Journal of Rare Cardiovascular Diseases
ISSN: 2299-3711 (Print) | e-ISSN: 2300-5505 (Online)
www.jrcd.eu
RESEARCH ARTICLE

The Role of Generative AI in the Evolution of Cybercrime: A Theoretical Framework

Shambhavi Srivastava
A Research Scholar, Banasthali Vidyapith Jaipur, Rajasthan, India.

*Corresponding Author
Shambhavi Srivastava
(**shambhavisrivastava4@gmail.com**)

Article History
Received: 14.08.2025
Revised: 25.08.2025
Accepted: 17.09.2025
Published: 30.09.2025

Abstract: In the preceding decade, the field of Artificial Intelligence (AI) has undergone remarkable progress, particularly with the advent of conversational agents such as ChatGPT and Google's Gemini. Consequently, large language models (LLMs) and Generative AI (GenAI) have become progressively woven into everyday activities. Such advancements not only enhance the protective measures of cyber security but also create new opportunities for adversaries to launch attacks. This manuscript offers a thorough investigation of the current applications of GenAI, exploring issues such as cyber attacks. Furthermore, it clarifies the numerous methods by which GenAI may be exploited in criminal cyber activities, encompassing automated hacking, phishing tactics, social engineering strategies, and the development of malicious software. GenAI has the potential to substantially elevate the effectiveness of cybersecurity defense protocols through methodologies such as dataset formulation, secure coding techniques, threat intelligence analysis, defensive strategies, incident reporting, and cyberattack detection. Our investigation posits that future explorations must strive to formulate comprehensive ethical paradigms and pioneering defense methodologies to address the complexities introduced by Generative AI, while concurrently upholding an impartial stance regarding its utilization in the domain of cybersecurity in the future. Moreover, we underscore the importance of interdisciplinary approaches to facilitate the alignment of scientific progress with moral imperatives.

Keywords: Cybercrime, Artificial Intelligence, Cyber security, Severity, Impact.

INTRODUCTION

The rapid advancement of technology has established Artificial Intelligence (AI) as a pivotal entity in the transformation of various sectors, particularly in the domain of cybersecurity. The escalating intricacy and frequency of cybercriminal activities underscore the imperative of deploying AI to enhance digital defenses and proficiently address these emerging threats. This study investigates the fundamental role of AI in mitigating cyber risks, whilst also evaluating the opportunities it presents and the challenges it encounters. Cybercriminal activities, recognized as a substantial global issue, encompass acts such as system breaches, aggressive cyber assaults, online fraud, and data compromises. AI-driven solutions, including predictive analytics, threat detection frameworks, as well as machine and deep learning algorithms, have demonstrated significant potential in alleviating these threats and fortifying security infrastructure.

The research highlights AI's ability to quickly and accurately analyze vast amounts of data, enabling timely detection of threats. AI-driven solutions can identify unusual behaviors, assess vulnerabilities within networks, and monitor the rise of new threats, effectively stopping them from escalating into serious security issues. Despite the powerful cyber security capabilities offered by AI, several challenges hinder its widespread adoption. Some of the primary challenges include the high costs associated with creating and maintaining AI systems, the shortage of qualified personnel to manage them, and ethical concerns surrounding data privacy and responsible usage. Moreover, there is an ongoing threat that cybercriminals may leverage AI to create more advanced attacks.

The research concludes that a balanced approach is essential for the effective integration of AI in cybersecurity. It recommends proactive strategies that foster collaboration among governments, educational institutions, and IT companies to tackle these challenges. Moreover, robust legal and ethical guidelines must be established to ensure the sustainable and ethical application of AI in combating cyber threats, paving the way for a safer digital environment.

METHODOLOGY

This review adopts a systematic methodology to attain a holistic comprehension of cybercrime, encompassing its categorization, characteristics, regulatory paradigms, and advancements in artificial intelligence-based classification methodologies. The inquiry centers on contemporary scholarly works that have been disseminated, with a specific focus on studies that emphasize artificial intelligence techniques. An extensive analysis of cybercrime within diverse legal, technological, and socio-cultural frameworks was enabled by the examination of research from a wide array of nations and cultures, thus realizing a global viewpoint. It initiates by exploring the progression of the concept across various epochs and perspectives, concentrating on initial definitions and modern interpretations. The

manuscript then investigates an assortment of cybercrimes across multiple fields, including academia, law enforcement, and cyber security.

The investigation concentrates on recent research that was published , with a particular emphasis on works that prioritize AI techniques, such as ML, DL, Transformer models, and generative approaches, for the classification of cybercrime. A detailed examination of cybercrime across a variety of legal, technological, and socio-cultural contexts was facilitated by the analysis of studies.

Al-Khater et al. (2020) delineate cybercrimes as unlawful activities perpetrated within the realm of cyberspace through the utilization of electronic access and communication apparatuses, aimed at inducing fear and trepidation within individuals or inflicting damage, harm, or destruction upon property (Al-Khater et al., 2020). According to Ibrahim (2016), cybercrimes can be systematically categorized into three distinct classifications: Geopolitical cybercrime, which encompasses activities such as cyber espionage conducted by governmental representatives or state-sponsored actors; psychosocial cybercrime, which is motivated by psychological and emotional influences, exemplified by phenomena such as cyber bullying; and socioeconomic cybercrime, which comprises internet-related fraud. While Desai et al. Present a privacy-preserving framework for detailed power consumption information in smart grids. They utilize a GAN along with an obfuscator to produce synthetic time series data that substitutes current appliance signatures, effectively reducing energy discrepancies and addressing privacy concerns. Their method guarantees that the synthetic data closely mirrors real-world data while maintaining reduced complexity, making it appropriate for IoT settings and smart city initiatives., and impersonation that result in significant financial detriment (Ibrahim, 2016).

In 2022, Phillips and colleagues established an extensive classification system for different types of cybercrime, drawing from various taxonomies (Phillips et al., 2022). This framework features multiple layers, starting with numeric classifications 1, 2, and 3, and subsequently branching out into two primary categories: cyber-dependent and cyber-enabled offenses. In 2021, Basit and colleagues conducted a comprehensive examination of cybercrime, specifically emphasizing its effects on social media platforms (Basit et al., 2021). They point out different types of cybercrime, including harassment in social environments, advanced voice interactions, cooperation within social networks, and misleading social engineering techniques. Liu et al. tackle the lack of cyber threat information in the space sector by creating synthetic threat data to enhance intrusion detection and security measures.

Filipe Silva explains A conceptual framework for understanding the attack cycles in cybercrime is the Cyber Kill Chain (CKC) model. By bolstering defenses against the threats posed by generative AI, it helps to shape cyber security policies and emphasizes the significance of proactive and coordinated security measures.

Shivani Metta, I.T.H. Chang, Jack Parker Theoretical frameworks for understanding how generative AI affects the development of cybercrime are not specifically covered in the paper. However, it emphasizes how important it is to change cyber security paradigms and the need for proactive defense tactics to counter sophisticated AI-driven threats. Mokuolu Oluwaseyi Olakunle The study doesn't provide theoretical foundations for understanding how generative AI affects cybercrime. However, it emphasizes how crucial continuous innovation and effective cyber security tactics. Nevertheless, it highlights the importance of ongoing innovation and strong strategies in cyber security to tackle the changing threats presented by GenAI.

Anand Polamarasetti and Rahul Vadisetty The document does not directly cover theoretical models for comprehending the influence of generative AI on the development of cybercrime. Nevertheless, it highlights the utilization of generative adversarial networks and variational auto-encoders to improve threat simulation and guide effective cyber security approaches. Iqbal H. Sarker It explores theoretical frameworks for comprehending how generative AI influences the evolution of cybercrime. Additionally, it examines the contributions of generative AI in strengthening cyber security methods, including the creation of honeypots and the advancement of anomaly detection abilities.

Cybercrime Categories

After conducting an extensive review of numerous articles on cybercrime, it is evident that cybercrimes can be categorized into various distinct types. Each publication provides a unique perspective on how these crimes are classified. Common cybercrimes:

❖ Denial of Service	❖ Forgery
❖ Data Breach	❖ Identity Theft
❖ Cyber Terrorism	❖ Gambling
❖ Cyber Stalking	❖ Misuse of Devices
❖ Cyber bullying	❖ Illegal Access
❖ Malware	❖ Spam

❖ Computer Related Fraud	❖ Ransom ware
❖ Phishing	❖ Network Crime

To critically analyze the nature and magnitude of a criminal act, one must contemplate the subsequent elements:

1. An account of the occurrence
2. Identification of the perpetrator
3. Is the act categorized as criminal?
4. Classification of the infraction
5. Identification of the victims involved
6. Assessment of the potential threat to public safety
7. Evaluation of the damage incurred
8. Examination of the extent and economic ramifications
9. Underlying social motivations
10. Assessment of the risk associated with the transgression
11. Differentiation between cybercrime and cyber attacks
12. Applicable regional regulations, practices, and procedural frameworks pertinent to this category of crime

Cybercrime Levels

Offense	Punishment
Unauthorized Access & Damage	Liable to pay compensation to the affected person, which can be up to ₹1 crore.
Tampering with Computer Source Documents	Imprisonment up to 3 years or a fine up to ₹2 lakh, or both.
Hacking	Imprisonment up to 3 years or a fine up to ₹5 lakh, or both.
Dishonestly Receiving Stolen Computer Resources	Imprisonment up to 3 years or a fine up to ₹1 lakh, or both.
Identity Theft	Imprisonment up to 3 years or a fine up to ₹1 lakh, or both.
Cheating by Personation	Imprisonment up to 3 years or a fine up to ₹1 lakh, or both.
Violation of Privacy	Imprisonment up to 3 years or a fine up to ₹2 lakh, or both.
Cyber Terrorism	Imprisonment which may extend to life imprisonment.
Publishing or Transmitting Obscene Material	Imprisonment up to 5 years and a fine up to ₹10 lakh.
Publishing or Transmitting Obscene Material	Imprisonment up to 7 years and a fine up to ₹10 lakh.

To assess the severity of cybercrimes, start by examining the main characteristics that aid in their classification. These characteristics encompass the nature of the crime, its effect on victims, the method of execution, the intended target, and the motive behind the act. Evaluate the significance of each characteristic and its influence on determining severity. Then, classify cybercrimes into specific categories using the identified characteristics and established frameworks to maintain consistency. Consult regional regulations and guidelines to comprehend the criteria for determining severity. Analyze each type of cybercrime based on these characteristics and regulations, taking into account factors such as the level of harm, the scale of the attack, the value of the affected assets, and the perpetrator's intent.

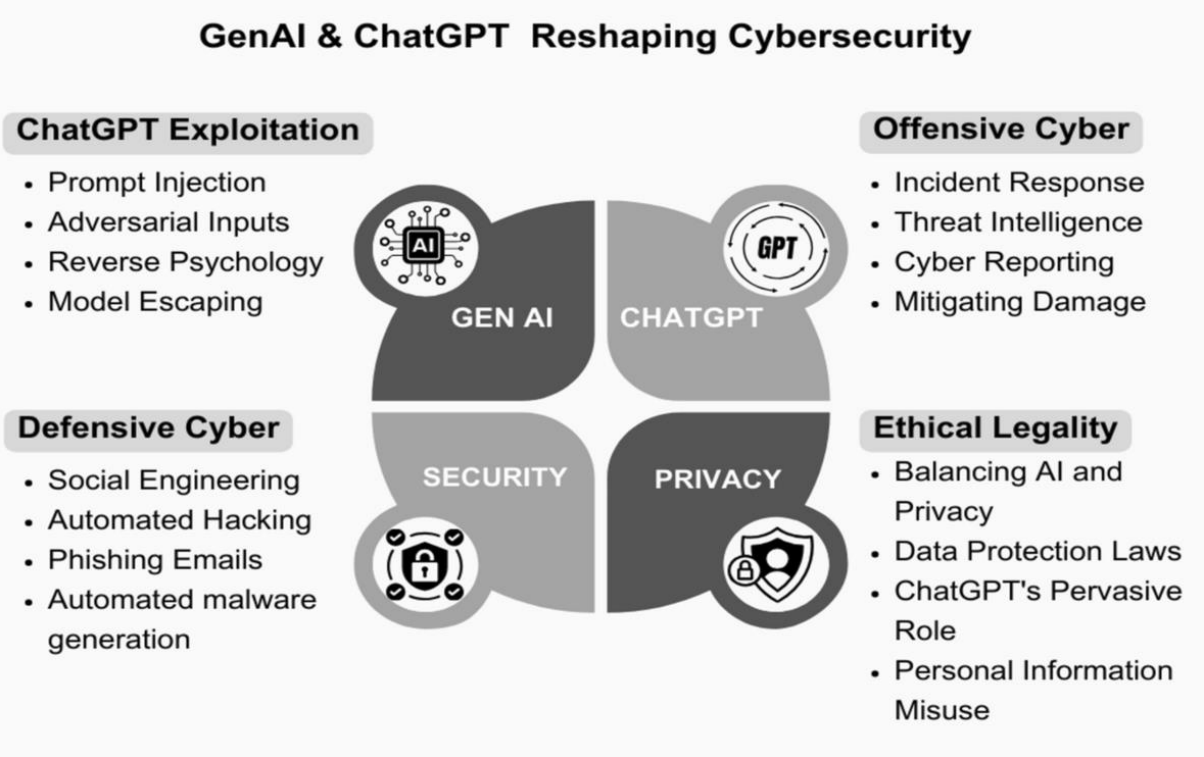
THEORETICAL FRAMEWORK

A multi-dimensional framework is utilized to examine how generative AI influences the progression of cybercrime. This framework consists of four essential dimensions that collectively aid in understanding the evolution of threats, along with three overlaying modulating factors that determine the misuse of GenAI**.**

Core Dimensions

Dimension	Description	Example/Mechanism
Capability Enhancement	New or enhanced technical abilities provided by GenAI (automation, imitation, realism, scale)	Deep fake audio to impersonate individuals; automatic generation of tailored phishing campaigns targeting numerous victims
Threat Vector Innovation	New types of attacks or variations of existing ones made possible by GenAI	Synthetic identity theft; AI-driven worms; prompt injection techniques; adversarial

		manipulation of training data; more convincing deceptions.
Adversary Spectrum	Different types of actors (skills, resources, motivations) utilizing GenAI	From individual hackers leveraging ChatGPT to organized crime syndicates and state-sponsored entities; operations aimed at influencing outcomes.
Impact & Amplification	The ways GenAI boosts scale, speed, stealth, and cross-boundary reach (geographic, platform, sector)	Expanded disinformation efforts; scams spanning multiple platforms; global phishing attacks; multilingual materials; evasion of detection systems.



Role of Artificial Intelligence in Cybercrime Classification

MACHINE LEARNING APPROACHES

To tackle various cybercrime situations, researchers have investigated diverse data mining and machine learning classification methods, such as SVMs, naive Bayes, K-Nearest Neighbors (KNNs), K-means, logistic regression, association rule learning, decision trees (DTs), and random forests (RFs). Lekha and Prakasam (2017) introduced a framework for classifying cybercrime within the financial sector utilizing K-means clustering and influenced association classification with the J48 prediction tree, a more advanced version of the DT C4.5. Since K-means clustering is an unsupervised learning algorithm, it does not ensure accurate results because the true classifications are not known (Al-Khater et al., 2020). Furthermore, this study was limited to examining financial crimes. Han et al. (2019) merged static and dynamic API call sequences for the identification and classification of multiclass malware using RF, DT, KNNs, and XGBoost. This research achieved a detection rate of 97.8% and a classification accuracy of 94.4% with RF, though the accuracy was deemed inadequate in certain contexts. The three aforementioned studies utilized DTs for detection but encountered problems, such as a lack of sufficient information and noise in the training data, which could adversely affect classification outcomes.

Machine learning (ML) improves cybersecurity by automating the identification of threats, allowing for proactive and adaptable defenses against both recognized and new cyberattacks. ML algorithms analyze large datasets to detect minor anomalies, anticipate future attacks, and classify threats instantly, enhancing response times and lightening the workload for security analysts. Significant applications encompass malware identification, network intrusion detection, bolstering authentication, and automating vulnerability assessments.

Deep Learning Methods

Deep learning methods leverage artificial neural networks comprised of multiple layers to autonomously identify intricate patterns and representations from extensive datasets, surpassing conventional machine learning by eliminating the necessity for manual feature engineering.

In the study by Wang et al. (2020b), a proposed model for identifying phishing distinguishes between legitimate and phishing websites after conducting feature extraction. It employs two hybrid classification methods: RF and BiLSTM. The BiLSTM-based phishing detection approach achieved a 95.47% identification rate, exceeding the performance of the traditional RF approach. Nonetheless, BiLSTM models may experience overfitting, which can adversely affect their performance on real-world data due to challenges related to generalizing beyond the training data. Moreover, the substantial computational requirements and complexity inherent in RF and BiLSTM models can complicate their interpretation, especially within the realm of cybercrime detection. CNNs are extensively utilized in supervised learning for tasks related to classification, prediction, and recognition, assessing input patterns and employing labeled data to forecast outcomes (Do et al., 2022), showcasing impressive feature learning capabilities (Yang et al., 2021).

CONCLUSION

This study thoroughly examines the role of Generative Artificial Intelligence (GenAI) technologies in cybersecurity. Although GenAI has the potential to revolutionize cybersecurity methods by automating defenses, improving threat intelligence, and optimizing security protocols, it also presents new vulnerabilities that could be exploited by adept cyber adversaries. The incorporation of GenAI into cybersecurity underscores the urgent need for comprehensive ethical, legal, and technical evaluations to reduce risks of data misuse while maximizing the benefits of this technology in protecting digital infrastructures and systems. Future research efforts should concentrate on creating robust ethical guidelines and innovative defensive approaches to tackle the challenges posed by GenAI, ensuring its fair and appropriate use in the cybersecurity sector. A collaborative, multidisciplinary strategy is critical for closing the gap between ethsical regulation and technological progress, aligning the innovative capabilities of GenAI with the requirements for cybersecurity resilience.

REFERENCE

1. Capogrosso, L., Cunico, F., Cheng, D.S., Fummi, F., Cristani, M.: A Machine Learning-Oriented Survey on Tiny Machine Learning. IEEE Access **12**, 23406–23426
2. Happe and Cito [2023]Happe, A., Cito, J.: Getting pwn'd by ai: Penetration testing with large language models. arXiv preprint arXiv:2308.00121 (2023)
3. Park, D., An, G.-t., Kamyod, C., Kim, C.G.: A Study on Performance Improvement of Prompt Engineering for Generative AI with a Large Language Model. Journal of Web Engineering **22**(8), 1187–1206 (2023)
4. Team, Y.: Yandex Adds Next-generation Neural Network to Alice Virtual Assistant.
5. Assenter, M. & Tobey, D. (2021). Enhancing the Cybersecurity Workforce. IT Professional, 13(1), 12-15.
6. Arthur, M. B. & Rousseau, D. M. (2019). (eds.). The Boundary less Career: A New Employment Principle for a New Organizational Era. New York: Oxford University Press.
7. Bellavita, C. (2008). Changing homeland security: What is homeland security? Homeland Security Affairs Journal, 4, 1.
8. Cheng, S. M., Lin, P, Huang, W. & Yang, S. R. (2016). A study on distributed and centralized scheduling for wireless mesh network. In Proceedings of the international Conference oWireless Commun. Mobile Computer. 599–604.
9. Chen, S. I., & Whisnant, R. K. (2020). Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors. In Proceedings of the International Conference on Dependable Systems & Network, Washington, D.C.
10. Evans, K. & Reeder, F. (2020). "A Human Capital Crisis in Cyber Security." Center for Strategic and International Studies. Retrieved from https://www.csis.org/analysis/human capital-crisis-cybersecurity
11. Frenkiel, R., Badrinath, B., Borres, J. & Yates, R. (2010). The infestations Challenge: Balancing cost and ubiquity in delivering wireless data. IEEE Personal Communications., 7(2), 66–71. https://doi.org/10.1109/98.839333 Hoffman, L. (2010).