

# Chapter 10

## Cyber AI Trends: Future Trends in AI for Cyberbullying Prevention

**Mir Mehedi Rahman**

 <https://orcid.org/0009-0002-7837-8639>

*Emporia State University, USA*

**Sazzad Hossain**

 <https://orcid.org/0009-0004-5379-8754>

*Emporia State University, USA*

**Bishnu Bhushal**

 <https://orcid.org/0000-0001-7522-5878>

*University of Missouri, Columbia, USA*

**Naresh Kshetri**

 <https://orcid.org/0000-0002-3282-7331>

*Rochester Institute of Technology, USA*

### ABSTRACT

*Generative Artificial Intelligence (AI) is opening new paths in the detection and prevention of cyberbullying. As we know, AI is shaping and improving the future of cyber, industry, automation, manufacturing, healthcare etc. with challenges of privacy concerns, job losses issues, and increased rules. This chapter explores future trends in AI-driven tools designed to reduce online bullying including various cybercrime across social media platforms, messaging apps, and other digital platforms. Ethical concerns like security and privacy, fairness, and avoiding bias are also discussed, aiming to ensure that AI tools are used responsibly and transparently. By combining technical advancements with an understanding of social impact, this chapter presents a vision for AI systems that create safer, more supportive online spaces. The*

DOI: 10.4018/979-8-3373-0543-1.ch010

*chapter highlights the potential of generative AI to shape digital environments that are inclusive, resilient, and protective, fostering healthier interactions for everyone involved with the future scope of the study.*

## INTRODUCTION

Cyberbullying has become a pervasive issue in the digital era, deeply impacting the psychological and emotional well-being of individuals, especially children and adolescents. Unlike conventional bullying, which is sometimes limited by physical bounds, cyberbullying is unrelenting and persistent when it enters the internet realm. Along with providing venues for communication, the explosion of social media channels and messaging apps has opened the path for harassment and abuse. Conventional approaches for spotting and correcting such actions, such keyword filtering and hand editing, sometimes fail to find subtle and context-dependent cases of cyberbullying. Recent developments in generative artificial intelligence (AI) provide chances to investigate creative ideas able to efficiently solve these problems by means of tools analyzing intricate patterns in multimedia content and textual data (Chaudhary, 2024).

Including artificial intelligence (AI) into cyberbullying prevention marks a major progress in tackling the widespread problem of internet harassment. Overwhelmed by a lot of negative content, social media companies are turning to artificial intelligence technologies such as natural language processing (NLP), machine learning (ML), and deep learning (DL) to support moderation initiatives. These technologies enable platforms to move from conventional reactive approaches where users report harmful conduct for review to proactive ways that find and reduce damaging information before it gets out there. By spotting subtle trends in text, photos, and videos, artificial intelligence technologies help to identify inappropriate content that human moderators might miss. These developments, however, create serious ethical questions even as they improve content monitoring. Scanning private conversations and user-generated content is common in proactive artificial intelligence moderation, which starts discussions on how to strike a balance between safety and freedom of speech. Errors in artificial intelligence detection—such as mistaking informal conversations or jokes for cyberbullying may cause unwarranted strife and perhaps raise societal tensions. These problems draw attention to how artificial intelligence systems should give ethical issues such justice, openness, and user rights top priority along with technical efficiency. Researchers support the creation of AI interventions that precisely balance these aspects to guarantee they are both respectful of personal privacy and expression and successful in identifying negative content. While platforms keep implementing AI-driven solutions, the emphasis should still

be on developing systems that promote trust and diversity while tackling the several problems of cyberbullying (Chaudhary, 2024) (Milosevic, 2023).

Artificial Intelligence (AI) especially Large Language Models (LLMs) and multimodal analysis systems have seen major developments in the creation of cyberbullying detection technology. Conventional methods, usually based on Natural Language Processing (NLP) for text-based communication analysis, have exhibited difficulties to adequately depict the complexity of online interactions. For example, irony, cultural subtleties, and multimedia materials including photos and videos have sometimes made these methods less useful. Recent research highlights the need of including advanced models such as GPT-4 Vision, which combine picture recognition with linguistic analysis, allowing a better knowledge of context and intent in digital interactions (Vanpech, 2024). By simultaneously assessing visual and textual signals, these systems process multimodal data and bridge gaps in conventional detection techniques. Using such systems, however, presents difficulties with scalability, ethical issues, and the requirement for varied training sets to guarantee inclusion and fairness. The continuous improvement of AI-driven systems to manage the dynamic character of digital communication reflects the increasing need for strong solutions able to solve the always changing terrain of cyberbullying (Vanpech, 2024).

Beyond conventional, fixed methods, the fast development of artificial intelligence (AI) has presented revolutionary chances to solve the complexity of cyberbullying detection and prevention. Particularly those using natural language processing (NLP) and deep learning (DL), modern artificial intelligence-driven systems shine in evaluating complex interactions, identifying context-dependent harassment, and spotting abusive behavior across text, photos, and multimodal content. Graph neural networks (GNNs) and generative adversarial networks (GANs) are reinventing how cyberbullying is detected and provide real-time, scalable solutions able to adjust to the always shifting dynamics of online platforms (Bokolo, 2024). Although related efforts to improve privacy and data integrity have investigated blockchain and federated learning approaches, the focus in this chapter is still on the pragmatic and scalable uses of artificial intelligence algorithms to reduce cyberbullying (Alabdali, 2024). Achieving balanced detection algorithms that limit false positives while preserving high accuracy across several linguistic, cultural, and contextual settings still presents difficulties notwithstanding these developments. Integration of artificial intelligence into cyberbullying prevention systems must give ethical issues including privacy, justice, and inclusiveness top priority as it develops. Emphasizing their potential to create safer, more inclusive digital environments by creative, context-aware systems, this chapter explores the technical developments, problems, and prospects of AI-driven solutions in addressing cyberbullying.

Advanced AI technologies, including NLP, DL, GNNs, and GANs, have redefined approaches to tackling the complexities of nuanced and context-dependent online interactions, particularly in cyberbullying detection. These developments provide scalable, real-time solutions that exceed the constraints of conventional approaches, therefore combating abusive behavior across many digital platforms. Still, there are important obstacles to overcome such as guaranteeing ethical standards, safeguarding user privacy, and promoting inclusiveness across many linguistic and cultural settings. These difficulties form the basis for a more general investigation of the historical and theoretical underpinnings of AI developments, the links between cyberbullying and more general cybersecurity dangers, and the part modern technology will play in determining future policies. Under this prism, a thorough examination of the application of AI approaches and their consequences is done, leading to practical findings and suggestions for building safer and more inclusive digital environments.

## Background Study

Modern artificial intelligence (AI) has been found by researchers as a useful tool for both assuring public safety and vice-versa (Michael, 2023). Since exposures and outages have long-lasting trust consequences, it is necessary to find underlying causes of cybersecurity challenges. Developing advanced artificial intelligence bots to fight against cyberattacks apart from implementing techniques to produce an AI application would not solve cybersecurity issues. Large language models (LLMs) showed several uses in the framework of generative artificial intelligence with a variety of negative potentialities including data and bias issues, explainability hurdles, environmental concerns, and privacy issues. Driven by developments in machine learning, artificial intelligence, and natural language processing (Anisha, 2021), big data has grown to be a major focus of study.

Generative AI (GenAI) models like Google Bard and ChatGPT are highlights of digital evolution transformation as can be exploited by hackers and penetration testers (Gupta, 2023). Making GenAI as trustworthy, ethical, safe, and secure including cyber defense automation, malware detection, incident response plans, secure code generation is a must. Prompt injection attacks on ChatGPT, successful attacks like Jailbreaks, reverse psychology, use of GenAI by cyber offenders, creation of social engineering attacks by adversaries, malware like polymorphic malware creation by malicious users are the popular vulnerabilities along with the capabilities of GenAI models. As the evolution of OpenAI's GPT from GPT-1 (released in 2018) to GPT-4 (current model as of June 2023), it has trained with a large corpus of texts and can take image inputs via Bing AI in Microsoft Edge browser as shown in Table 1.

*Table 1. Summary of background study for AI in cyberbullying prevention*

Ref	Strategy for Cyberbullying Prevention	Advances in AI	Challenges for Future
(Michael, 2023)	AI in Cybersecurity, OODA loop, AI applications	LLMs, AI threats, Machine Learning	Human intervention, New vulnerabilities
(Gupta, 2023)	Generative AI in Cyber Security and Privacy	GenAI tools, AI Chatbots, NLP, DNNs	ChatGPT to ThreatGPT, OpenAI
(Chan, 2019)	AI in Cybersecurity for IT Management	Big data, AI policy and managerial implications	Opportunity for cyber criminals
(Hofstetter, 2020)	AI technologies and services for anomaly patterns detection	Machine learning algorithms, AI systems	Lack of awareness, limited resources
(Roshanaei, 2024)	Cybersecurity enhancement through AI and ML	AI and ML driven models for prediction	New threats and sophisticated attacks

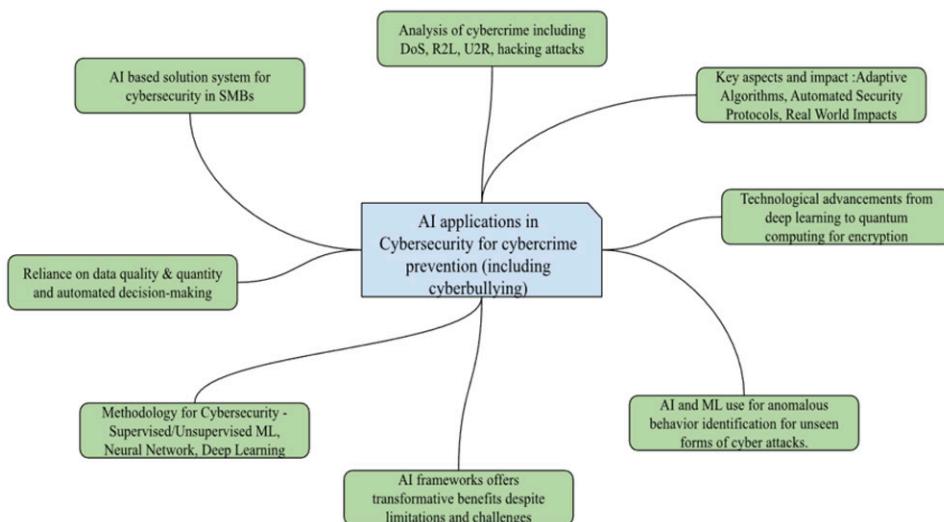
Applied in various fields like pharmaceuticals, job hopping prediction, bioinformatics and many more, AI is a thriving field (Chan, 2019). AI in cybersecurity can detect various cyber threats (existing threats and future threats) and make real-time (RT) decisions as this new age calls for strong development and deployment for future trends. As a part of cyber security and information security management, applications of AI will be largely considered the AI softwares the company and customer data. As one common method for cybersecurity is with supervised learning, AI can check interactions relating to malicious IP traffic, calculate behavior patterns and flag it. Cybercrime analysis for information security via AI like denial of service (DoS) attacks, remote to local (R2L) attacks, user to root (U2R) attacks, hacking where cyber attackers including penetration testers gain access through weak points in the system.

As cybersecurity is a complex and fast growing field, many small and medium sized businesses (SMBs) lack cybersecurity awareness and allocate limited technical resources for that (Hofstetter, 2020). Big organizations and businesses may afford their own in-house cybersecurity measures but SMBs may face a lack of all types of resources including financial resources, technical resources, human resources, and many other resources. Helping to identify anomalous behavior (taking account of false positives and false negatives) could indicate future forms of cyber-attacks for all businesses to improve performance and accuracy. AI engine provides an ability when it comes to detect cybersecurity incidents based on pattern matching and pattern analysis as displayed in Figure 1.

The enhancement of cybersecurity through AI and ML via defenses against increasingly sophisticated cyber threats highlighting new vulnerabilities (Roshanaei, 2024). Beside several challenges and limitations of AI integration such as Operational & integration costs, adversarial AI attacks, model bias & fairness, data quality & availability, AI frameworks offer transformative benefits. There are ethical con-

siderations around automated decision making, heavy dependency on data quality & quantity, vulnerability to sophisticated attacks, and enhancing AI resilience by exposing systems to improve ability of such cyberattacks. The potential bias in AI decision-making for cybersecurity can result from non-representative data sets also called as training models and/or errors in training data.

*Figure 1. Summary of AI applications in AI for Cybersecurity from our Background Study for several cyberattacks and cybercrimes (Michael, 2023) (Gupta, 2023) (Chan, 2019) (Hofstetter, 2020) (Roshanaei, 2024)*



## Cybercrime, Cyberattacks, and Cyberbullying

Cybercrime refers to illegal activities conducted using computers, networks, or digital platforms. With the rapid growth of technology, including the rise of new applications, networks, and the deep web, cybercrime has become a significant global challenge. Cybercriminals exploit weaknesses in systems to achieve various objectives, from stealing sensitive information to causing large scale disruptions. There are different types of cybercrime. In some cases, the computer itself is the target, such as when hackers attempt to breach systems or disrupt networks. In other instances, the computer serves as a tool to commit crimes, like spreading malware or stealing financial data. Lastly, digital devices may play an incidental role in facilitating crimes, such as using social media to plan illegal activities. Hackers, often associated with cybercrime, operate with varying motivations. Some act for

personal amusement, like defacing websites, while others aim for recognition by breaching high-security systems.

Regardless of their motives, hackers significantly influence the world of digital crime, and understanding their methods and intentions can help in predicting and countering cyber threats. Efforts to combat cybercrime require a balance between privacy and security. Governments and researchers are increasingly focusing on privacy issues, regulatory compliance and understanding societal norms around data sharing. The creation of effective cybercrime laws across nations is critical, but international cooperation remains vital. Organizations like Interpol, private companies, academic institutions, and national law enforcement agencies must work together to strengthen cybersecurity and develop strategies to counteract cyber threats. By understanding the complexities of cybercrime and enhancing collaborative efforts, societies can better defend against digital threats and build more secure online environments (Sabillon, 2016).

Cyberattacks are deliberate attempts by individuals or organizations to compromise the security of digital networks, systems, or devices. They target private data, interfere with regular business operations, or take advantage of weaknesses for their own financial, political, or personal benefit. In today's interconnected world, the sophistication of these attacks has increased, affecting not only people but also corporations and governments. The impact of cyberattacks on public institutions is one major topic of concern. These institutions frequently handle and preserve important data pertaining to education, health, and basic services. Whole societies may suffer because of their systems being corrupted.

For example, during the COVID-19 pandemic, Ecuador faced numerous cyber-attacks that revealed weak information security practices. These breaches caused misunderstandings, postponed important decisions, and interfered with essential services that citizens relied on, such as basic utilities and healthcare. Social media platforms have also become a major target for cyberattacks. Hackers use these networks to steal information, disseminate false information, and manipulate public opinion. When individuals are largely dependent on online platforms for communication and information during emergencies like pandemics or natural disasters, this misuse intensifies. In Ecuador, during the pandemic, discrepancies in data from various government sources stoked mistrust and brought attention to the need for improved cybersecurity procedures. To combat cyberattacks, experts emphasize the importance of strengthening information security. Important steps include creating policies that guarantee data integrity and confidentiality, putting in place real-time monitoring tools, and embracing strong encryption. In Ecuador, proposals like blockchain-based systems aim to provide a secure framework for managing public data and minimizing risks during emergencies. Ultimately, addressing cyberattacks requires a combination of advanced technology, skilled personnel, and clear reg-

ulations. Governments and organizations must prioritize cybersecurity to protect critical infrastructure, maintain public trust, and ensure that vital services remain uninterrupted, even during challenging times (Toapanta, 2020).

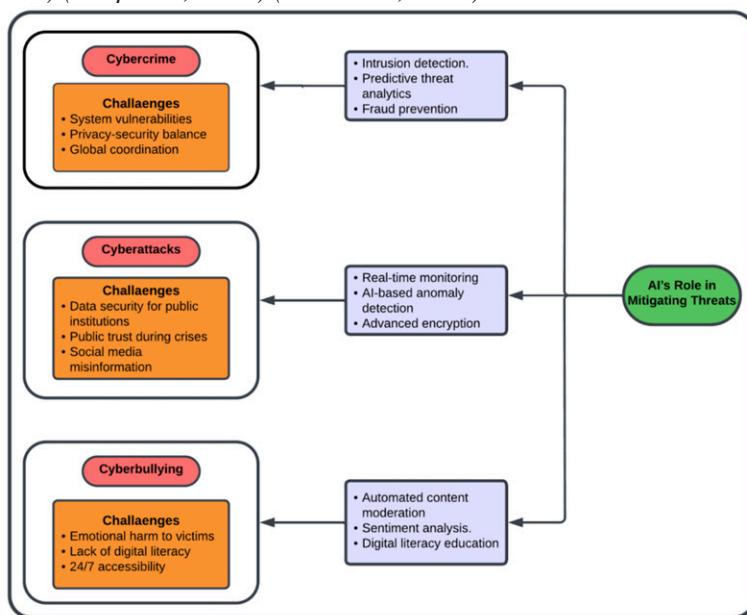
Cyberbullying is a detrimental behavior that takes place in the digital world, where individuals use technology to intimidate, harass, or harm others. It can occur across various platforms, including social media, messaging apps, and online forums, making it a widespread issue in today's internet-driven society. Unlike traditional bullying, cyberbullying has unique characteristics, such as its ability to occur 24/7 and reach a wide audience, which amplifies its impact on victims. Adolescents are particularly vulnerable to cyberbullying due to their frequent and extended use of social media and other online platforms. Research highlights that most teenagers' own smartphones and spend significant time online, increasing their exposure to cyberbullying risks. Young people are also more vulnerable to emotional distress, such as despair, anxiety, and feelings of loneliness, since they frequently lack the psychological skills such as resilience and critical thinking necessary to deal with these situations (Fulantelli, 2022).

Studies show that cyberbullying often overlaps with another form of online aggression known as cyberhate. While cyberbullying typically involves targeted harassment of an individual, cyberhate is broader and often directed at groups based on race, religion, gender, or other identity markers. Both forms of aggression share common predictors, such as poor parent-child relationships, exposure to harmful online content, and the lack of strong social support systems. Preventing and addressing cyberbullying requires a multi-faceted approach. Building positive relationships within families and fostering open communication can help reduce risks. Additionally, educators and policymakers must implement strategies that empower young people to navigate the online world responsibly. By promoting digital literacy and emotional well-being, we can create a safer environment where adolescents are less likely to become victims or perpetrators of cyberbullying. Ultimately, addressing cyberbullying and its related forms of aggression is essential to ensuring the mental health and well-being of young people in the digital age (Fulantelli, 2022) as shown in Figure 2.

This section explores how advancements in AI can tackle digital issues like cybercrime, cyberattacks, and cyberbullying. Cybercrime encompasses illegal activities using digital platforms, where hackers exploit system vulnerabilities for motives ranging from financial gain to disruption. Tackling cybercrime requires a delicate balance between security and privacy, as well as international collaboration among governments, organizations, and law enforcement agencies to develop effective laws and strategies (Sabillon, 2016). Cyberattacks, a specific form of cybercrime, focus on breaching systems to steal sensitive information or disrupt operations, often targeting public institutions and social media platforms. These attacks can cause

widespread harm, such as undermining trust in public services during crises like pandemics, emphasizing the need for robust cybersecurity measures like encryption and blockchain systems (Toapanta, 2020). Cyberbullying, a prevalent online threat, disproportionately affects adolescents due to their extensive use of social media. Its 24/7 nature and broad reach amplify the emotional impact on victims, leading to issues like anxiety and depression. Addressing cyberbullying requires building family support systems, promoting digital literacy, and implementing policies that encourage responsible online behavior (Fulantelli, 2022). AI can play a pivotal role in detecting and mitigating these threats, offering proactive solutions to create safer digital environments.

*Figure 2. AI's Role in Mitigating Cybercrime, Cyberattacks, & Cyberbullying (Sabilon, 2016) (Toapanta, 2020) (Fulantelli, 2022)*



## AI for Future of Cybersecurity

Artificial intelligence represents more than a technological upgrade; it is a fundamental reimaging of cybersecurity paradigms. As digital threat landscapes grow increasingly complex and dynamic, AI emerges as a transformative force in

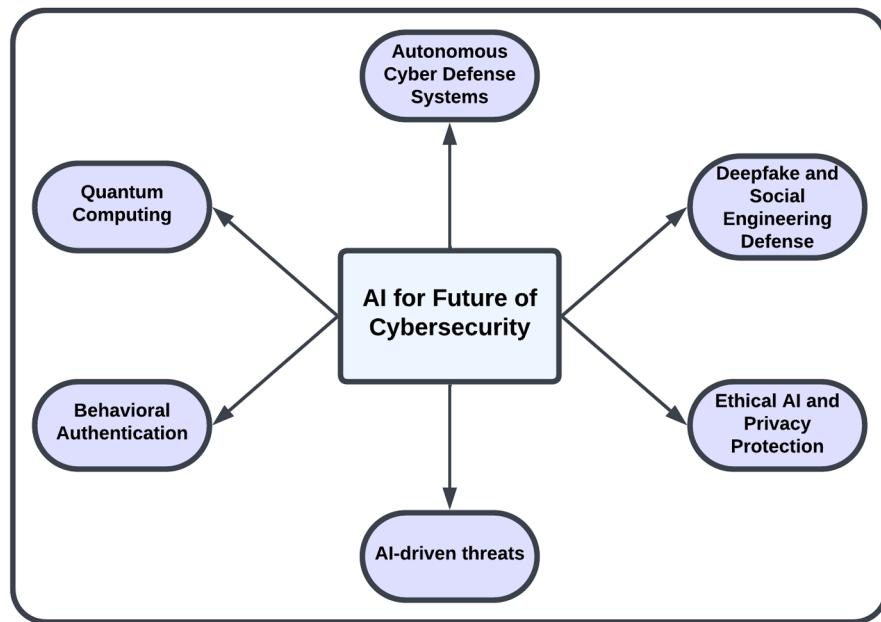
proactive threat management, offering unprecedented capabilities in risk mitigation and strategic response.

The promise of AI-driven cybersecurity lies in its ability to address the most challenging aspects of digital defense. Quantum computing-powered machine learning revolutionizes cybersecurity by harnessing immense computational power to process vast datasets (Shara, 2023). This enables advanced, real-time threat detection by rapidly identifying patterns, anomalies, and vulnerabilities. As a result, organizations can deploy robust defenses against sophisticated cyber threats, including those utilizing complex encryption techniques. Modern cybersecurity tools excel at tackling the toughest challenges in digital defense. Similarly, techniques like GANs and VAEs improve accuracy and solve data gaps in areas like medical imaging, showing their potential to uncover subtle patterns and make online spaces safer (Peryala, 2024).

Autonomous cyber defense systems further enhance these capabilities by combining AI and machine learning to detect, predict, and neutralize cyber threats in real time (Kaur, 2023). By continuously monitoring networks, these systems can swiftly identify and respond to anomalies, providing proactive protection with minimal human intervention (Madireddy, 2020). This approach significantly improves the speed, accuracy, and operational efficiency of threat responses, especially in the face of evolving cybersecurity challenges.

AI is also revolutionizing cybersecurity by deploying advanced algorithms to combat sophisticated social engineering threats. Machine learning enables real-time detection of deepfakes (Gambin, 2024), prediction of phishing attempts, and dynamic adjustment of security protocols. These intelligent systems analyze communication patterns, identify anomalies, and implement multi-layered authentication, transforming cybersecurity from a reactive defense mechanism into proactive threat prevention (Camacho, 2024) as depicted in Figure 3.

*Figure 3. Artificial intelligence for the future of cybersecurity and cyberbullying prevention*



Complementing these advancements, the future of ethical AI and privacy-preserving technologies promises to deepen trust and broaden the scope of responsible AI innovation (Santos, 2024). Next-generation privacy-preserving methods, such as multi-party computation, zero-knowledge proofs, and enhanced differential privacy techniques (Chadha, 2023), will enable highly secure collaborations where sensitive data can be analyzed or verified without being shared. Advances in federated learning will further enhance decentralized systems by allowing model training across distributed devices while protecting data privacy and minimizing risks of breaches. Blockchain ensures data integrity, enhances identity management, and prevents fraud, complementing AI in building secure systems to tackle cyberbullying and online abuse (Singh, 2024). Ethical AI will also benefit from the integration of explainable AI (XAI) frameworks, providing transparent and interpretable decision-making processes. Additionally, the convergence of blockchain technology with AI will offer immutable audit trails, ensuring accountability and fairness in AI-driven applications. These developments will continue to balance the need for technological progress with the imperative of safeguarding privacy, equity, and ethical integrity in an increasingly interconnected digital world.

Behavioral authentication is also set to evolve with advanced AI. Future behavioral authentication will leverage advanced AI to create hyper-personalized security profiles. Machine learning algorithms will analyze intricate user behaviors beyond traditional biometrics—including typing patterns, device interaction dynamics, contextual movement, and micro-gestures (Wang, 2024). These systems will develop predictive models that can authenticate users with near-absolute certainty, detecting even the most subtle anomalies in real-time. Quantum computing and neuromorphic AI will enable instantaneous, multi-dimensional behavioral analysis, making authentication seamless and virtually unbreakable.

However, the integration of AI into cybersecurity is not without substantial challenges. Adversarial attacks pose a significant threat, with malicious actors developing increasingly sophisticated techniques to exploit vulnerabilities in AI systems. Data poisoning emerges as a critical concern, where attackers attempt to compromise the integrity of AI training data, potentially rendering security solutions ineffective. The potential for advanced AI-driven threats targeting critical infrastructure adds another layer of complexity to the cybersecurity landscape (Tao, 2021).

## Cyberbullying Prevention via AI Advancements

The use of technology to meet various business needs is growing and so is for cyberbullying detection, prediction, and prevention via AI-driven framework (Meduri, 2024). Behavioral analysis, data breach risk prediction, cyber fraud detection, spam detection as cybercrime are the key AI frameworks considered for evaluation purposes. Mitigating cyber threats at various locations under different environmental settings are most essential for predicting and averting cyberattacks. AI frameworks for faster threat detection are crucial for behavior analysis, spam filtering, regression analysis, and breach risk prediction. Handling massive amounts of data with greater scalability, speed, and accuracy compared to traditional solutions for cyberbullying as advancements in AI via AI-based security systems. Explainable AI (XAI) enhances education by making machine learning transparent, helping educators trust tools, address biases, and track outcomes (Fatima, 2024).

Cryptographic attacks, malicious code integration, and several variants of phishing attacks always bypass security architectures when it comes to system development for detection and prevention of cyberattacks (Abdiyeva-Aliyeva, 2021). Data gathering which is processed into information later is always precious in prevention and detection of cybercrimes. Deep neural network (DNN) as an architectural form of artificial neural network can create learning models and learning platforms for network behavior. Out of several benefits of integrating AI for cybersecurity (and then for cyberbullying prevention), advancements like DNN serve as an excellent reinforcement against cybercrimes.

Prediction is dependent on a strong database for cyberattacks identification and prevention as we depend on technologies to defend from cyberthreats (Amarasinghe, 2019). Time series algorithm SARIMA (Seasonal Auto Regressive Integrated Moving Average) extends Auto Regressive Integrated Moving Average (ARIMA) technique. Data mining steps (as part of Phase I of suggested methodology) comprise data cleaning, data integration, data selection, data transformation, data mining, and data representation as a dataset transformed to the arbitrary shape and dataset saved in the cloud. While convolutional neural networks (CNN) finds vulnerability, artificial intelligence-based generative models do the preventive processing and enhance dependability.

Applications and future vision of artificial intelligence are not only for cybersecurity and cyber defense but also in microgrids of communication networks and physical devices from a security standpoint (Beg, 2023). Comprising modern microgrids, today cyber-physical systems have physical assets including distributed energy resources (DERs), power devices, loads, and cyber-layer in the network. AI-based cyber-attack mitigating, and cyber-attack detection applied to address data-driven cyberattacks in a distributive cooperative control-based AC microgrid. Table 2 shows that a great amount of power users lose and suffer major damage from malfunctioning microgrids and cyberattacks on them.

There is no doubt that AI has emerged as a key component of cybersecurity in terms of security enhancement and cyber threat detection and threat prevention (Rizvi, 2023). As of today's digital, environment for countering cyberattacks and cyberbullying prevention, AI is becoming a key tool to prevent cyberattacks via predictive modeling. Detection of emerging cyber threats (in contrast to traditional signature-based approaches) is the main AI advantage in cybersecurity and cyberbullying prevention. User behavior may indicate a potential cyber threat as artificial intelligence (with use of machine learning, deep learning, pattern recognition algorithms) can detect anomalies and trends in network traffic including incoming and outgoing traffic.

*Table 2. Prevention of Cyberbullying and Cyber-attacks via several countermeasures, methods, and techniques with use of Artificial Intelligence (AI)*

Prevention method(s)	Rationale of the Study	Impacts on Future AI Trends	Ref
AI-driven framework	Importance of organization automating AI processes to bolster cybersecurity.	Delves into AI frameworks for predicting and preventing cyberattacks.	(Meduri, 2024)
AI-based DNN architecture	DNN torrent structure to monitor and review impact of network traffic and host level events to warn.	DNN performs better than conventional machine learning classification.	(Abdiyeva-Aliyeva, 2021)
Time Series algorithm - SARIMA	An automated system consisting of a mechanism to deploy vulnerabilities and a rich database with known vulnerabilities.	With an output of considerable accuracy, evaluated results of cyberattacks detection, has the pattern-based attack pool.	(Amarasinghe, 2019)
AI-based techniques in microgrids	Techniques employed to tackle data-driven cyberattacks due to exceptional pattern recognition.	Performance of AI-based cyberattack mitigation in a distributed cooperative control-based AC microgrid.	(Beg, 2023)
AI in cybersecurity for threat detection	AI can be used to prevent cyberattacks through predictive modeling, protect networks and sensitive data from online threats.	AI-based systems provide complex and cutting-edge methods to counter cyberattacks including predictive analytics.	(Rizvi, 2023)

## CONCLUSION AND FUTURE SCOPE

As the challenges of cybercrime, cyberattacks, and cyberbullying continue to evolve, artificial intelligence (AI) has emerged as a key player in the fight against these. This chapter highlights the disruptive potential of technologies driven by artificial intelligence, notably in areas such as real-time threat identification, predictive analytics, and multimodal analysis enabling nuanced and context-aware intervention. Artificial intelligence offers solutions that are scalable and adaptive, which go beyond the capabilities of traditional methods. These solutions can be used to protect public institutions from cyberattacks and to mitigate the emotional and social harm caused by cyberbullying. However, as artificial intelligence systems continue to evolve, it is important that concerns such as guaranteeing justice, eliminating biases, protecting privacy, and maintaining ethical transparency continue to be at the forefront of research. The complexity of cyber risks necessitates an approach

that is collaborative and multidisciplinary, engaging policymakers, technologists, and educators, to find the optimal balance between innovation and accountability.

AI has a wide range of potential applications in the fight against digital threats, as we look in the future. The incorporation of quantum computing enables artificial intelligence systems to achieve processing rates that have never been seen before, which in turn enables faster and more precise threat detection. Federated learning and decentralized frameworks hold the promise of improved privacy and security while also reducing the dangers associated with data sharing. In addition, explainable artificial intelligence (XAI) is going to play a significant part in contributing to the development of trust by providing transparency in the decision-making process.

The identification and prevention techniques for cyberbullying will be further refined because of developments in natural language processing, image recognition, and behavioral analytics that are driven by artificial intelligence. Future computer systems will be able to more successfully address the subtleties of global digital interactions if they place an emphasis on training datasets that are both inclusive and culturally varied respectively. In addition, the combination of artificial intelligence and blockchain technology has the potential to produce records that cannot be altered, which would improve accountability in online contexts.

Ultimately, the success of these technologies will be contingent on a worldwide commitment to promoting innovation while simultaneously respecting ethical standards. By utilizing artificial intelligence in a responsible manner, we can pave the way for digital spaces that are safer and equal, ensuring that the internet continues to serve as a platform for constructive and beneficial engagement. This journey requires continued research, collaboration, and investment in AI to meet the ever-evolving challenges of the digital age.

## REFERENCES

- Abdiyeva-Aliyeva, G., Hematyar, M., & Bakan, S. (2021). Development of System for Detection and Prevention of Cyber Attacks Using Artificial Intelligence Methods. In *2021 2nd Global Conference for Advancement in Technology (GCAT)* (pp. 1-5). IEEE. DOI: 10.1109/GCAT52182.2021.9587584
- Alabdali, A. M., & Mashat, A. (2024). A novel approach toward cyberbullying with intelligent recommendations using deep learning-based blockchain solution. *Frontiers in Medicine*, 11, 1379211. <https://doi.org/10.1109/ICAC49085.2019.9103372>
- Amarasinghe, A. M. S. N., Wijesinghe, W. A. C. H., Nirmana, D. L. A., Jayakody, A., & Priyankara, A. M. S. (2019). AI based cyber threats and vulnerability detection, prevention, and prediction system. In *2019 international conference on advancements in computing (ICAC)* (pp. 363-368). IEEE. DOI: 10.1109/ICAC49085.2019.9103372
- Anisha, P. R., Reddy, K. K. C., & Nhu, N. G. (2021). Big data. Trends, challenges, opportunities, tools, success factors, and the keyway toward pandemic analytics. In *Handbook of research for big data concepts and techniques*. Apple Academic Press. DOI: 10.1201/9781003144526-11
- Beg, O. A., Khan, A. A., Rehman, W. U., & Hassan, A. (2023). A review of AI-based cyber-attack detection and mitigation in microgrids. *Energies*, 16(22), 7644. DOI: 10.3390/en16227644
- Bokolo, B. G., & Liu, Q. (2024). Artificial intelligence in social media forensics. A comprehensive survey and analysis. *Electronics*, 13(1671), 1-24. <https://doi.org/10.1201/9781003144526-11>
- Camacho, N. G. (2024). The Role of AI in Cybersecurity. Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN. 3006-4023*, 3(1), 143-154DOI: 10.1201/9781003144526-11
- Chadha, R., Sistla, A. P., Viswanathan, M., & Bhushal, B. (2023). Deciding Differential Privacy of Online Algorithms with Multiple Variables. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1761-1775). DOI: 10.1145/3576915.3623170
- Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., . . . Cao, R. (2019). Survey of AI in cybersecurity for information technology management. In *2019 IEEE technology & engineering management conference (TEMSCON)* (pp. 1-8). IEEE. DOI: 10.1109/TEMSCON.2019.8813605

- Chaudhary, P. K., Alam, N., Yalamati, S., Kolasani, S., Palakurti, N. R., & Whig, P. (2024). Detecting and preventing child cyberbullying using generative artificial intelligence. In *2024 Asia Pacific Conference on Innovation in Technology (APCIT)* (pp. 1-9). IEEE. DOI: 10.1109/APCIT62007.2024.10673710
- Fatima, S., Reddy, C. K. K., Sunerah, A., & Doss, S. (2024). Innovations in education. Integrating explainable AI into educational intelligence. In *Internet of behavior-based computational intelligence for smart education systems*. IGI Global. <https://doi.org/10.4018/979-8-3693-8151-9.ch002>
- Fulantelli, G., Taibi, D., Scifo, L., Schwarze, V., & Eimler, S. C. (2022). Cyberbullying and cyberhate as two interlinked instances of cyber-aggression in adolescence. a systematic review. *Frontiers in Psychology*, 13, 909299. DOI: 10.3389/fpsyg.2022.909299 PMID: 35712182
- Gambín, Á. F., Yazidi, A., Vasilakos, A., Haugerud, H., & Djenouri, Y. (2024). Deepfakes. current and future trends. *Artificial Intelligence Review*, 57(3), 64. DOI: 10.1007/s10462-023-10679-x
- Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From chatgpt to threatgpt. Impact of generative ai in cybersecurity and privacy. *IEEE Access : Practical Innovations, Open Solutions*, 11, 80218–80245. DOI: 10.1109/ACCESS.2023.3300381
- Hofstetter, M., Riedl, R., Gees, T., Koumpis, A., & Schaberreiter, T. (2020, September). Applications of AI in cybersecurity. In *2020 Second International Conference on Transdisciplinary AI (TransAI)* (pp. 138-141). IEEE. DOI: 10.1109/TransAI49837.2020.00031
- Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity. Literature review and future research directions. *Information Fusion*, 97, 101804. DOI: 10.1016/j.inffus.2023.101804
- Maddireddy, B. R., & Maddireddy, B. R. (2020). AI and Big Data. Synergizing to Create Robust Cybersecurity Ecosystems for Future Networks. *International Journal of Advanced Engineering Technologies and Innovations*, 1(2), 40–63.
- Meduri, K., Gonaygunt, H., & Nadella, G. S. (2024). Evaluating the Effectiveness of AI-Driven Frameworks in Predicting and Preventing Cyber Attacks. *International Journal of Research Publication and Reviews*, 5(3), 6591–6595. DOI: 10.55248/gengpi.5.0324.0875

- Michael, K., Abbas, R., & Roussos, G. (2023). AI in cybersecurity. The paradox. *IEEE Transactions on Technology and Society*, 4(2), 104–109. DOI: 10.1109/TTS.2023.3280109
- Milosevic, T., Verma, K., Carter, M., Vigil, S., Laffan, D., Davis, B., & O'Higgins Norman, J. (2023). Effectiveness of artificial intelligence-based cyberbullying interventions from youth perspective. *Social Media + Society*, 9(1), 1–12. DOI: 10.1177/20563051221147325
- Peryala, A., & Reddy, C. K. K. (2024). Utilization of generative AI in medical imaging to improve evaluation and therapy. In *Intelligent systems and IoT applications in clinical health*. IGI Global. <https://DOI: 10.4018/979-8-3693-8990-4.ch007>
- Rizvi, M. (2023). Enhancing cybersecurity. The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, 10(05), 055–060. DOI: 10.22161/ijaers.105.8
- Roshanaei, M., Khan, M. R., & Sylvester, N. N. (2024). Enhancing Cybersecurity through AI and ML. Strategies, Challenges, and Future Directions. *Journal of Information Security*, 15(3), 320–339. DOI: 10.4236/jis.2024.153019
- Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016). Cybercriminals, cyberattacks and cybercrime. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1-9). IEEE.
- Santos, O., & Radanliev, P. (2024). *Beyond the Algorithm. AI, Security, Privacy, and Ethics*. Addison-Wesley Professional.
- Shara, J. (2023). Quantum machine learning and cybersecurity. *Quantum : the Open Journal for Quantum Science*, 12(6), 47–56.
- Singh, T. M., Reddy, C. K. K., & Lippert, K. (2024). The revolution and future of blockchain technology in cybersecurity. A comprehensive analysis. In *Artificial intelligence for blockchain and cybersecurity-powered IoT applications*. CRC Press. <https://DOI: 10.1201/9781003497585>
- Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity. A comprehensive survey. *EAI Endorsed Transactions on Creative Technologies*, 8(28), e3–e3. DOI: 10.4108/eai.7-7-2021.170285
- Toapanta, S. M. T., Carpio, J. A. E., & Gallegos, L. E. M. (2020). An Approach to Cybersecurity, Cyberbullying in Social Networks, and Information Security in Public Organizations during a Pandemic. Study case COVID-19 Ecuador. In *2020 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)* (pp. 1-6). IEEE.

Vanpech, P., Peerabenjakul, K., Suriwong, N., & Fugkeaw, S. (2024). Detecting cyberbullying on social networks using language learning model. *InProceedings of the 2024 International Conference on Knowledge and Smart Technology (KST)* (pp. 1–9). IEEE. DOI: 10.1109/KST61284.2024.10499678

Wang, C., Tang, H., Zhu, H., Zheng, J., & Jiang, C. (2024). Behavioral authentication for security and safety. *Security and Safety*, 3, 2024003. DOI: 10.1051/sands/2024003