. I would like to say that I am very grateful as the chief editor to all thecontributors whose commitment, professionalism, and innovativeness have added value to the contents of this eBook. I believe ICT Trends that Matter will be useful to academicians and students, as well as any industry professional, policymaker and those who are keen to learn more about the dynamic ICT environment.

Whether you are an academic, student, or industry professional, ICT Trends that Matter provides valuable insights into the technologies that are redefining our world today. May this work inspire further dialogue, innovation, and collaboration toward building a smarter and more sustainable digital future.

Dr. Shamsatun Nahar Ahmad
Chief Editor
Brain Hub: ICT Trends that Matter

SYNOPSIS

ICT Trends that Matter is a compilation of 14 thought-provoking chapters, which discuss the most significant trends in Information and Communication Technology (ICT) and their implications on education, industry, and society.

The elements cut across essential areas of the digital world. Discussions about the harmonisation of big data and artificial intelligence to fight cybersecurity and comparative studies concerning popular AI tools will be available to the readers.The eBook also highlights innovative approaches to teaching and learning, such as Easymath2U and V-CCMPedia, to improve conceptual learning in calculus, and AI-assisted tools to improve student engagement.

The useful experience is presented with the help of the following topics: computer tips and tricks, free e-learning applications used by children, and the successful utilisation of social media analytics tools. The role of contemporary communication mediums such as Telegram and the global presence of TikTok are also discussed in the chapters, as well as reflections on institutional work towards data-driven digital ecosystems, such as the UiTM Johor RSP16 experience.

This eBook contains the work of numerous scholars and researchers and offers both theoretical insights and practical solutions, which is why it can be of interest to academics, students, practitioners in the industry, or policymakers. ICT Trends that Matter is not merely an anthology of articles but rather is a convenient way to learn about the latest trends in ICT and predict what to expect and what to take advantage of in the digital age.

ACKNOWLEDGEMENT

The Editorial Board of ICT Trends that Matter would like to thank everyone whose assistance and commitment enabled us to make this publication possible.

We would like to thank the Department of Linkage Industry and Alumni, UiTM Johor, Segamat Campus, for enabling the acquisition of eISBN and subsequent guidance throughout the publication process.

A special mention of gratitude belongs to all contributors, whose skills, knowledge and dedication have been instrumental in the content of this eBook. Every chapter is an embodiment of how well, creatively, and committed our writers were to delivering substantial discussions on the current issues in ICT.

We also recognise the unwearying efforts on the part of the Editorial Board, which have been tireless from the very beginning of the conception to the final production of this eBook, which makes it and guarantees its success.

We are most thankful to all who have assisted this undertaking either directly or indirectly. May Allah SWT bless this endeavour and enable it to do good for the readers and the community at large.

THE ROLE OF ARTIFICIAL INTELLIGENCE (AI) IN CYBERSECURITY: THREATS AND DEFENSES

PALANIAPPAN SHAMALA, MURUGA CHINNIAH

Introduction to AI in Cybersecurity

Artificial intelligence (AI) is changing cybersecurity by making both attack and defence tactics stronger. Cybercriminals take advantage of AI to come up with smarter threats. Industries are deploying AI-powered security tools to discover threats, prevent them, and respond to them. To protect systems and lower hacking risks, AI plays an important role. We could say it is now more important than ever to protect against these risks.

Cyber-attacks are increasingly smarter and more harmful to people. In view of this, it's hard for us to rely on old-fashioned security measures to remain up. This highlights the requirement of AI-powered systems for real-time threat detection and response. AI improves safety by automating important tasks, lowering human error, and using machine and deep learning to find threats more accurately. AI can look at huge amounts of data to predict attacks. This prowess plays a big role in helping organizations strengthen their defences before any breach occurs.

AI-Driven Cyber Threats

AI is involved in all sophisticated attacks today. Attackers use AI to find new ways to attack, and in that sense, AI has undoubtedly made cyber threats more sophisticated. However, what about the threats that AI itself creates? Alas, even within the topic of AI-driven attacks, some experts see them mainly to automate killing in cyberspace. For instance, with or without AI, some automated programs scan the entire Internet looking for weak systems; when they find them, they alert other automated programs to make up a bot army that can take down the targeted system.
Attacks based on advanced artificial intelligence, such as Deep Locker, show the risk potential of highly targeted and evasive threats. To protect against these evolving threats, organisations must invest in AI-powered cybersecurity solutions that can make sense of the large amount of data we throw at them, identify the chatter in our data which means something bad is about to happen, and do it all in real time if we expect to stop tomorrow's threats today. Despite the discussions over the years, AI is not the answer, or the only answer, to all our cybersecurity problems. Here are some keyways AI is being used maliciously against us.

I. Automated Attacks

Hackers are using AI to create phony emails that have the appearance of genuine emails, thereby making them more difficult to identify. AI-driven malware is not just smarter, but is also working in tandem with the bad actors it was created for. These "smart" malware programs are learning how to evade normal cybersecurity measures and are getting better at doing so. This permits hackers the audacity to carry out complex attacks with far less effort than they used to have to expend.

Table 1: Summarising Five Major Types of Automated Cyberattacks

Attack Type	Description	Problem Caused
AI-Powered Phishing	AI generates personalised phishing emails that mimic human communication styles.	Increases the success rate of phishing attacks, leading to unauthorised access to sensitive information.
Deepfake Impersonation	AI creates realistic fake audio or video to impersonate trusted individuals.	Facilitates fraudulent activities and unauthorised disclosure of confidential information.
AI-Enabled Malware	Malware uses AI to adapt and evade traditional security measures.	Compromises systems by avoiding detection, leading to prolonged breaches and data theft.
Supply Chain Attacks	Cyberattacks target vulnerabilities in third-party vendors to infiltrate larger networks.	Breaches through trusted partners compromise multiple organizations, causing widespread data breaches.
Bad Bots & Review Bombing	Automated bots perform malicious activities like posting fake reviews to damage reputations.	Undermines trust in online platforms and manipulates public opinion, leading to reputational damage.

II. Deepfakes

AI can successfully impersonate anyone, making fake video and voice recordings of them. These recordings can - and are - being used to defraud people into making fake payments or giving them private information. They are used to pull off phone scams, trying to get people to do things they would not do if they knew who they were really talking to. They also make fake video conferences that look like the real time. Businesses are taking on more risk as deepfake technology gets better. To stop this, companies need to make their protection better. They should use strict name verification and more than one way to prove who they are.

Table 2: Summarising Five Major Types of Deepfake Attacks

Attack Type	Description	Problem Caused
Audio Deepfake Fraud	AI-generated voice mimics individuals to deceive victims into transferring money.	Leads to financial losses due to fraudulent transactions.
Attack Type	**Description**	**Problem Caused**
Fake Job Interview Scams	Deepfakes are used to impersonate job candidates or employers in video calls.	Misleads employers or applicants, leading to identity theft or hiring fraud.

Political Disinformation	Deepfakes depict politicians saying or doing things they never did.	Erodes public trust and undermines democratic processes.
Corporate Impersonation	Deepfake videos or audios impersonate executives to authorise fraudulent activities.	Results in significant financial and reputational damage to organisations.
Cyberbullying via Deepfakes	Manipulated media is used to harass or embarrass individuals online.	Leads to emotional trauma and social withdrawal among victims.

III. Social Engineering

Criminals use AI to sift through the public profiles of social media users. They take the time to understand the users and their unrivalled personal details. They then proceed to make custom-fit digital cons that are indistinguishable from reality and that use the kind of language, inside jokes, or references that only the users and their close friends would understand. If you have ever considered that your Facebook page is too revealing, you are beginning to understand the implications.

Table 3: Summarising Five Major Types of Social Engineering Attacks

Attack Type	Description	Problem Caused
Phishing	Attackers send deceptive emails to trick users into revealing sensitive information.	Leads to unauthorised access to personal and financial data, causing identity theft and financial loss.
Pretexting	Attackers create a fabricated scenario to persuade victims to divulge information.	Compromises confidential information, leading to data breaches and privacy violations.
Baiting	Attackers offer something enticing to lure victims into a trap.	Results in malware infections and unauthorised access to systems.
Tailgating	Unauthorised individuals gain access to restricted areas by following authorised personnel.	Leads to physical security breaches and potential theft of sensitive information.
Quid Pro Quo	Attackers promise a benefit in exchange for information or access.	Exploits human curiosity or greed, leading to compromised systems and data loss.

AI in Défense Strategies

AI is transforming cybersecurity works by making it simpler for experts to discover threats, fix problems, and minimise risks. Artificial intelligence (AI) is transforming cybersecurity by finding threats quicker and more accurately, automating responses, and making risk management better across digital infrastructures. AI technologies such as machine learning, deep learning, and natural language processing can analyse vast amounts of data in real time, identifying subtle patterns and anomalies

that may indicate cyber threats, including advanced persistent threats, zero-day vulnerabilities, and phishing attacks. These capabilities allow security teams to proactively address issues and adapt to evolving attack methods, often outperforming traditional security measures. AI-driven systems also support automated incident response and behavioural analysis, reducing the burden on human analysts and enhancing overall security posture. Here's how AI is changing safety today:

I. Threat Detection and Predictive Analysis

Artificial intelligence helps to identify cyber dangers by looking at data for unusual trends and managing to accurately estimate the likelihood of assaults. Machine learning improves its capability to handle new hazards. Artificial intelligence also reduces false alarms and double-checks data to ensure it is correct. Real-time tracking helps prevent intrusions by identifying and reporting unusual activity. Organisation that employs AI to safeguard critical platforms in Malaysia
are CyberSecurity Malaysia, TM, and MCMC.

Table 4: Examples of Threat Detection and Predictive Analysis initiatives in Malaysia

Initiative	Description
Cybersecurity Malaysia's Tableau-Powered SOC	Utilises Tableau analytics to swiftly identify cyberattack patterns and profile threat actors across various industries.
AI-Driven Threat Detection for Critical Infrastructure	Implements AI systems to monitor and protect essential services like power grids and water supply from cyber threats.
Coordinated Malware Eradication and Remediation Platform (CMERP)	A national system developed to automatically detect and alert organisations about malware threats.
Zero Trust Architecture with AI Integration	Combines Zero Trust security models with AI to continuously verify and monitor access, enhancing predictive threat detection.
CyberSecurity Malaysia's Threat Intelligence Dashboards	Employs data visualisation tools to analyse threat patterns and predict potential cyberattacks across sectors.

II. Incident Response and Automated Security Systems

AI is very important for quickly and effectively reacting to cyber threats because it automates security actions to limit damage. AI-powered incident response and automated security systems leverage artificial intelligence and machine learning to speed up threat detection, analysis, and response, minimising human intervention and improving security posture. These systems analyse vast amounts of data, identify patterns, and automate predefined actions to contain and mitigate incidents. AI enhances incident response automation by reducing human intervention, increasing response speed, and improving accuracy.

Table 5: Examples of AI Incident Response and Automated Security Systems

Initiative	Description
Automated Response Systems (ARS)	It can immediately isolate compromised systems, block malicious IPs, and alert cybersecurity teams, preventing threats from spreading.
AI-driven forensic analysis	It examines attack patterns, helping security teams understand the nature of a breach and improve future defences.
Automated threat mitigation	It allows AI to take instant action, such as quarantining infected files, revoking access to compromised accounts, or forcing password resets.
Self-learning AI security frameworks	constantly evolve by analysing new cyber threats, ensuring they can respond to emerging attacks in real time.

Challenges and Ethical Considerations

AI presents both exciting opportunities and significant ethical challenges. Key concerns include bias in algorithms, privacy violations, lack of transparency, and the potential for misuse. Ethical frameworks and responsible development practices are crucial to mitigate these risks and ensure AI benefits society as a whole. Despite AI's countless advantages to cybersecurity, it does come with certain threats that businesses must mitigate to make sure it is used ethically and productively.

Table 6: Challenges and Considerations

Challenges	Description
Bias in AI Models	Training data teaches artificial intelligence systems. AI can aggravate data prejudices. This can misinterpret user actions as threats. Unfixed bias makes AI discriminatory and untrustworthy. Companies must use various data, assess AI decisions, and update models to stay away from this.
Privacy Concerns	AI security monitors user activity for threats, but it also poses privacy concerns. Tracking may become unethical in the absence of transparency. Clear policies and privacy-focused technologies, such as encryption and anonymisation, assist in the reconciliation of individual rights and security.
Lack of Transparency	Many AI algorithms are complex and difficult to interpret, making it hard to understand how they make decisions and identify potential biases or errors.
Accountability	Determining who is responsible when AI systems cause harm or make mistakes is a complex issue.

Misinformation and Manipulation	AI can be used to generate fake news and manipulate public opinion, potentially exacerbating social divisions and interfering with elections.
Job Displacement	Automation driven by AI can lead to job losses in certain sectors, requiring workforce adaptation and retraining initiatives.

Case Studies and Real-World Applications

AI is playing a crucial role in strengthening cybersecurity, which is being used by several companies to detect and prevent threats, improving cybersecurity.

Table 7: AI implementation by several companies

AI in cybersecurity	Description
Darktrace	Uses self-learning AI to detect and respond to cyber threats autonomously. Monitors network activity in real-time and adapts to emerging threats.
Microsoft's AI for Cybersecurity	Scans 6.5 trillion signals daily to detect and block cyber threats. Integrates AI-driven threat intelligence to enhance global security.
AI-Generated Phishing	Cybercriminals use AI to create highly convincing phishing emails. These emails mimic human writing, making them harder to detect.

Conclusion

AI is transforming cybersecurity by enabling both advanced threats and stronger defences. Organisations must integrate AI to protect systems, data, and users. AI's real-time threat detection and response help contain cyber incidents quickly. However, continuous updates and ethical use are key to staying ahead of evolving risks. AI-driven technologies, such as threat detection, automated response systems, and predictive intelligence, allow security professionals to stay ahead of evolving threats and create a safer digital environment.

AI is a transformative technology that will continue to reshape our world, offering numerous opportunities and challenges across various fields. Its integration into education, business, and research has the potential to enhance efficiency, personalise experiences, and address complex problems. However, responsible development, ethical considerations, and on-going engagement are crucial to ensure that AI benefits society as a whole and minimises potential negative impacts.

References

D. B. Rawat, R. Doku, and M. Garuba, ‘‘Cybersecurity in big data era: From securing big data to data-driven security,’’ IEEE Trans. Services Comput., vol. 14, no. 6, pp. 2055–2072, Nov. 2021.

N. M. S. Surameery and M. Y. Shakor, ‘‘Use chat GPT to solve programming bugs,’’ Int. J. Inf. Technol. Comput. Eng., no. 31, pp. 17–22, Jan. 2023, https://doi.org/10.55529/ijitc.31.17.22.

Ashish Singh et al. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, Volume 79, https://doi.org/10.1016/j.jnca.2016.11.027