# A Machine Learning Framework for Detection and Documentation of Cyberstalking on Non-Spam Email

**Arvind Kumar Gautam[1],**
[1]Department of Computer Science, IGNTU,
Amarkantak, M.P., India,
analyst.igntu@gmail.com

**Dr. Abhishek Bansal[2]**
[2]Assistant Professor, Department of Computer Science,
IGNTU, Amarkantak, M.P., India,
abhishek.bansal@igntu.ac.in

**Abstract:** Cyberstalking is growing as a social and international problem and creating the pandemic situation for users of internet applications. In modern days of life due to huge use of the Internet technology, cyberstalking has become a major fear for users, society and institutions. Like social media, cyberstalkers are using the email technology to target the victim as cyberstalking. Email is widely used internet applications and so much popular to share the information among peoples and organizations for personal, business and official purpose. Generally cybercriminal use the fake email id either from popular email service provide or from fake email service provider to perform the cybercrimes such as phishing, spamming and cyberstalking. Mostly, through spam email, victims were targeted but in the recent trends non-spam email is also using by the criminals for cyberstalking and cyberbullying. Victim can be easily targeted by cyberstalker using the non-spam email because cyberstalker often use the fake email id and messages which is difficult to block and filter as spam email category. Filtration, Detection and proper evidence documentation of non-spam email based cyberstalking are a challenging and interesting task for researchers. In this paper, we are proposing a Machine Learning framework to filter, detect, and collect cyberstalking evidence on textual data of non-spam email.