DETECTION OF MALICIOUS SOCIAL BOTS

A project report submitted in partial fulfillment of the requirements for the award of the Degree of

BACHELOR OF TECHNOLOGY
In
COMPUTER SCIENCE AND ENGINEERING

Submitted by:

P. SHARMILA
Regd. No.18811A0546

M. DEVI PRIYANKA
Regd.No.18811A0545

D.VANI VASUNDHARA
Regd.No.18811A0508

G. BHARADWAZ
Regd.No.18811A0512

A.Y.V.M. VARMA
Regd.No.19815A0505

Under the guidance of

MR. B. GANESH (M.TECH, Ph.D)
Assistant professor

Department of Computer Science and Engineering

AVANTHI INSTITUTE OF ENGINEERING &TECHNOLOGY
(Approved by AICTE, New Delhi & Permanently affiliated to JNTU Kakinada)
(Accredited by NAAC, UGC & NBA, AICTE)
MAKAVARAPALEM, NARSIPATNAM,
VISAKHAPATNAM DIST
(2018-2022)

AVANTHI INSTITUTE OF ENGINEERING &TECHNOLOGY

(Approved by AICTE, New Delhi & Permanently affiliated to JNTU Kakinada)(Accredited by NAAC, UGC & NBA, AICTE)
MAKAVARAPALEM,NARSIPATNAM,
VISAKHAPATNAM-531113

CERTIFICATE

This is to certify that the project entitled "DETECTION OF MALICIOUS SOCIAL BOTS" in partial fulfillment for the of degree of Bachelor of Technologyin COMPUTER SCIENCE AND ENGINEERING. at AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY, MAKAVARAPALEM, VISAKHAPATNAM is an bonafide work carried out by P. SHARMILA (18811A0546),M.DEVI PRIYANKA(18811A0545), D. VANI VASUNDHARA (18815A0508), G. BHARADWAZ NAIDU (18811A0512), A.Y.V.M.VARMA(19815A0505) under the guidance and supervision during 2021-2022.

Project Guide

Head of the Department

External Examiner

ABSTRACT

Malicious social bots generate fake tweets and automate their social relationships either by pretending e a follower or by creating multiple fake accounts with malicious activities. Moreover, malicious social bots st shortened malicious URLs in the tweet in order to redirect the requests of online social networking ticipants to some malicious servers. Hence, distinguishing malicious social bots from legitimate users is one the most important tasks in the Twitter network. To detect malicious social bots, extracting URL-based features ch as URL redirection, frequency of shared URLs, and spam content in URL) consumes less amount of time comparison with social graph-based features (which rely on the social interactions of users). Furthermore, licious social bots cannot easily manipulate URL redirection chains. In this project, a learning automata-based licious social bot detection (LA-MSBD) algorithm is proposed by integrating a trust computation model with L-based features for identifying trustworthy participants (users) in the Twitter network. Experimentation has en performed on Twitter data sets, and the results illustrate that the proposed algorithm achieves improvement precision, recall, F-measure, and accuracy compared with existing approaches for MSBD.