# A DISSERTATION ON THE ROLE OF ARTIFICIAL INTELLIGENCE IN PREVENTING CYBERCRIME

Submitted to

Guru Ghasidas Vishwavidyalaya, Bilaspur(C.G.)

**For the Partial fulfilment of paper IV of M.A. IV SEMESTER In Journalism & Mass Communication**

**Academic Session: 2022-2023**

Submitted To:

Research Guide:

Dr. Amita

Assistant Professor

Submitted By:

Apurva Rani

Roll no. 21008105

Enrollment no.- GGV/21/00504

**Department of Journalism & Mass Communication Guru Ghasidas Vishwavidyalaya, Bilaspur(C.G.)**

# SUPERVISOR'S CERTIFICATE

This is to certify that the Research report title on "Role of AI in preventing cybercrime ' is an original work done by Apurva Rani as a partial fulfillment of the requirement of Master of Journalism and Mass Communication, Guru Ghasidas University, Bilaspur. The report has been prepared under my guidance and is a record of the bonafide work carried out successfully. She has completed her project work under my supervision and guidance. I wish her a bright future.

Amita

Dr. Amita

Assistant professor
Dept. of Journalism and Mass communication
Guru ghasidas University
Bilaspur

# Chapter 1
# Introduction and Research Methodology

## I. INTRODUCTION

The rapid advancement of technology in the digital age has brought numerous benefits and conveniences to society. However, it has also given rise to a new form of crime known as cybercrime. Cybercriminals exploit vulnerabilities in computer systems and networks to gain unauthorized access, steal sensitive information, conduct financial fraud, and disrupt critical infrastructure. The ever-evolving nature of cyber threats poses significant challenges to traditional security measures, necessitating innovative approaches to combat this growing menace. Artificial Intelligence (AI) has emerged as a promising tool in preventing cybercrime. AI refers to the development of intelligent systems that can perform tasks that typically require human intelligence, such as learning, problem-solving, and decision-making. Through the use of algorithms and machine learning techniques, AI has the potential to revolutionize the field of cybersecurity by enhancing threat detection, anomaly detection, user behavior analysis, and incident response. The primary objective of this dissertation is to explore the role of AI in preventing cybercrime. By analyzing its applications and examining the existing literature, this study aims to shed light on the effectiveness of AI in combating cyber threats. Furthermore, it aims to highlight the ethical considerations surrounding the use of AI in cybersecurity.

To provide a comprehensive understanding of the topic, this dissertation will commence with a thorough literature review. The literature review will offer an overview of cybercrime, including its types, motives, and impact on individuals, organizations, and society. Additionally, it will delve into the traditional approaches to cybersecurity and discuss their strengths and limitations. Following the literature review, this study will introduce the concept of AI and its potential in addressing the limitations of traditional security measures. It will explore the various applications of AI in cybercrime prevention, such as threat detection, anomaly detection, user behavior analysis, and incident response. Each application will be examined in detail to understand its underlying mechanisms and benefits. One of the key areas of focus in this dissertation is threat detection. AI can be employed to analyze network traffic, identify patterns, and detect known and unknown cyber attack signatures. By utilizing machine learning algorithms, AI can continuously learn and adapt to evolving threats, significantly enhancing the accuracy and speed of threat detection.

Anomaly detection is another critical aspect where AI can play a significant role. By establishing normal patterns of system behavior, AI algorithms can identify deviations that may indicate potential cyber threats. This proactive approach allows for early detection and mitigation of attacks, reducing the potential impact of cybercriminal activities. User behavior analysis is an emerging area where AI can contribute to preventing cybercrime. AI algorithms can analyze user activities, create behavior profiles, and detect suspicious or abnormal behaviors that may indicate insider threats or compromised accounts. By continuously monitoring user behavior, AI can assist in detecting and mitigating potential security breaches.