E-MAILSINK AI : DEEP LEARNING MODEL FOR MULTICLASS E-MAIL CLASSIFICATION FOR FORENSIC ANALYSIS.

Abstract

Under the guidance of
Dr.S.Saravanan.M.E.,Ph.D

E-mail is an essential application for carrying out transactions and efficiency in business processes to improve productivity. E-mail is frequently used as a vital medium of communication and is also being used by cybercriminals to commit crimes. Cybercrimes like hacking, spoofing, phishing, E-mail bombing, whaling, and spamming are being performed through E-mails. Hence, there is a need for proactive data analysis to prevent cyber-attacks and crimes. To investigate crimes involving Electronic Mail (e-mail), analysis of both the header and the email body is required since the semantics of communication helps to identify the source of potential evidence. With the continued growth of data shared via emails, investigators now face the daunting challenge of extracting the required semantic information from the bulks of emails, thereby causing a delay in the investigation process. The existing email classification approaches lead towards irrelevant E-mails and/or loss of valuable information. Keeping in sight these limitations, this project proposed to design a novel efficient approach named E-mailSinkAI for E-mail classification into four different classes: Normal, Fraudulent, Threatening, and Suspicious E-mails by using LSTM based GRU. The LSTM based GRU efficiently captures meaningful information from E-mails that can be used for forensic analysis as evidence. E-mailSinkAI effectively out performs existing methods while keeping the classification process robust and reliable.