Online Child Exploitation: The Role of Technology and Cyber Security in Preventing and Addressing Cyber Crimes during the Pandemic

N. Renuka
Research Scholar
University of Technology, Jaipur
Dr. Vimla Kumari Verma,
Research Supervisor
University of Technology, Jaipur

Abstract

As of right now, a large amount of international economic, commercial, social, and legislative activities as well as international cooperations involving individuals, non-legislative organizations, and governmental and administrative foundations are carried out online. The modern world is heavily dependent on electronic technology, so protecting this data from cyber-attacks is a challenging problem. The goal of cyberattacks is to financially harm businesses. Cyber-assaults can occasionally be used for military or political ends. Up until this time, numerous methods to prevent cyber-assaults or lessen the harm they cause have been put forth by scientists from all over the world. The goal of this study is to review and thoroughly investigate the typical advancements made in the field of cyber security as well as to look at the challenges, flaws, and strengths of the suggested techniques. Different types of new relative assaults are perceived as subtle. The set of experiences and early-stage cyber-security methods are used to analyze standard security structures. In addition, new trends and ongoing developments in cyber security, as well

as security risks and challenges, are presented. It is expected that the comprehensive audit study made available for itself and cyber security analysts will be beneficial.

Keywords: *Online Child Exploitation, Technology, Cyber security, Preventing, Addressing, Cyber Crimes, Pandemic*

1. Introduction

The internet has gradually become an essential component of children's lives, serving as a vital method for regular communication with a wide range of individuals and for pursuing a variety of interests. Children make up 33% of all Web users worldwide, with that percentage likely to be greater in low-income countries where the Internet is swiftly encroaching on all spheres of public life. However, this omnipresence is causing numerous concerns for administrators, guardians, watchmen, instructors, and organizations that support children. The use of the internet in India has grown extraordinarily over the last 20 years. Due to their affordability and availability of small information plans, mobile phones are the essential device for connecting to the internet in both urban and rural India.

On the web, customers have a ton of opportunities. However, with the availability of financial resources for one's own data on the internet, information safeguarding, protection, and security are some of the major concerns, increasing the need for cyber security as a virtually more successful and solid necessity. People who save sensitive financial information and private data online in dispersed storage accounts, for instance, are more defenseless against online threats, highlighting the unavoidable necessity to strengthen their online security. Without compromising any confidential data, cyber security creates and supports the reliability, accessibility, and secrecy of the clients' information. In this way, modern web usage and reception patterns create some concerns about an unanticipated conflict with cybercrime. Nevertheless, the role of automated reasoning in weighing these cybercrimes is evident, providing quick solutions for the police. Functional security frameworks gain certain benefits from including computerized reasoning into the cyber framework, as demonstrated by Cole et al. For instance, artificial reasoning reduces administrator fatigue, speeds up the possibility of finding cybercrimes, and enables security

employees to pay more attention where it is needed. Man-made reasoning also reduces administrative costs, maintains the dynamic cycle, provides effective solutions to eliminate internal risks, and organizes asset assignment.

In essence, an intriguing anomaly is the continually rising frequency of cybercrimes against children. According to Kumar, children are the most vulnerable segment of our population and may be easily manipulated and used. Focusing on a youngster has grown commonplace, especially in this day and age when the internet gives more transparency and convenience. Therefore, it is impressive that youngsters are using the internet more frequently without being aware of the risks. We must admit that there are harmful activities on many web platforms that only take a single tick and do consumers and kids harm.

2. Literature Review

Khweiled, Raghad & Jazzar, Mahmoud &Eleyan, Derar (2021) The coronavirus epidemic has fundamentally altered peoples' methods of living. Because of these situations, people had to struggle with new lifestyle patterns. Consequently, total and cumulative dependence on the dangerous Web network for every aspect of life. For instance, many organizations have begun to operate formally online, students have shifted to online learning, internet shopping has increased, etc. These circumstances have created the ideal environment for cybercriminals to expand their operations and take advantage of the tensions that affect human behavior to aid the success of their attacks. In order to demonstrate how cybercrime increased during the Coronavirus flare-up, this essay will study data from international organizations that specialize in online misrepresentation and cyber security. This study is important and valuable because it demonstrates how criminals take advantage of catastrophes and the necessity to develop techniques and increase client awareness in order to more easily identify and stop future cybercrime.

Ishraque Labib and Saifa Rati (2021) This study examines the impact of the Coronavirus epidemic on the rise of online harassment and obscene conduct in Bangladesh, particularly among women of all ages. The paper's main focus will be on a fundamental examination of current laws and guidelines intended to protect women's online safety. The paper acknowledges that women

can be better protected online if end provisions are added to current laws and procedures. The discussion ends with socio legitimate resolutions to the problem.

Sanjeev Kumar, (2021) The newest and trickiest problem in the online world is cybercrime. Cybercrime is an illegal act in which a computer is used as a tool or as a target. Because of the evolution of the web, anyone may now easily access information and data from one side of the world to the other. In any event, some people are misusing PCs and the internet instead of taking use of its benefits by engaging in illegal activities including online jacking, email spamming, infection attacks, and cybersex entertainment. In addition to these crimes, thugs utilize the internet to commit child abuse, a type of cybercrime. In cyberspace, the production, distribution, and use of materials depicting child sexual abuse are acts of cruelty and harm against children and youth that are comparable to new technology. The most frequent method of gaining a child's confidence to lead them toward a situation where they could be damaged is through online sales, often known as "preparing." It is forbidden to be receptive to things that could seriously or mentally harm a child or be used for other misdeeds. Provocation includes harassing, terrorizing, and tormenting. Children are the most recent victims of cybercrime. Children engage in horrible activities like internet preparing in order to become their victim. Crimes committed against children utilizing PCs and the internet include child exploitation, the creation, distribution, and ownership of child erotic entertainment, exposure to harmful substances, preparation, badgering, and sexual abuse, as well as cyberbullying. In study distributions, it was examined how online thugs abuse children and the relationship between children and cybercrime. The paper's conclusion looks at a few preventative measures.

Amrita Prakash and Ajit Singh (2021) Every aspect of a man's life is impacted by technology, including education, transportation, health care, and correspondence. The Coronavirus pandemic has significantly increased the use of technology. When we use any technology, we encounter many concerns and challenges. Security is the most important consideration while using any sophisticated Coronavirus stage. When we talk about cyber security, "cyber wrongdoing," which is growing alarmingly quickly, is the first thing that comes to mind. Cybersecurity is the process of maintaining the reliability, categorization, and accessibility (ICA) of data. Cybersecurity is

defined as the action or state of protecting and regaining projects, devices, and organizations from any sort of cyberattack. It includes an ever-evolving combination of tools, risk management techniques, innovations, planning, and best practices for defending networks, devices, projects, and information from attacks or unauthorized access. India is now the fourth most targeted nation on the planet due to the growth of cyberattacks. Cyber-assaults are becoming a more severe threat to many organizations, employees, and customers in some businesses in the midst of the coronavirus pandemic. They can be altered to obtain or completely destroy important data, change any type of information, or force people to pay. According to a review, the majority of online users are victims of cybercrime, which includes, among other things, PC viruses, spyware, Visa fraud, online scams, phishing, and mass fraud. The cost of these crimes to the nation in terms of dollars or rupees, as well as the time and money required to put things right, will be high. This study primarily focuses on the various aspects of cyber security and the challenges involved in implementing and utilizing the most recent breakthroughs during Coronavirus. Additionally, the paper examines India's legal cyber security framework.

Erola, Arnau&Epiphaniou, Gregory & Maple, Carsten &Bellekens, Xavier (2021) The 2021 Coronavirus Pandemic was a unique, unmatched occurrence that altered the lives of billions of people throughout the globe and established what is now regarded as the new normal in terms of societal norms and how we live and operate. In addition to having an impact on society and business, the pandemic also resulted in a series of noteworthy conditions relating to cybercrime. The pandemic's increased awareness increased the likelihood that cyber-assaults would be successful, leading to an increase in the quantity and variety of cyber-assaults. This article examines the Coronavirus pandemic from the perspective of cybercrime, highlighting the numerous cyberattacks that took place around the world during the pandemic. Cyber-assaults are broken down and focused on in relation to significant global events to reveal the business as usual of these tasks. The review explains how gaps that at first glance appeared to be enormous between the initial pandemic episode in China and the first cyberattack related to the Coronavirus turned out to be significantly more common, to the point where three or four separate cyberattacks were accounted for on particular days. In order to demonstrate how hackers actively created and carried

out cyber-wrongdoing operations, the study goes on to use the Unified Realm as a backdrop for research.

3. Cybercrimes against Children

When someone uses online technology to target, disturb, compromise, or actually hurt, it is known as online psychological abuse or cyber torment. They frequently encounter this provocation in addition to mental harm because smart devices are now used and claimed even by children. Posting personal information about and images of children, as well as sharing other materials that can harm the children and their reputations, are a few examples of cyberbullying. Fake documents that claim to be someone are also known to harass and do serious harm to children when they are focused on them. An investigation of child cyberbullying was directed in 28 countries by a report from Initial Public Offerings Worldwide Counselor. Results showed that after 2011, reports of cyber tormenting significantly increased.

However, despite the fact that online bullying and psychological abuse of children are commonplace, sexual crimes against them are also more prevalent. The group discovered a lot of clients using various internet platforms in 2019 to steal and trade images and videos that clearly depict sexual and perverted acts with infants and children. Another case in Spain had a suspect who had sexually explicit material for children and offered it to adults without their knowledge or consent.

4. Cyber Safety and Children – Perspectives

Concerns concerning the physical and emotional well-being of youngsters who use cutting-edge technologies are the main themes of cyber security.4 Online games are becoming more and more ingrained in kids' lives as an increasing number of households and networks gain access to the internet. Thus, it has become simple to understand how these technological advancements are also affecting how children interact, participate, learn, and teach. Understanding when these locations are likely to cause them harm has become essential in this situation. By providing answers to a few

essential questions, this part introduces important fundamental ideas on cyber-wellbeing that bridge the knowledge gap between child insurance rules and characteristics of online spaces.

1. How could we determine what is harmful to children online and how that might be so? Is it dangerous for a youngster, for instance, to be open to vulgarity or porn, to get hostile or prejudiced comments, to visit a self-harm discussion channel, or to have their long-distance interpersonal communication profile destroyed? Feelings on these vary; for instance, there is disagreement over the precise harm that results from exposing a child to pornography. Is it dangerous because it disturbs or stuns the child, because it alters the child's sexual development, or because it pressures young women to perform particular sexual gestures?

2. Where is the child's mischief at long last? In actuality, hurt is perpetually lingering as physical harm, major distress, or social prohibition. Therefore, it is important to revisit the understanding of remote harm to children in the child assurance discipline in order to understand online mischief. In actuality, other related issues to online mischief, like the extent of parental responsibility and moral questions about when exposure to the adult world is appropriate, are not web-specific issues; rather, they are related to how we view childhood and are normal topics of conversation in the disconnected world.

3. A small number of kids exhibit all the signs that they are destined to encounter danger or, when they do, destined to believe that it is harmful. persons who gamble off-line are also more likely to bet online, and persons who gamble online are also more likely to suffer other risks. This variability in the risk of online mischief can be attributed to age-related, organic, and mental components.

4. A child may gamble or have gambling experiences, but not abuse or mischief. For instance, many kids may post personal information online, which many adults may view as risk-taking behavior, but only a small percentage is likely to get into serious trouble. This reflects a discrepancy between children's and adults' perceptions of what is attractive or harmful online. Additionally, it considers the nature and frequency of complaints related to online abuse/damage. Delivering strategy estimations that successfully intervene between adults and children therefore requires taking into consideration the viewpoints of youngsters. Online safety entails tackling

online gambling by aiming to strike a balance between preventing access to open doors and taking measures to protect the defenseless from harm. Online opportunities that benefit kids may have negative side effects if restricted for some people due to advanced avoidance.

5. AI-Enabled Approaches to Counteract Cybercrimes against Children in India

Many wonder how artificial intelligence may help to reduce internet violence against minors, even while framework models may be able to balance out such acts. In order to prevent internet crimes against youngsters in India, programming designers and suppliers are providing enticing computer-based intelligence apps. It is interesting that the insightful specialist framework only handles a small portion of computational intelligence (CI), a larger framework for artificial intelligence. Fluffy Rationale, Multitude Intelligence, Artificial Safe Framework, AI, and Brain Organizations are important areas of strength for several special nature-driven abilities that fall under the umbrella of computational intelligence (CI). These techniques make it easier to make decisions, especially when web client security is needed. When we refer to the "Nature Propelled Resistant Framework," we mean a computer-based intelligence technology that can mimic the conventional safe framework and is focused on detecting crimes and has the ability to recognize, retain, process, and organize data. Therefore, the following are some significant computer-based intelligence-enabled frameworks that distinguish cybercrimes against minors and provide a means of resolving them:

❖ **Child Safe AI**

One of the leading artificial intelligence platforms, Child Safe simulated intelligence, screens web content, particularly child abuse-related information, to ensure a reduction in child maltreatment in the online environment. The US law enforcement also sends Child Safe artificial intelligence, which efficiently gathers indications about dubious activities or content from the online environment. The appropriate framework supports multiple associations by continuously monitoring and evaluating the web content, including images, videos, speeches, and other materials.

❖ **Spotlight**

Spotlight, developed by Thistle, is a computerized system for tracking online crimes against children, including child trafficking and child sex abuse. To differentiate between key exercises and casualties, this technique employs foresight evaluation. According to Oriel (2022), Spotlight uses data gleaned from escort services and sex advertising to identify the perpetrators and victims of child sexual abuse and internet trafficking. The US Government Division uses Spotlight, a similar computer-based intelligence system to Child Safe, to spot child selling activities. It is also remarkable that over 14,874 incidents of internet child trafficking have been identified and stopped thanks to Spotlight during the past four years.

❖ **AI technology by UNICRI**

According to Secretary-General of the United Nations Antonio Guterres, joint efforts to combat internet crime can protect children and ensure peace for all. The Assembled Countries Interregional Wrongdoing and Equity and Exploration Foundation uses advanced mechanics and artificial intelligence in its man-made intelligence technology for police (to identify and locate the long-missing youngsters). Additionally, it helps identify locations and activities that engage in child and illegal exploitation as well as separate illicit online sexual content. However, even though UNICRI uses advanced mechanics and simulated intelligence, the relevant technology isn't fully employed. According to UNICRI, using artificial intelligence to ensure children's safety online necessitates routinely monitoring and updating the key framework. Additionally, including computer-based intelligence technology is important since, during a considerable portion of the Coronavirus event, children's web usage increased, which led to an increase in cases of online crimes against minors. As a part of today's conclusive emerging technologies, artificial intelligence not only detects crimes but also screens what a human eye, in some situations, is unable to detect.

❖ **Google's AI Tool**

Technology colossus Google introduced a program that uses artificial intelligence to look for online crimes against minors. In addition to helping non-administrative organizations and experts

recognize the audio and video content in light of child sexual abuse, this toolkit of simulated intelligence also contained picture handling using Profound Brain Organizations. The crucial simulated intelligence tool compartment also aids the classifiers in identifying wrongdoers by identifying content that is not specifically related to child sexual abuse. According to Detrick, the Google device with artificial intelligence can help experts filter and identify more than 700% of the deplorable children's content that is available online. Although Google's artificial intelligence apparatus is prominently available without charge, it still requires human arbitrators to laboriously evaluate the profane images and other types of content, necessitating human efficiency and effort as supporting intelligent frameworks for the wrongdoing recognition.

❖ **Safer**

As one of the top AI businesses that can identify 99% of crimes against children online, Thorn created Safer. An online platform can identify, take down, and prohibit the sources and platforms used for cybercrimes against minors with the use of Safer. In its beta phase, Safer had already removed more than 100,000 pertinent files, and it will continue to get better (Gray et al., 2016). The following services are provided by Safer:

1. First Image Hash Coordination creates endless and cryptographic hashes to coordinate them with the information that contains prior instances of child sexual abuse, primarily to identify the pornographic images of children.

2. CSAM The photo Classifier determines whether a photo is consistent with the elements of child sexual abuse.

3. Video hash coordination, like picture hash coordination, provides ongoing and cryptographic hashes to coordinate them with previously published content that contains references to child sexual abuse, primarily to identify the horrifying images of children.

❖ **Griffey**

According to UK Work space (2015), Griffeye uses various computer vision and recognition tools, such as facial recognition, to examine and identify the photographs in light of the boundaries old

enough and bareness. Griffeye is also supported and used by US government organizations to counteract any online activities against children. According to the official Griffeye stage, three resources can be used to track cyber crimes against children: Examine the DI Star software, which enables users to import, interact with, and analyze the complex information related to the appalling images and videos of children available online. Examine CS Activities contains group projects that aid in the uncovering of misbehavior. For further information, see Examine CS Activities. Groups using these activities are given electronic bases for analyzing and checking the relevant material. Break down CS Undertaking finally makes it possible for the associations to continue ongoing cross-examinations over cybercrimes against minors. The Investigate CS Venture uses a special vault over time to examine and identify the suspicious data.

❖ **Some Buddy**

UNICEF developed "Some Mate," a significant piece of programming using artificial intelligence to protect kids who use the internet for socializing, learning, and entertainment. Some Pal's "Medical aid" stage assists and makes it easier for kids to report cyberbullying and provocation. It has strengths for both human oversight and artificial intelligence (intelligence based on computers) to differentiate and classify the type of provocation, offering them the most logical options regarding the next course of action. Additionally, it teaches kids to be attentive of their actions and to weigh any potential violation. According to Wrongdoing Identifier, Some Pal initially adopted a remote helper interface; nevertheless, the designers discovered the talk bots to be ineffective due to their more involved conversational nature. Therefore, Some Pal adopted a simple yet automated method of handling to offer the clients more time to elaborate on the information they received. The relevant plan yield encouraged enhancing and easing the admission capabilities.

4. Conclusion

One of the primary sources of power in the third millennium is cyberspace and related technological breakthroughs. The characteristics of cyberspace, such as its low entry costs, obscurity, bricolage, and deviation, have created the peculiarity of force dispersal, which really means that on the off chance that legislatures have so far divided the round of force among

themselves, it should be different actors, such as privately owned businesses, coordinated oppressor and criminal groups, and individuals, even though still state run administrations still hold sway. Normal circumstances won't prevent states from maintaining their public safety. The rise in cybercrimes against children in Pakistan raises more concerns about how trustworthy and popular internet spaces are among kids. Online risks and harm should be understood within the context of the larger kid assurance scene in the country/district since the web has added a new dimension to child security offerings. This shows that the current child insurance architecture can be used to implement the reaction and anticipation systems. Technology solutions are not a panacea for solving online security problems; while they may lessen the extent of online harm, they cannot create safe havens without the adoption of the proper regulations, training of the current child insurance labor force, and client empowerment.

References

1. Aiello, L. M., & McFarland, D. (2014). Detecting child grooming behaviour patterns on social media. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8851, 16.

2. Alhumaid, K., Habes, M., &Salloum, S. A. (2021). Examining the factors influencing the mobile learning usage during COVID-19 pandemic: An integrated SEM-ANN method. IEEE Access, 9(July), 102567–102578.

3. Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. January, 170–192.

4. Chandra, M. (2019). Reduction of cyber crimes by effective use of artificial intelligence techniques. International Journal of Recent Technology and Engineering (IJRTE), 4, 8643–8645.

5. Charalambous, E., Kavallieros, D., Brewster, B., Leventakis, G., Koutras, N., &Papalexandratos, G. (2016). Combatting cybercrime and sexual exploitation of children: An open source toolkit. Open Source Intelligence Investigation.

6. Coole, M., Evans, D., &Medbury, J. (2021). Artificial intelligence in security: Opportunities and implications.

Free / Unpaid
Peer Reviewed
Multidisciplinary
International

7. *Detrick, H. (2018). Google's new AI tool to fight child sexual abuse will help reviewers scan 700% more material.*

8. *Dilek, S. (2017). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review., 6(1), 21–39.*

9. *EUROPOL. (2022). 146 children worldwide saved in an operation targeting child abuse online.*

10. *Finch, A., &Ryckman, L. (2020). Strategies to prevent online sexual abuse of children: A systematic review of the literature protocol. March, 1–7.*

11. *Global Human Rights Defence. (2021a). Cybercrime towards children in Pakistan.*

12. *Jarno, K., & November, T. (2020). Cyberbullying, an overlooked and ever growing danger to the development of children. November, 1–23.*

13. *Lewczuk, K., Wójcik, A., & Gola, M. (2021). Increase in the prevalence of online pornography use: Objective data analysis from the period between 2004 and 2016 in Poland. Archives of Sexual Behavior.*

14. *Rehnström, F. (2021). How capable is artificial intelligence (AI) in crime prediction and prevention?*

15. *Sunde, N., &Sunde, I. M. (2021). Article fagfellevurdert conceptualizing an AI-based police robot for preventing online child sexual exploitation and abuse: July.*

Author's Declaration

I as an author of the above research paper/article, here by, declare that the content of this paper is prepared by mean if any person having copyright issue or patent or anything other wise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website/amendments/updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and the entire content is genuinely mine. If any issue arise related to Plagiarism / Guide Name / Educational Qualification / Designation/Address of my university/college/institution/ Structure or Formatting/

N. Renuka
Dr. Vimla Kumari Verma

******