Cyber Technology in the Postmodern Era and the Growing Significance of Its Accountability

Ujjwal Ray Rajbangshi, *Ph. D Research Scholar, Law College Dehradun, Uttaranchal University*
Mona Sehgal, *Ph. D Research Scholar, Law College Dehradun, Uttaranchal University*
Shreya Suman, *Ph. D Research Scholar, UIT, Uttaranchal University*
Dr. Bhawna Arora, *Associate Professor, Law College Dehradun, Uttaranchal University*
Prof. (Dr.) Sumit Chaudhary, *HOD, UIT, Uttaranchal University*

DOI: 10.55662/CYLR.2024.3401

Abstract

Cyber technology encompasses all technological innovations, algorithms, the internet of things, and so on, resulting in an interconnected digital world. Although the integration of artificial intelligence and blockchain secures cyberspace, which has a positive impact on internet globalisation. However, the growing significance of security in cyber technology, including artificial intelligence (AI-enabled technologies), is a growing phenomenon and vital because of the increase in cyber-related risks. The usefulness of Internet of things (IoT) like smartphones, other smart gadgets, etc., for day-to-day life is very crucial, and the security of such devices is an urgent concern. Hence, the more secure the AI-enabled technologies, the greater their reliability and accountability. However, the lack of sufficient legislation and the misuse of artificial intelligence (AI) may increase the compromise of data and privacy of numerous individuals, leading to potential cyber threats that could negatively impact internet globalisation. The purpose of the study is of threefold: first, to examine the rise of cyber criminality; second, to highlight the importance of law to regulate AI; and third, to highlight the significance of security in IoT to combat cyber risk.

Keywords – *Cyber technology, Artificial Intelligence, IoT, Blockchain, Cybersecurity, Cybercrime.*

I. INTRODUCTION

The growing dynamic of internet globalisation and technological innovation creates trends in IoT devices, artificial intelligence, which become an inevitable demand from users. The reliability and convenience of cyberspace also come with accountability. And that accountability talks about how much cyberspace is protected from ongoing challenges like online fraud, inefficiency in privacy and security, and misuse of Artificial intelligence.

The integration of artificial intelligence and blockchain also has gained significant attention due to its potential to improve encryption, effectiveness, and quality in commercial settings. Supply chain has shown significant benefits from artificial intelligence and blockchain, including enhanced data accuracy, process adaptability, easier and cheaper product delivery, and enhanced traceability of goods [1]. AI is gaining popularity as a disruptive innovation, particularly in smart cities. These areas, empowered by community, technology, and policy, offer productivity, innovation, wellness, sustainability, convenience, accountability, and excellent planning, thereby increasing demand for AI-powered solutions [2]. Americans are more concerned about AI privacy, particularly the disclosure of information by AI apps, while Chinese citizens are more confident in AI's potential to increase privacy security. Safety, security, finance, and application drive American polarization, while technology and algorithms affect Chinese polarization. It also assists agencies of government along with other professionals in formulating regulations on AI legislation for safeguarding personal data [3].

The Internet of Things (IoT) is a vital component of our daily lives, with applications in smart homes, cities, industrial automation, mobile technology, and health monitoring systems. However, these systems are becoming vulnerable to cybersecurity threats due to disparate communication standards, lack security settings, and software updates. It proves crucial for researchers to work on machine learning techniques and Intrusion Detection System (IDS) designs for IoT devices [4].

ISSN 2583 7060
Volume 3 Issue 4 [October - December 2024]

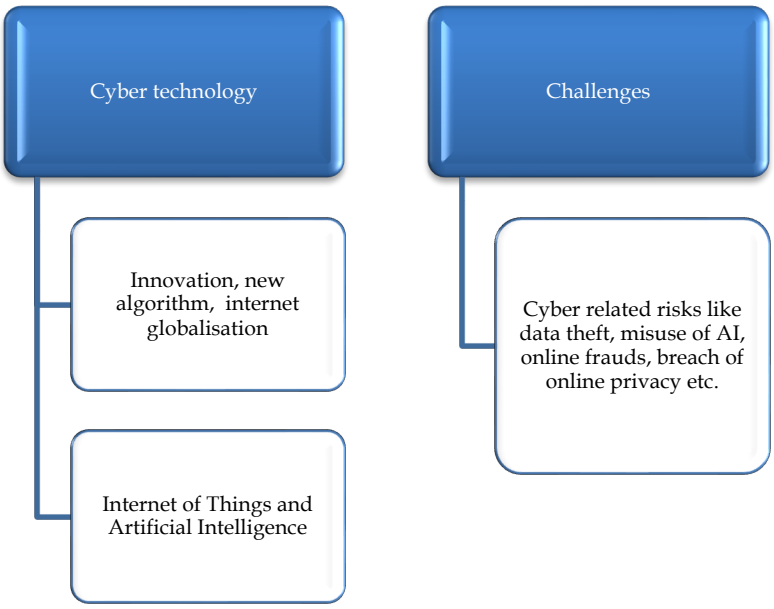

Fig 1: Reflects the cyber technology and its challenges.

The internet's dynamic ability for detached and unaccredited audiences to create and share content has sparked the innovation in information technology and sparked new creative endeavours in the vast number of personal computers connected to it. But at the same time, the issue and concerns has led to a surge in government and consumer reactions, particularly regarding security and privacy concerns that may exploit the flexibility of the internet and of course, personal computers. The sudden shift from generativity to stability in customer preferences could lead to unfavourable reactions from authorities and markets, potentially causing significant disruptions in the current open internet computing environment [5].

The study is an analysis based on secondary data collected from various publications, including government and international reports. The primary focus of this research is to place emphasis on security and privacy in cyberspace and the importance of AI and IoT to promote accountability in cyberspace and to mitigate cyber risk.

II. RISE OF CYBER CRIMINALITY: A SPUR OF CYBER RISK

Modern technology is transforming cyber forensics on computers, exposing the rise of illicit activity and network cybercrime. Computer's "system logs" contain valuable information that

can be used to combat crime. However, these systems also introduce security vulnerabilities. New forms of unlawful behaviour are using computer networks as criminal tools. Therefore, cracking down on computer and internet-based crimes and ensuring data confidentiality is crucial for national economic development and social stability. Cyber-related crime is a technologically advanced crime that differs from traditional societal criminality, involving the exchange and retention of binary digital data through computers or network devices [6].

Many unlawful acts are assisted by computer-enabled, often by the individuals with prior criminal justice experience seeking financial gain [7]. The digital world, characterized by rapid computation and advanced technology, offers a vast array of information, entertainment, education, and data access. It offers nearly every facility available in the physical world for personal activities like transactions, online shopping, and data retrieval. The use of information technology and artificial intelligence has enabled ordinary people to access and exchange knowledge. By June 2020, there was be around 4,833 million global users, demonstrating the rapid growth of the digital world [8].

White collar criminal activities like bribery, theft, and corruption often go unpunished, causing financial losses, reputational damage, and economic insecurity. Despite this, there is limited research on the use of Industry 4.0 technologies and innovations like the Internet of Things, Blockchain, and Artificial Intelligence to combat these crimes [9]. Online crime has become a significant issue, with cybercrime operations outnumbering the drug trade, with an estimated annual value of 6 trillion dollars. Projections predict this will rise to 10.5 trillion dollars by 2025. US corporations are more concerned about cyberattacks (46%) than the pandemic (43%) or skills shortages (38%). Ransomware attacks are a significant threat to organizations such as, posing a significant risk to their systems. These attacks often involve compromised passwords and credentials, leading to the encryption of files or lockdowns for payment. In 2022, ransomware assaults accounted for 41% of breaches, taking 49 days longer to detect and contain than in the previous year. The average cost of a ransomware attack was 4.54 million dollars. Information breaches have a significant financial consequence, with the US average costing 9.44 million dollar per breach, double the global average. Detection and containment take 277 days, with compromised credentials being the costliest. Compromised credentials take the longest to discover and cost more than the average breach, making them 150,000 dollars more expensive than typical information compromises [10]. Crime has evolved alongside digitization, enabling digital methods in every aspect of modern crime. Cybercrime

ISSN 2583 7060
Volume 3 Issue 4 [October - December 2024]

has become a multibillion-dollar underground industry, with the FBI estimating losses of 3.5 billion dollar in the US alone. The World Economic Forum has identified this growth as the second most serious threat to global trade over the next decade. The COVID-19 pandemic has exacerbated the situation, with increased cybercrime activity highlighting the need for effective digital solutions in criminal investigations [11].

The Internet of Things (IoT) is becoming increasingly prevalent, but it also poses risks and incidents. Cyber related crimes are becoming a significant part of IoT, causing damage to users and societies. Urgent actions are needed to protect against cyber-attacks, which threaten global infrastructure and may harm people in various ways. Cybercrime is expected to cost the global economy up to 6 trillion dollars annually. Many different strategies are tried to slow down those cyber-attacks, but they are not successful. Consequently, a safe and secure IoT platform is vital at this time, and an awareness of incidents and risks in IoT architecture should be thoroughly investigated [12]. Based on the Securing the Future: Asia Pacific Cybersecurity Readiness Survey's research shows that 83% of Indian organizations experienced a computer-related breach in the previous year, resulting in millions of dollars in losses, with 48% reporting ten or more cyber assaults, primarily for money gain, spyware installation, and data theft. A report in India reveals that despite increasing cyber vulnerability events, only 52% of respondents believe they are highly prepared. 47% of firms reported economic impacts exceeding $1 million in the past year, while 27% reported losses of at least $2 million. Additionally, 46% of respondents reported decreased hybrid work, personnel layoffs, and delayed growth plans due to cybersecurity events [13].

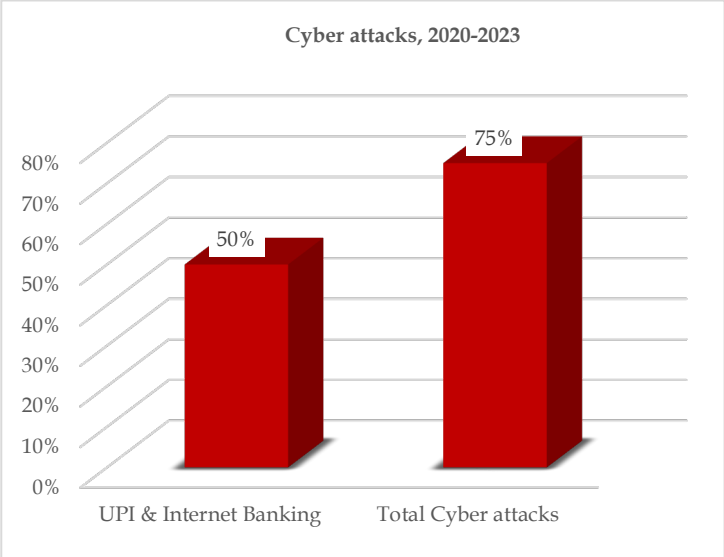

Fig 2: Here it reflects that UPI & Internet Banking alone accounts for cyber-attacks about 50% and all total cyber-attacks accounts for 75% in India, 2020-2023 [14]

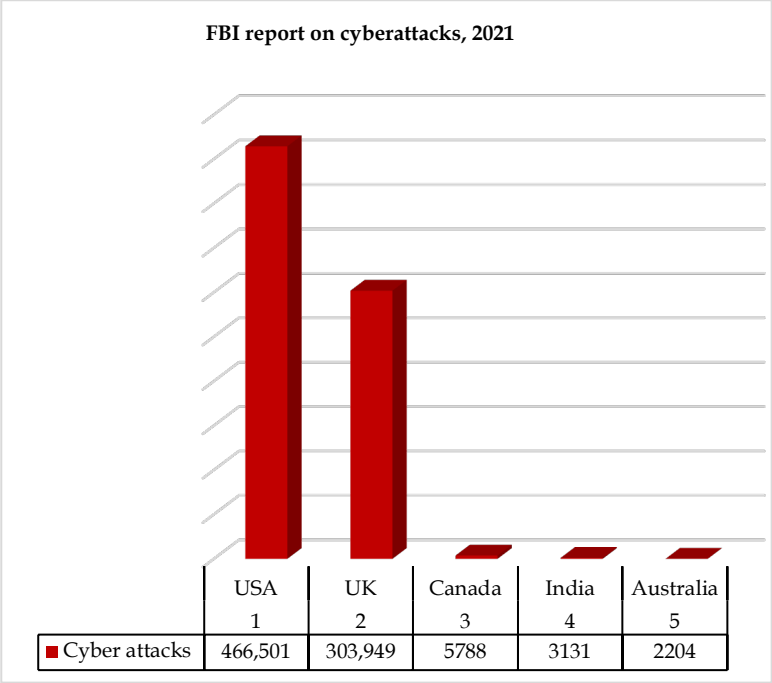

Fig 3: Here it reflects that FBI has revealed that India ranks among the top five nations in terms of total cybercrime victims in 2021 [15]

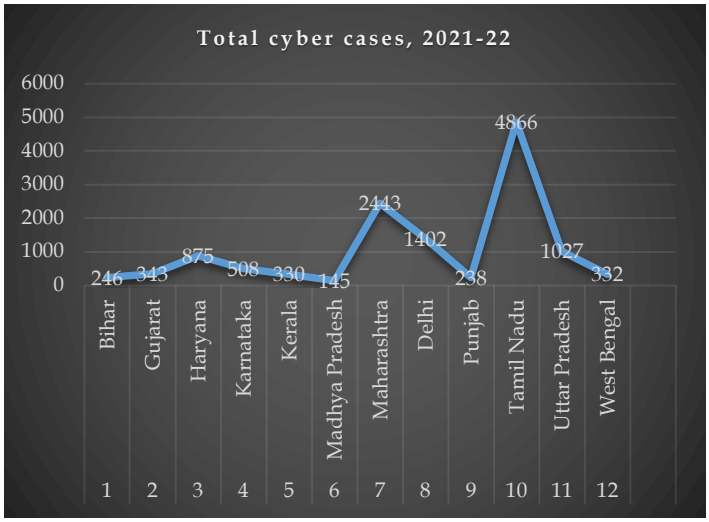

Fig 4: Here it reflects the 12 selected cities increased in cyber fraud cases in the year of 2021-22, state wise details report by Reserve Bank of India [16]

ISSN 2583 7060
Volume 3 Issue 4 [October - December 2024]

III. DO WE NEED DEDICATED LAWS TO REGULATE ARTIFICIAL INTELLIGENCE AND ITS IMPACT?

Fig 5: It reflects the relationships of AI with Ethics & Laws which is counted as accountable.

Google and Facebook have been mining user data respectively, for massive revenues, while India is debating the "Personal Data Protection Bill." These sites have been found to encourage hate speech and harassment without effective control mechanisms. Artificial intelligence (AI) might exacerbate data abuse, with ramifications for privacy, economic growth, as well as information diffusion [17]. The lack of legal precedent in India regarding the criminal culpability of AI firms, focusing on fundamental ideas that can be used to create future legislation while adapting to rapidly changing technology. It aims to provide remedies for the legal dilemma of an AI entity's criminal culpability, ensuring flexibility and adaptability to rapidly changing technology.

There are many technologies that can help police to reduce crime, and AI is one of them. Companies and cities around the world are investing in crime prevention AI and detection [18]. India lacks AI-specific rules and laws, with the proposed "Personal Data Protection Bill" (2019) which has now become an Act i.e. Digital Personal Data Protection Act, 2023.

The UK host its first "artificial intelligence summit" in November 2023, gathering heads of state and technology leaders to discourse the chances of potential risks and exploitations of 'AI' capabilities, as concerns about rising technology threaten humanity. The summit discusses the potential use of AI systems by terrorists for creating biological weapons and the technology's potential to deceive humans and cause harm [19]. The US has ratified an order to govern AI and protect the general population, aiming to promote safety and protect customers and employees from AI related challenges. The directive outlines eight goals for AI development i.e., security, privacy, equality, safeguarding customers, labour assistance, progress, and government accountable usage are all priorities. The administration has introduced new AI security and integrity criteria, requiring developers to report models

potentially impacting national or economic security. Corporations must inform the federal government and disclose safety test data before distributing dangerous models [20].

In 2018, "Malicious Use of Artificial Intelligence Report" warns that AI can be manipulated by cybercriminals, potentially causing state attacks, and transforming civilization. The report highlights the critical juncture in AI and cybersecurity evolution and urges proactive preparedness for future attacks. The secure functioning of artificial intelligence relies on resolving complex situations, controlling system behaviour, preventing goal mis-specification, maintaining cordial human-machine interactions, and adopting rules and regulations. Technology is only used and embraced when there is accountability and transparency. When risks are recognized at an international level, protocols will be developed to handle the entire AI development cycle, including technology, efficiency, statistics, protection, ease of use, compatibility, accessibility, privacy, confidentiality, transparency, and domains. The issue of misleading data on social media platforms is a significant concern for businesses like Facebook, Twitter, Google, and Microsoft. Social media dominates internet-based discussions and interests, and while there is a significant body of knowledge in this field, there is still much to learn. One of the most challenging tasks in the online social media world is developing AI algorithms to identify false substance. Disruptive forces use social media for spreading beliefs, enlisting people for antisocial acts, extremism, and fundraising. AI-based methods can be used to monitor social media content for national security. Crawlers can be designed to monitor platforms for specific content, and triggers can be created to locate specific content at different levels. A panel led by NITI Aayog Vice Chairman Rajiv Kumar aims to determine a strategy for India's AI advancement and research. Machine learning is crucial for AI systems, and quantum algorithms can speed up their development. Ensuring data safety and confidentiality is crucial, and machine learning-capable encryption methods are preferred. Research is ongoing on quantum incident-resistant approaches for AI systems. To combat cyber threats effectively, it is crucial to develop AI-based cyber security tactics and tools. Research is needed to detect new vulnerabilities in AI-based systems. Drawing on international experiences is essential. Worldwide coordination is necessary to protect against cyber-attacks. The central government should establish a National Resource Centre for Artificial Intelligence in Cyber Security, which can also serve as a point of contact for safety, ethics, and law [21].

Fig 6: It reflects how the integration of both AI and Blockchain can lead to reliability and security in cyberspace.

The rapid growth of cybersecurity risks and the need for new attack vectors are leading to the need for advanced security measures. Artificial intelligence can help identify and respond to these risks, while blockchain technology ensures data security and integrity. The combination of both can lead to safer and more effective cybersecurity solutions for individuals, organizations, and governments. Artificial intelligence and blockchain technology are being integrated in the banking sector to improve security and efficiency in payment methods. AI can detect forged transactions and trends, while the blockchain ensures transaction safety and integrity. This integration can reduce transaction costs and time, making the banking system more accessible to unbanked individuals. The integration of AI and blockchain technology is gaining popularity in various sectors such as cybersecurity, supply chain management, banking, insurance, and autonomous markets. As these innovations progress, more applications and regulatory implementations are expected to fundamentally change our behaviour and operations [22].

IV. SIGNIFICANCE OF THE SECURITY OF THE INTERNET OF THINGS (IoT) TO COMBAT CYBER RISK

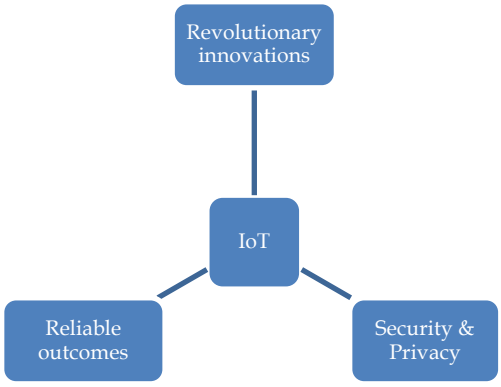

Fig 7: Reflects the potentiality of IoT to enhance revolutionary technological innovations, security & privacy, and reliable outcomes.

Apple, Microsoft, or Samsung are known for their innovative technology, and their annual product releases often come with new software, which can expose vulnerabilities, making security maintenance challenging. The increasing connectivity of in-house equipment to the internet raises concerns about potential hacker access, emphasizing the need for robust Internet of Things safety measures [23]. The Internet of Things (IoT) is increasingly relying on cybersecurity to protect its assets and privacy, reducing risks for both organizations and consumers. The advent of new cybersecurity technologies offers promising opportunities for improved IoT security management. The IoT, vital for smart cities, production, and health, also poses security risks due to inadequate security in smart devices allows hackers to access sensitive data and equipment results in challenging for organizations [24]. IoT devices collect and respond to data, but the security and reliability of externally accessible devices can be compromised, increasing the risk of internal anomalies and personal information disclosure. The study verified the transfer of parameter data in SIP/Session Description Protocol packets through an operation test between two devices. The accuracy of the target device's verification result was validated. The solution secures the smart home environment by preventing communication with malicious devices and establishing safe trust relationships between smart home devices and external smart devices or different IoT devices [25].

IoT devices, including heartbeat monitors, accelerometers, smartphones, refrigerators, smartwatches, and RFID systems, are gaining popularity due to their ability to collect and send data. The number of linked items worldwide is expected to reach over 20.4 billion in 2022, up from 8.4 billion in 2020. AI techniques like machine learning and deep learning enable IoT devices to learn from data representations and respond appropriately. These models can identify and forecast behavior, identify security incident patterns, and provide guidelines, protocols, or complex transfer functions for IoT data [26]. IoT networks, which handle vast amounts of data, are vulnerable to external threats. To protect their security, integrity, and confidentiality, an Intrusion Detection System (IDS) is essential. Modern IDSs struggle with detection and have significant device and connection overhead, making them unsuitable for real-time processing in IoT applications. The Teaching-Learning-Based Optimisation (TLBO-IDS) is an intrusion detection system designed to minimize overhead and defend Internet of Things networks against intrusion attempts. It can identify various attacks, including

backdoors, exploits, worms, fuzzing attacks, shellcode assaults, and Dos attacks. Its performance is compared to modern algorithms. The study compared TLBO-IDS to modern algorithms like the bat algorithm and GA, finding it performed 40% better than GA and 22.2% better than the bat algorithm, making it suitable for residential and commercial sectors requiring Internet of Things data security. It can differentiate between regular and invasive network traffic [27].

V. DISCUSSION AND ANALYSIS

A. Technological advancements, particularly the integration of artificial intelligence and blockchain, are gaining popularity due to their potential to enhance encryption, efficiency, and quality in business settings.

B. Computer networks are being utilized as criminal devices, necessitating the urgent need to combat computer and internet-based crime and safeguard data security for national economic progress and societal stability. *Fig 2, 3, & 4* shows the data of cyber terrorism in India.

C. AI and blockchain integration are gaining prominence in various industries like cybersecurity, finance, insurance, and independent markets. As these technological developments progress, more apps and governmental implementations are expected to significantly impact our behavior and activities.

D. IoT with the help of AI can possibly create reliable security. AI techniques like machine learning and deep learning enable IoT devices to identify security issues. The TLBO-IDS is an intrusion detection system designed to protect Internet of Things networks from various attacks, including backdoors, exploits, worms, fuzzing attacks, shellcode assaults, and Dos attacks.

E. NITI Aayog strategies on AI implementations would be a great approach. NITI Aayog is the soul of the federal structure of India. As the technological innovation advances, NITI Aayog would be a great platform to discuss the risks and benefits of any positive development in India. Hence, the need of dedicated laws to regulate AI is an urgent matter.

VI. CONCLUSION

In this paper, the only approach was to focused on cyberspace security. Though IoT and AI has the huge role to secure cyberspace and the constructive implementation on technological innovations. The benefits of AI in India would be a great initiative specially to regulate the large population section in other way if the secure algorithm is there. Reliability and integrity of AI with the integration of blockchain could be possible to lessen the risks of cyber threat. The significance of security in IoT platform is vital in the world of dynamic internet globalisation. IoT devices impacts a positive effect to the people in day-to-day life. The limitation is only the ignorance of cyberthreat which many people and even organisations still do.

But at the same time, it is also not possible without an adequate legislation to regulate the modern technological innovations. The inclusion of AI and IoT regulations and frame work in Information Technology Act 2000 and Digital Personal Data Protection Act, 2023 to make more efficiency. Ministry of Electronics & Information Technology (MeitY), and NITI Aayog should collaboratively form a committee to discuss the cyber risks and propose for a new algorithm to secure Cyberspace, and promote AI and IoT accountability.

REFERENCES

[1] V. Charles, A. Emrouznejad, and T. Gherman, "A critical analysis of the integration of blockchain and artificial intelligence for supply chain," Annals of Operations Research, vol. 327, no. 1, pp. 7–47, Jan. 2023, doi: 10.1007/s10479-023-05169-w. Available: https://doi.org/10.1007/s10479-023-05169-w

[2] T. Yigitcanlar, K. Desouza, L. Butler, and F. Roozkhosh, "Contributions and Risks of Artificial Intelligence (AI) in Building Smarter Cities: Insights from a Systematic Review of the Literature," Energies, vol. 13, no. 6, p. 1473, Mar. 2020, doi: 10.3390/en13061473. Available: https://doi.org/10.3390/en13061473

[3] Y. Xing, W. He, J. Z. Zhang, and G. Cao, "AI Privacy Opinions between US and Chinese People," Journal of Computer Information Systems, vol. 63, no. 3, pp. 492–506, Jun. 2022, doi: 10.1080/08874417.2022.2079107. Available: https://doi.org/10.1080/08874417.2022.2079107

[4] B. Kaur et al., "Internet of Things (IoT) security dataset evolution: Challenges and future directions," Internet of Things, vol. 22, p. 100780, Jul. 2023, doi: 10.1016/j.iot.2023.100780. Available: https://doi.org/10.1016/j.iot.2023.100780

[5] J. Zittrain, "Law and technology The end of the generative internet," Communications of the ACM, vol. 52, no. 1, pp. 18–20, Jan. 2009, doi: 10.1145/1435417.1435426. Available: https://doi.org/10.1145/1435417.1435426

[6] Y. Cai, D. Li, and Y. Wang, "Social IoT data mining and cyber-crime forensics under complex cloud environment," Internet Technology Letters, vol. 6, no. 1, Sep. 2020, doi: 10.1002/itl2.231. Available: https://doi.org/10.1002/itl2.231
[7] M. Šupa, V. Kaktinas, and A. Rinkevičiūtė, "Computer-dependent or computer-assisted? The social context of online crime in Lithuanian court judgements," International Journal of Law, Crime and Justice, vol. 73, p. 100577, Jun. 2023, doi: 10.1016/j.ijlcj.2023.100577. Available: https://doi.org/10.1016/j.ijlcj.2023.100577
[8] A. Singh, N. Singh, S. K. Singh, and S. K. Nayak, "Cyber-Crime and Digital Forensics: Challenges Resolution," Jan. 2023, doi: 10.1109/iccci56745.2023.10128333. Available: https://doi.org/10.1109/iccci56745.2023.10128333
[9] K. Singh, R. Bahuguna, S. Pandey, R. Singh, V. Pachouri, and G. Chhabra, "Shield of White-Collar Crime Through the Intervention of AI, IoT and Blockchain," Mar. 2023, doi: 10.1109/icscds56580.2023.10105021. Available: https://doi.org/10.1109/icscds56580.2023.10105021
[10] M. Kassab, B. Amaba, E. S. Pound, and B. Fox, "Is the Solution for Cybercrime Also a Path to Greater Productivity?," Computer, vol. 56, no. 11, pp. 91–94, Nov. 2023, doi: 10.1109/mc.2023.3290263. Available: https://doi.org/10.1109/mc.2023.3290263
[11] N. Lykousas, V. Koutsokostas, Fran, and C. Patsakis, "The Cynicism of Modern Cybercrime: Automating the Analysis of Surface Web Marketplaces," 2023 IEEE International Conference on Service-Oriented System Engineering (SOSE), 2023, doi: 10.1109/SOSE58276.2023.00027. Available: https://ieeexplore.ieee.org/abstract/document/10254768
[12] M. K. Kagita, N. Thilakarathne, T. R. Gadekallu, P. K. R. Maddikunta, and S. Singh, "A Review on Cyber Crimes on the Internet of Things," in Deep Learning for Security and Privacy Preservation in IoT, 2022. doi: 10.1007/978-981-16-6186-0_4. Available: https://link.springer.com/chapter/10.1007/978-981-16-6186-0_4
[13] Times of India, "Over 80% Indian companies hit with cyber attacks last year."
[14] "Financial fraud top cyber crime in India; UPI, e-banking most targeted: Study," Hindustan Times, Available: https://www.hindustantimes.com/business/financial-fraud-top-cyber-crime-in-india-upi-e-banking-most-targeted-study-101695036325725.html. [Accessed: Aug. 06, 2024]
[15] "India among top five victims of cybercrime: FBI report," Business Line, May 30, 2022. Available: https://www.thehindubusinessline.com/info-tech/india-among-top-five-victims-of-cybercrime-fbi-report/article65475805.ece
[16] "Increase in Cyber Fraud Cases." Available: https://pib.gov.in/PressReleasePage.aspx?PRID=1845004. [Accessed: Aug. 06, 2024]
[17] "AI needs a statutory regulator to prevent misuse," Business Line, Jul. 24, 2023. Available: https://www.thehindubusinessline.com/opinion/editorial/ai-needs-a-statutory-regulator-to-prevent-misuse/article67115781.ece
[18] N. Wickramarathna and E. Edirisuriya, "Artificial Intelligence in the Criminal Justice System: A Literature Review and a Survey," 2021. Available: https://www.researchgate.net/profile/Asela-Gunesekera/publication/358368941_COMPUTING/links/61fe4bdeb44cbe42272426a7/COMPUTING.pdf#page=342. [Accessed: Aug. 06, 2024]
[19] "What to know about the UK's AI Safety Summit," Al Jazeera, Nov. 01, 2023. Available: https://www.aljazeera.com/news/2023/11/1/what-to-know-about-uks-ai-safety-summit

[20] A. Kaustubh, "US President Joe Biden signs executive order to regulate artificial intelligence," The Times of India, Oct. 30, 2023. Available: https://timesofindia.indiatimes.com/gadgets-news/us-president-joe-biden-signs-first-executive-order-to-regulate-artificial-intelligence/articleshow/104824695.cms
[21] "Artificial Intelligence Committees Reports | Ministry of Electronics and Information Technology, Government of India." Available: https://www.meity.gov.in/artificial-intelligence-committees-reports
[22] B. Zemp, "The Intersection Between AI And Blockchain Technology – Industries Of Tomorrow," Forbes, Oct. 05, 2023. Available: https://www.forbes.com/sites/forbesbooksauthors/2023/02/28/the-intersection-between-ai-and-blockchain-technology--industries-of-tomorrow/?sh=216c98024de7
[23] "IoT Security and Privacy," IEEE Conference Publication | IEEE Xplore, May 19, 2022. Available: https://ieeexplore.ieee.org/document/9813933
[24] I. Lee, "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management," Future Internet, vol. 12, no. 9, p. 157, Sep. 2020, doi: 10.3390/fi12090157. Available: https://doi.org/10.3390/fi12090157
[25] J. Ahn, I.-G. Lee, and M. Kim, "Design and Implementation of Hardware-Based Remote Attestation for a Secure Internet of Things," Wireless Personal Communications, vol. 114, no. 1, pp. 295–327, Apr. 2020, doi: 10.1007/s11277-020-07364-5. Available: https://doi.org/10.1007/s11277-020-07364-5
[26] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions," Mobile Networks and Applications, vol. 28, no. 1, pp. 296–312, Mar. 2022, doi: 10.1007/s11036-022-01937-3. Available: https://doi.org/10.1007/s11036-022-01937-3
[27] A. Kaushik and H. Al-Raweshidy, "A novel intrusion detection system for internet of things devices and data," Wireless Networks, vol. 30, no. 1, pp. 285–294, Aug. 2023, doi: 10.1007/s11276-023-03435-0. Available: https://doi.org/10.1007/s11276-023-03435-0