GALGOTIAS UNIVERSITY

SCHOOLOFCOMPUTINGSCIENCE&ENGINEERING

PROJECTAPPROVALFORMANDABSTRACTF

all 2023-2024

B. Tech

ProjectDetails:Project Group ID: BT3581

Title	Email spam Detection with Machine Learning		
Project Type	☐ Community based designproblem (Interdisciplinary) ☐ Sustainable development goal ☐ App Development / Utility ☐ IOT/ML/Others	**Project Outcome**	☐ Project and Research ☐ PaperProject and Patent ☐ ProjectandBookChapter
Publication Target	☐ SCOPUSJournal ☐ SCOPUSConference ☐ SCOPUSBookChapter ☐ Patent	**GuideName: Mr Manikant Panthi**	

StudentDetails:

S. No	Name	Enrollment Number	Admission Number	Program /Branch	Sem
1	NEERAJ SINGH	21131011567	21SCSE1011675	BTECH/CSE	V
2	FAISAL HUSSAIN	21131011548	21SCSE1011654	BTECH/CSE	V
3	GAURAV KUMAR	21131012416	21SCSE1010962	BTECH/CSE	V

GuideLinesforOnePageAbstract:

1. ProjectTitleshouldbeinboldletters maximumoftwolines, andthefontmustbeinTimesNewroman with thesize of 22and it shouldbeincenteralignment.
2. TheAbstractshouldhaveminimumof150wordsandmaximumof250words.
3. TheAbstractshouldbeinJustifyalignment,andthefontmustbeinTimes Newromanwiththesize of 14 and the linespacingmustbe in 2.0 exactly.
4. Pleasereferthenextpagefortheabstractformat.

Email spam Detection with Machine Learning

Area/Domain of Project: Data Management and Machine Learning

ABSTRACT

- Email has become a crucial means of communication in various domains, ranging from personal to business settings. However, the prevalence of email spam poses a significant threat to the security and efficiency of communication systems. This project aims to address the challenge of identifying and filtering email spam through the application of advanced machine learning techniques.

- Despite existing spam filters, sophisticated spamming techniques continue to evade detection, leading to an increased risk of data breaches, malware dissemination, and phishing attacks. This project seeks to bridge the gap in current spam detection methodologies by developing a robust machine learning model that can adapt to the evolving nature of spamming tactics. By leveraging natural language processing and feature engineering, the study intends to enhance the accuracy and efficiency of spam detection, thereby minimizing the risk of fraudulent activities and preserving the integrity of email communication.

- The outcomes of this research are vital in fortifying cybersecurity measures and safeguarding sensitive information from malicious intrusions. By effectively differentiating between legitimate and spam emails, the proposed model can contribute to bolstering data protection, maintaining user privacy, and ensuring seamless communication channels. Given the critical role of email in contemporary communication, addressing the issue of spam through advanced machine learning methodologies is essential for reinforcing the security infrastructure and fostering a secure digital environment.

SignatureofStudent

SignatureofGuide