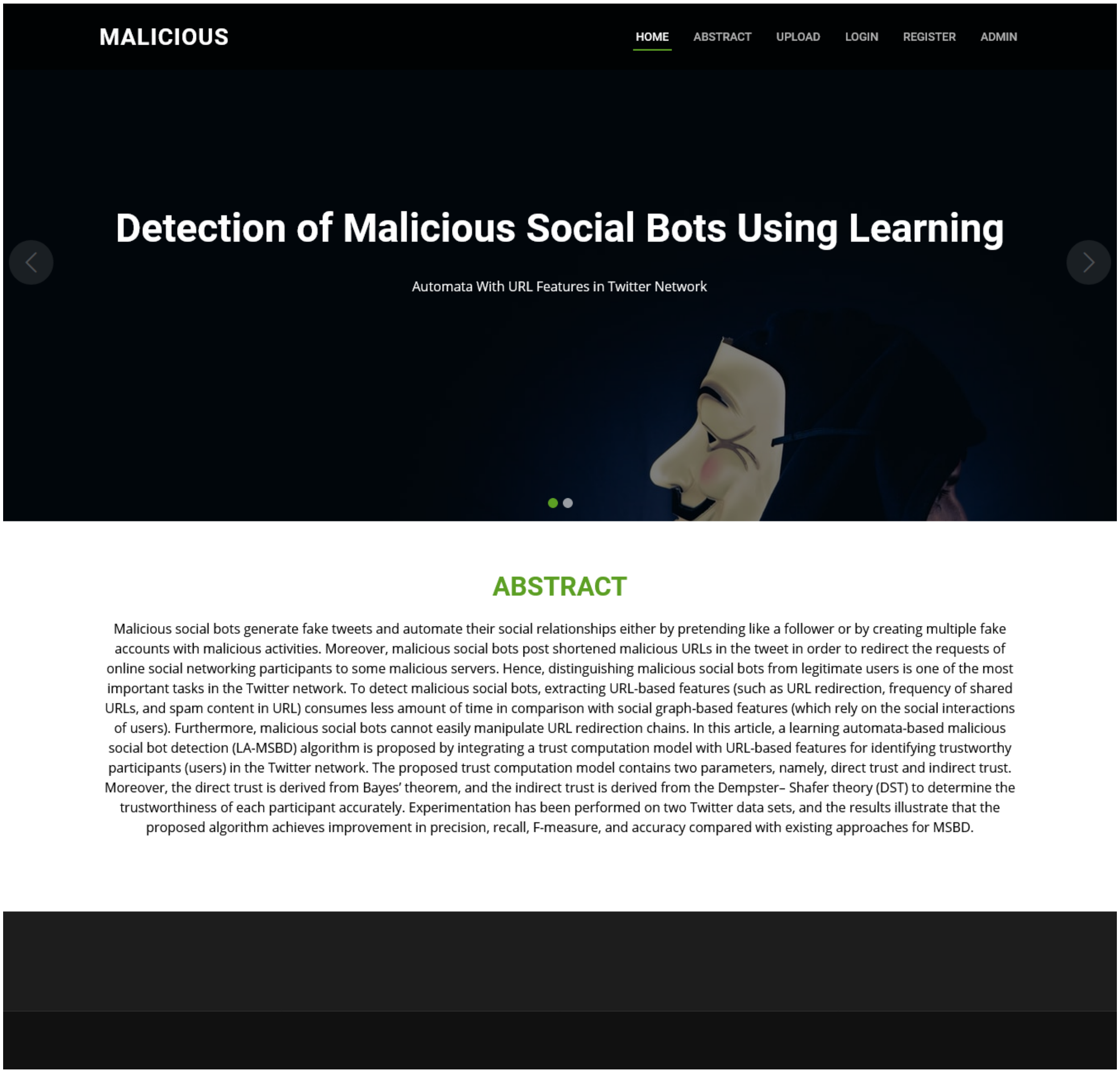
SCREEN SHOTS

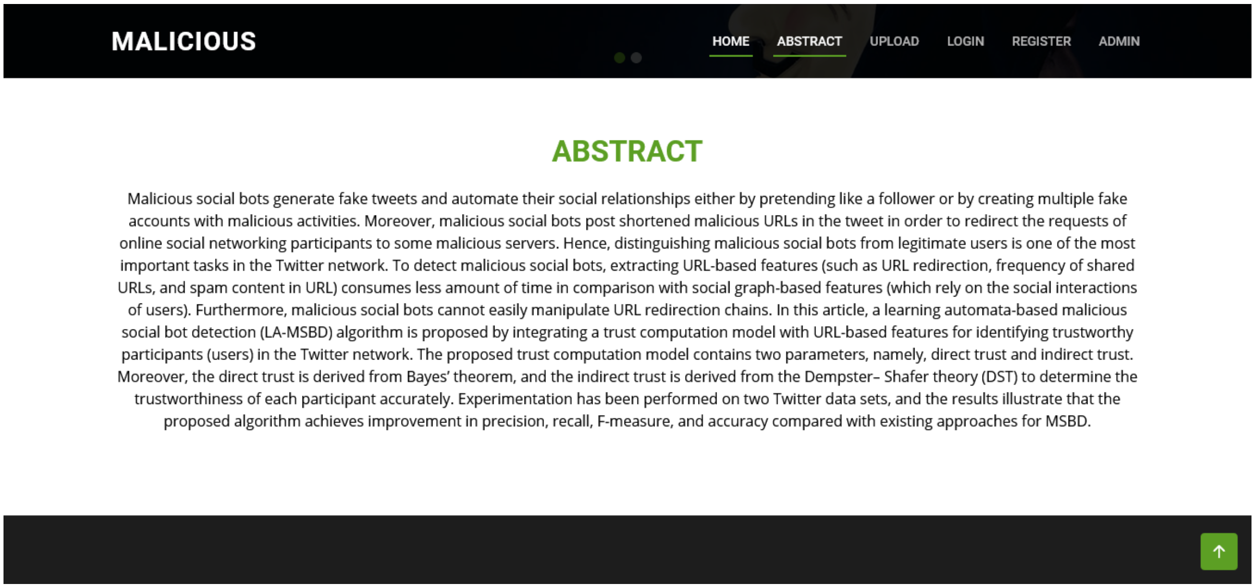


Detection of Malicious Social Bots Using Learning

Automata With URL Features in Twitter Network

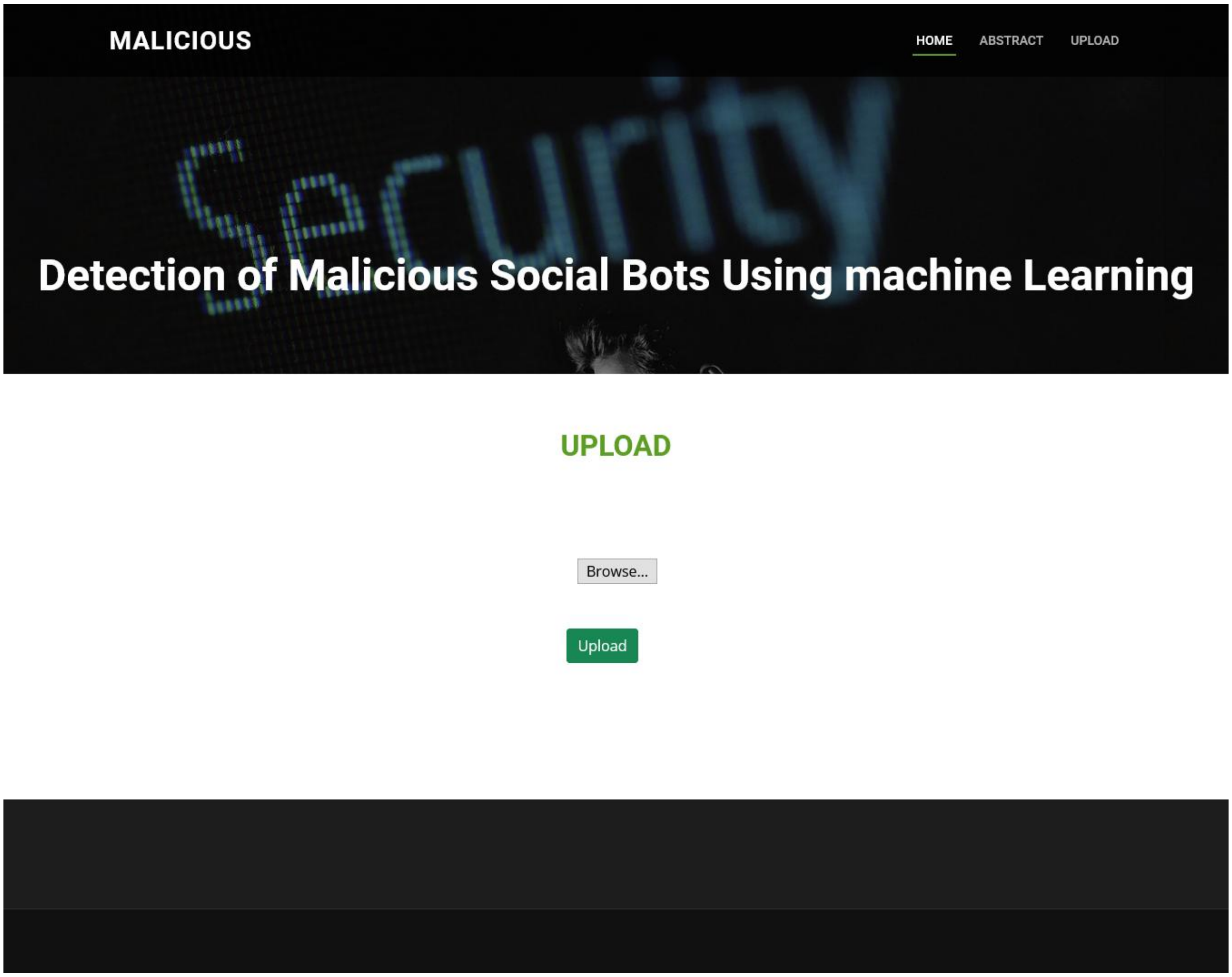
ABSTRACT

Malicious social bots generate fake tweets and automate their social relationships either by pretending like a follower or by creating multiple fake accounts with malicious activities. Moreover, malicious social bots post shortened malicious URLs in the tweet in order to redirect the requests of online social networking participants to some malicious servers. Hence, distinguishing malicious social bots from legitimate users is one of the most important tasks in the Twitter network. To detect malicious social bots, extracting URL-based features (such as URL redirection, frequency of shared URLs, and spam content in URL) consumes less amount of time in comparison with social graph-based features (which rely on the social interactions of users). Furthermore, malicious social bots cannot easily manipulate URL redirection chains. In this article, a learning automata-based malicious social bot detection (LA-MSBD) algorithm is proposed by integrating a trust computation model with URL-based features for identifying trustworthy participants (users) in the Twitter network. The proposed trust computation model contains two parameters, namely, direct trust and indirect trust. Moreover, the direct trust is derived from Bayes' theorem, and the indirect trust is derived from the Dempster– Shafer theory (DST) to determine the trustworthiness of each participant accurately. Experimentation has been performed on two Twitter data sets, and the results illustrate that the proposed algorithm achieves improvement in precision, recall, F-measure, and accuracy compared with existing approaches for MSBD.



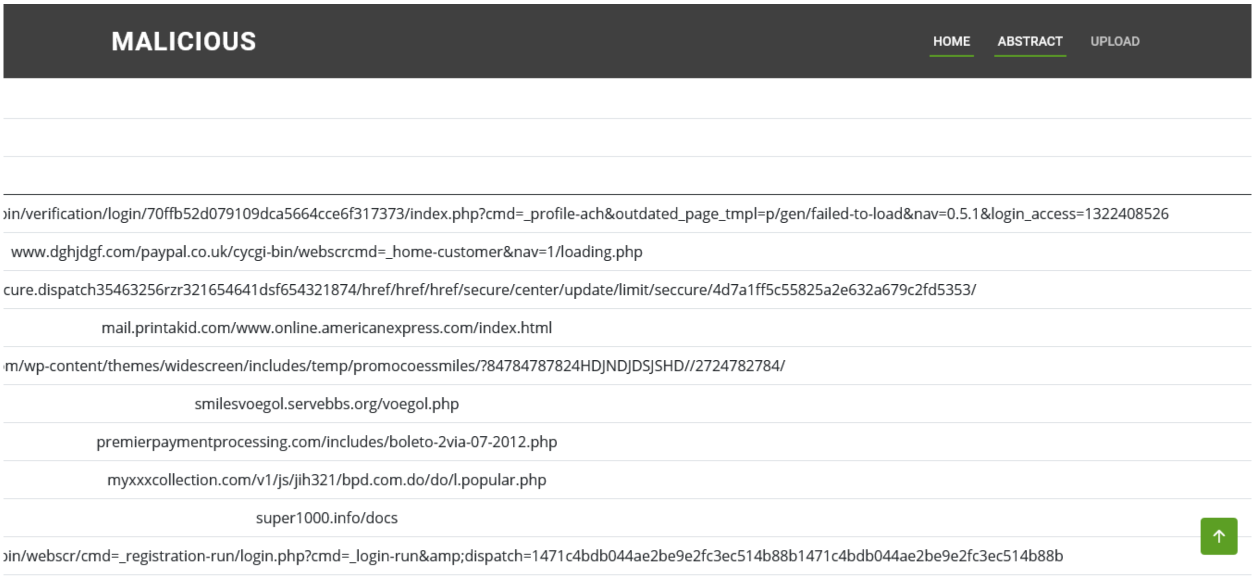
ABSTRACT

Malicious social bots generate fake tweets and automate their social relationships either by pretending like a follower or by creating multiple fake accounts with malicious activities. Moreover, malicious social bots post shortened malicious URLs in the tweet in order to redirect the requests of online social networking participants to some malicious servers. Hence, distinguishing malicious social bots from legitimate users is one of the most important tasks in the Twitter network. To detect malicious social bots, extracting URL-based features (such as URL redirection, frequency of shared URLs, and spam content in URL) consumes less amount of time in comparison with social graph-based features (which rely on the social interactions of users). Furthermore, malicious social bots cannot easily manipulate URL redirection chains. In this article, a learning automata-based malicious social bot detection (LA-MSBD) algorithm is proposed by integrating a trust computation model with URL-based features for identifying trustworthy participants (users) in the Twitter network. The proposed trust computation model contains two parameters, namely, direct trust and indirect trust. Moreover, the direct trust is derived from Bayes' theorem, and the indirect trust is derived from the Dempster– Shafer theory (DST) to determine the trustworthiness of each participant accurately. Experimentation has been performed on two Twitter data sets, and the results illustrate that the proposed algorithm achieves improvement in precision, recall, F-measure, and accuracy compared with existing approaches for MSBD.



Detection of Malicious Social Bots Using machine Learning

UPLOAD



in/verification/login/70ffb52d079109dca5664cce6f317373/index.php?cmd=_profile-ach&outdated_page_tmpl=p/gen/failed-to-load&nav=0.5.1&login_access=1322408526

www.dghjdgf.com/paypal.co.uk/cycgi-bin/webscrcmd=_home-customer&nav=1/loading.php

cure.dispatch35463256rzr321654641dsf654321874/href/href/href/secure/center/update/limit/seccure/4d7a1ff5c55825a2e632a679c2fd5353/

mail.printakid.com/www.online.americanexpress.com/index.html

m/wp-content/themes/widescreen/includes/temp/promocoessmiles/?84784787824HDJNDJDSJSHD//2724782784/

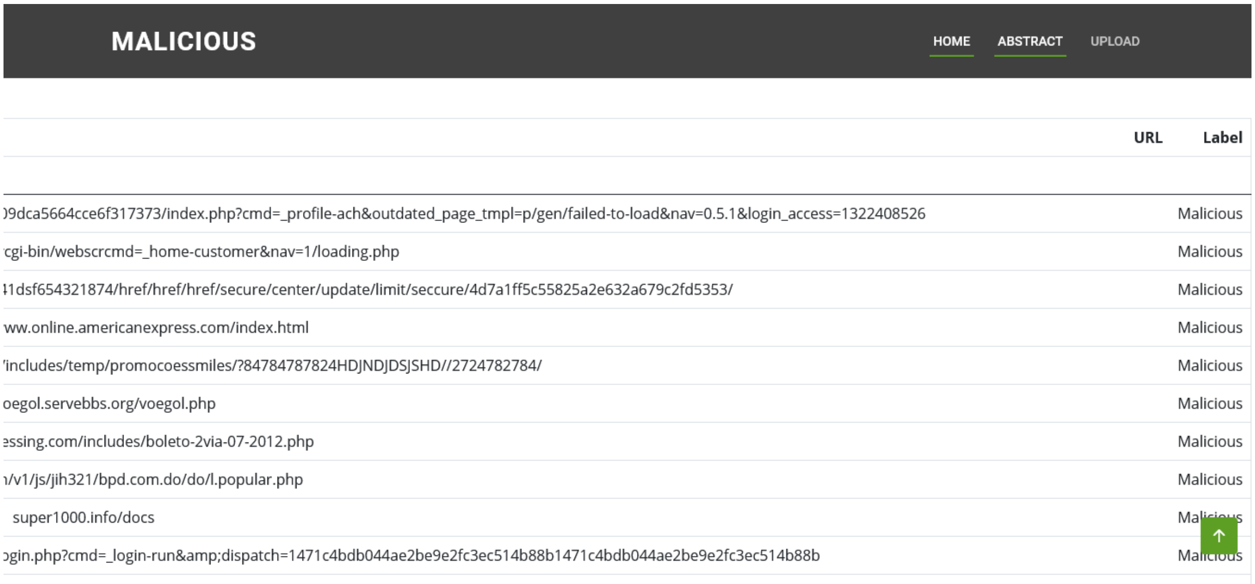
smilesvoegol.servebbs.org/voegol.php

premierpaymentprocessing.com/includes/boleto-2via-07-2012.php

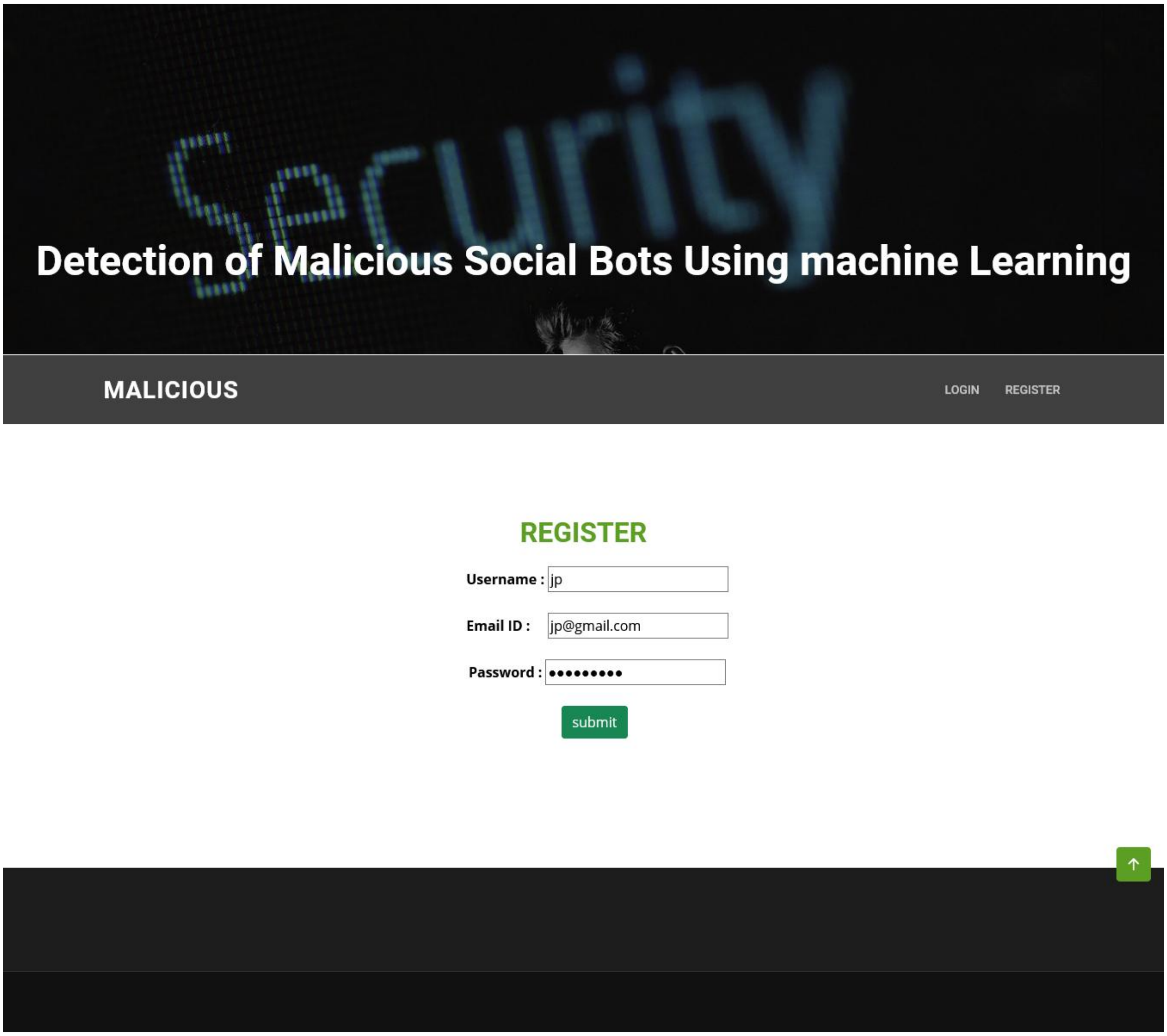
myxxxcollection.com/v1/js/jih321/bpd.com.do/do/l.popular.php

super1000.info/docs

in/webscr/cmd=_registration-run/login.php?cmd=_login-run&amp;dispatch=1471c4bdb044ae2be9e2fc3ec514b88b1471c4bdb044ae2be9e2fc3ec514b88b



URL	Label
09dca5664cce6f317373/index.php?cmd=_profile-ach&outdated_page_tmpl=p/gen/failed-to-load&nav=0.5.1&login_access=1322408526	Malicious
cgi-bin/webscrcmd=_home-customer&nav=1/loading.php	Malicious
41dsf654321874/href/href/href/secure/center/update/limit/seccure/4d7a1ff5c55825a2e632a679c2fd5353/	Malicious
ww.online.americanexpress.com/index.html	Malicious
/includes/temp/promocoessmiles/?84784787824HDJNDJDSJSHD//2724782784/	Malicious
oegol.servebbs.org/voegol.php	Malicious
essing.com/includes/boleto-2via-07-2012.php	Malicious
n/v1/js/jih321/bpd.com.do/do/l.popular.php	Malicious
super1000.info/docs	Malicious
ogin.php?cmd=_login-run&amp;dispatch=1471c4bdb044ae2be9e2fc3ec514b88b1471c4bdb044ae2be9e2fc3ec514b88b	Malicious



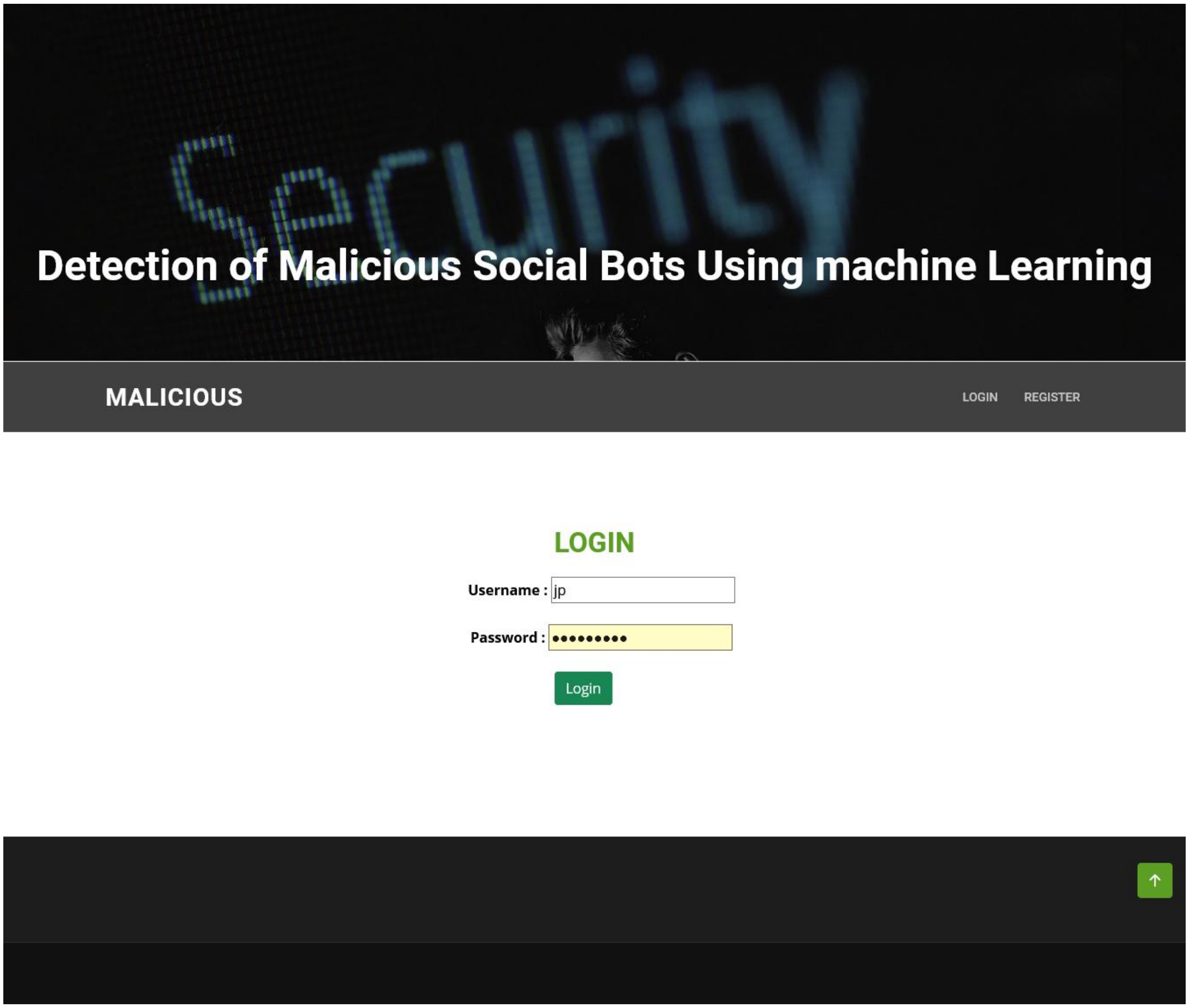
Detection of Malicious Social Bots Using machine Learning

REGISTER

Username : jp

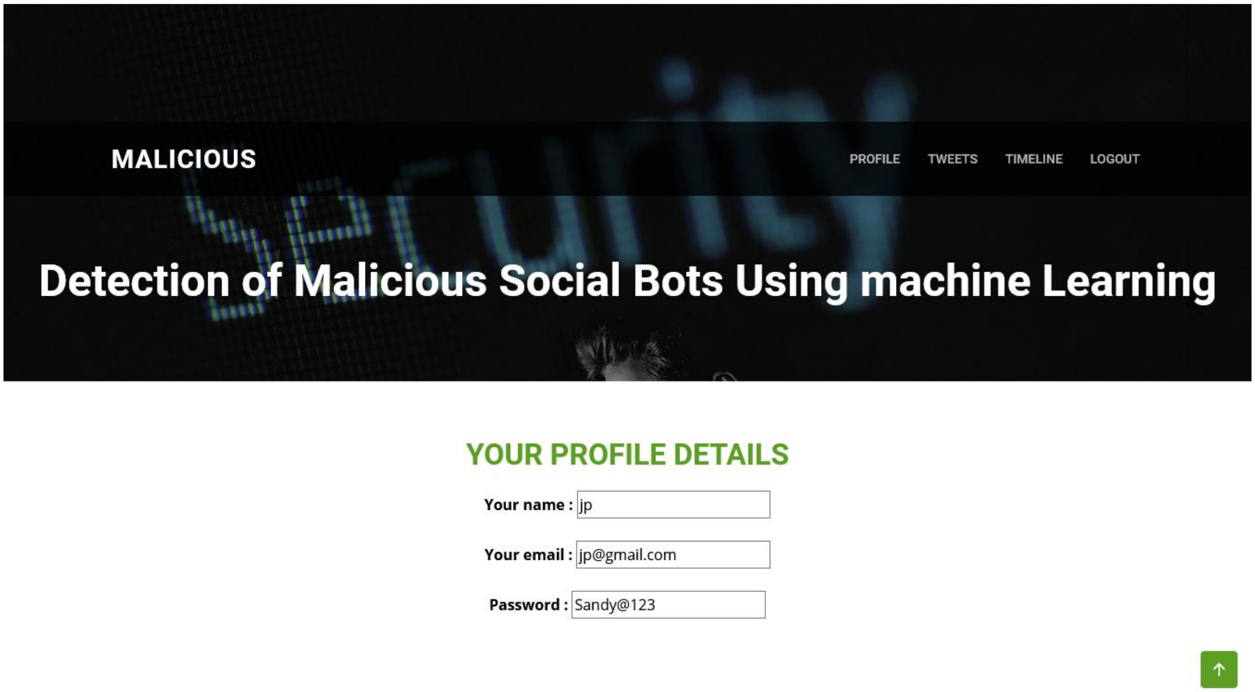
Email ID : jp@gmail.com

Password : ●●●●●●●●●



Username : jp

Password : ●●●●●●●●●



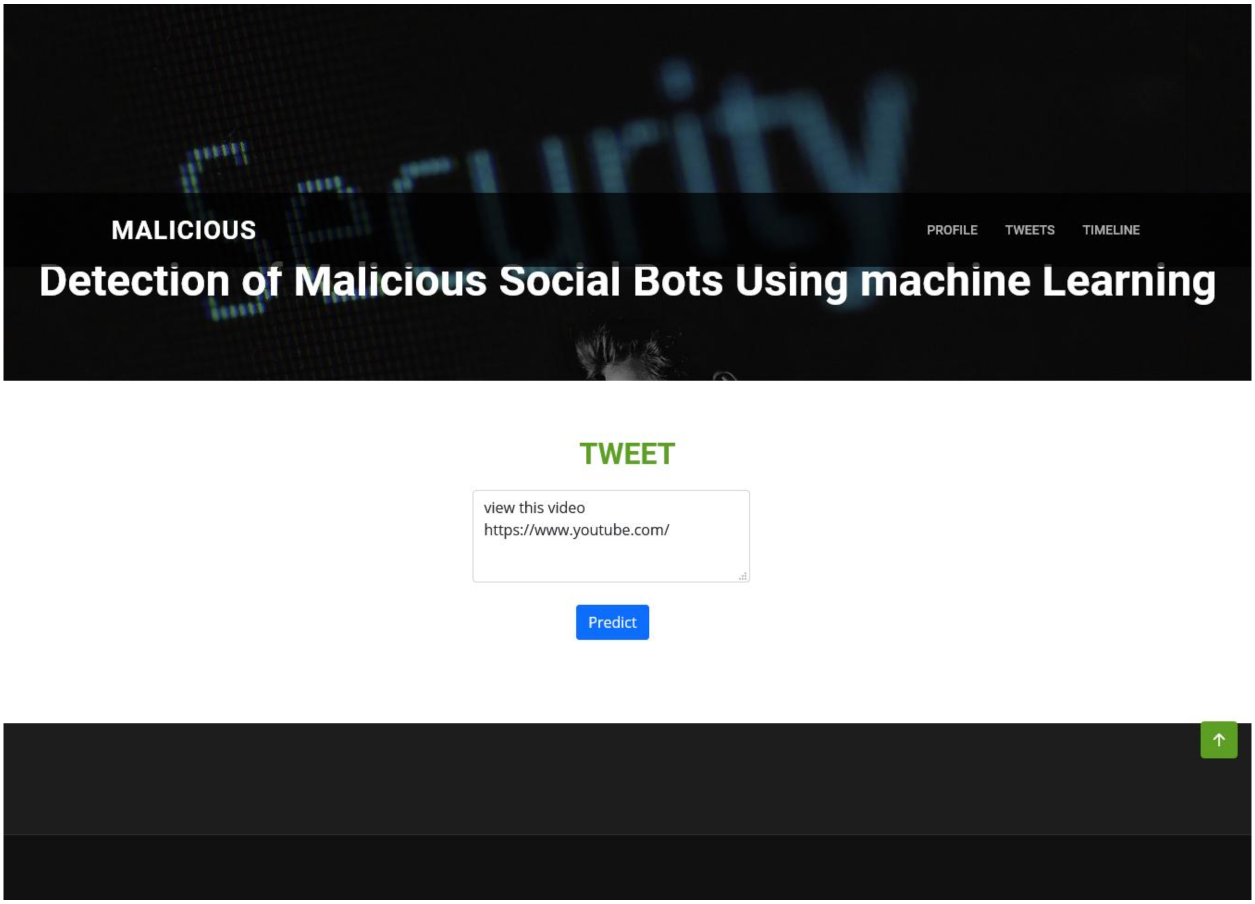
Detection of Malicious Social Bots Using machine Learning

YOUR PROFILE DETAILS

Your name : jp

Your email : jp@gmail.com

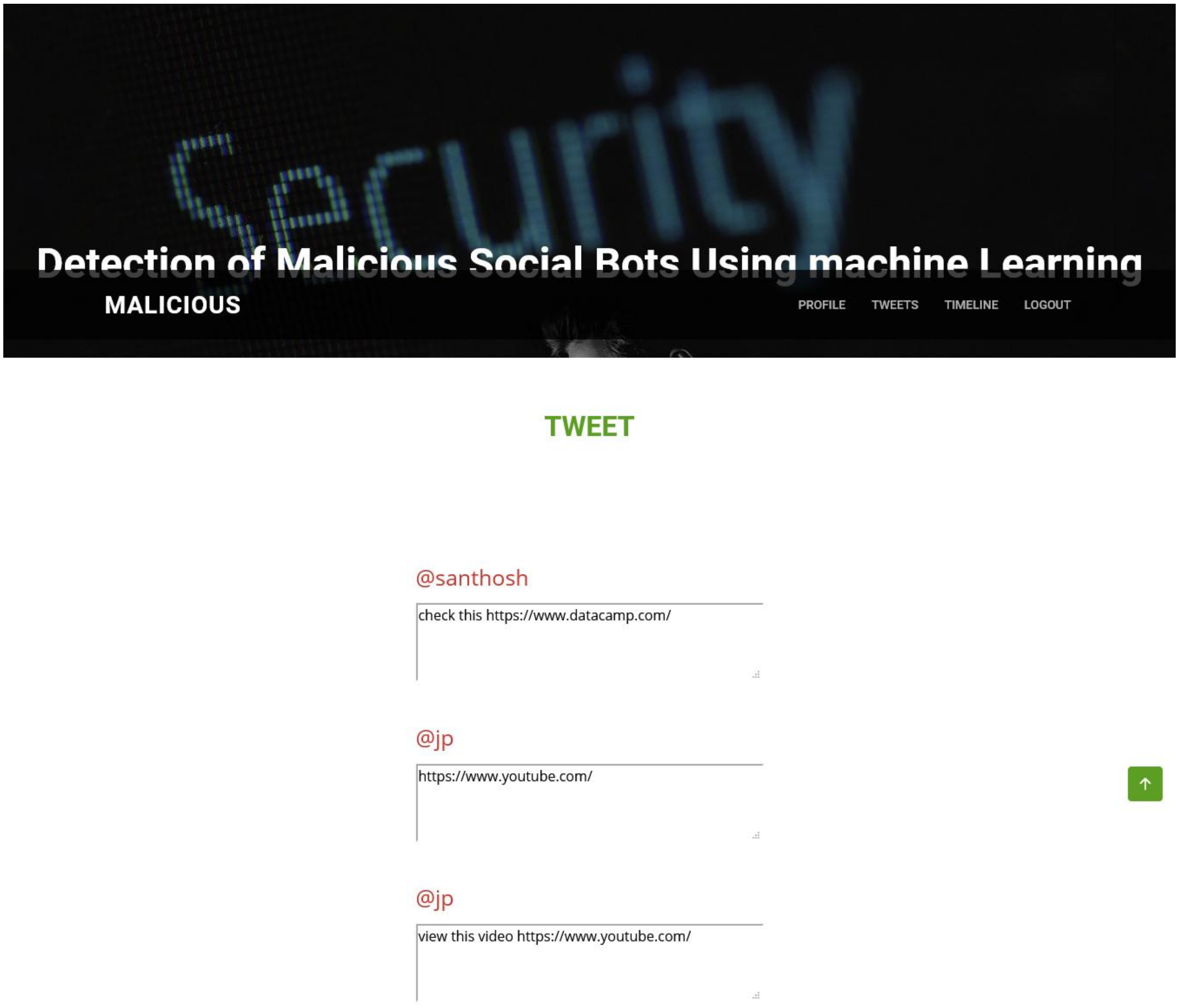
Password : Sandy@123



Detection of Malicious Social Bots Using machine Learning

TWEET

view this video
https://www.youtube.com/



Detection of Malicious Social Bots Using machine Learning

TWEET

@santhosh

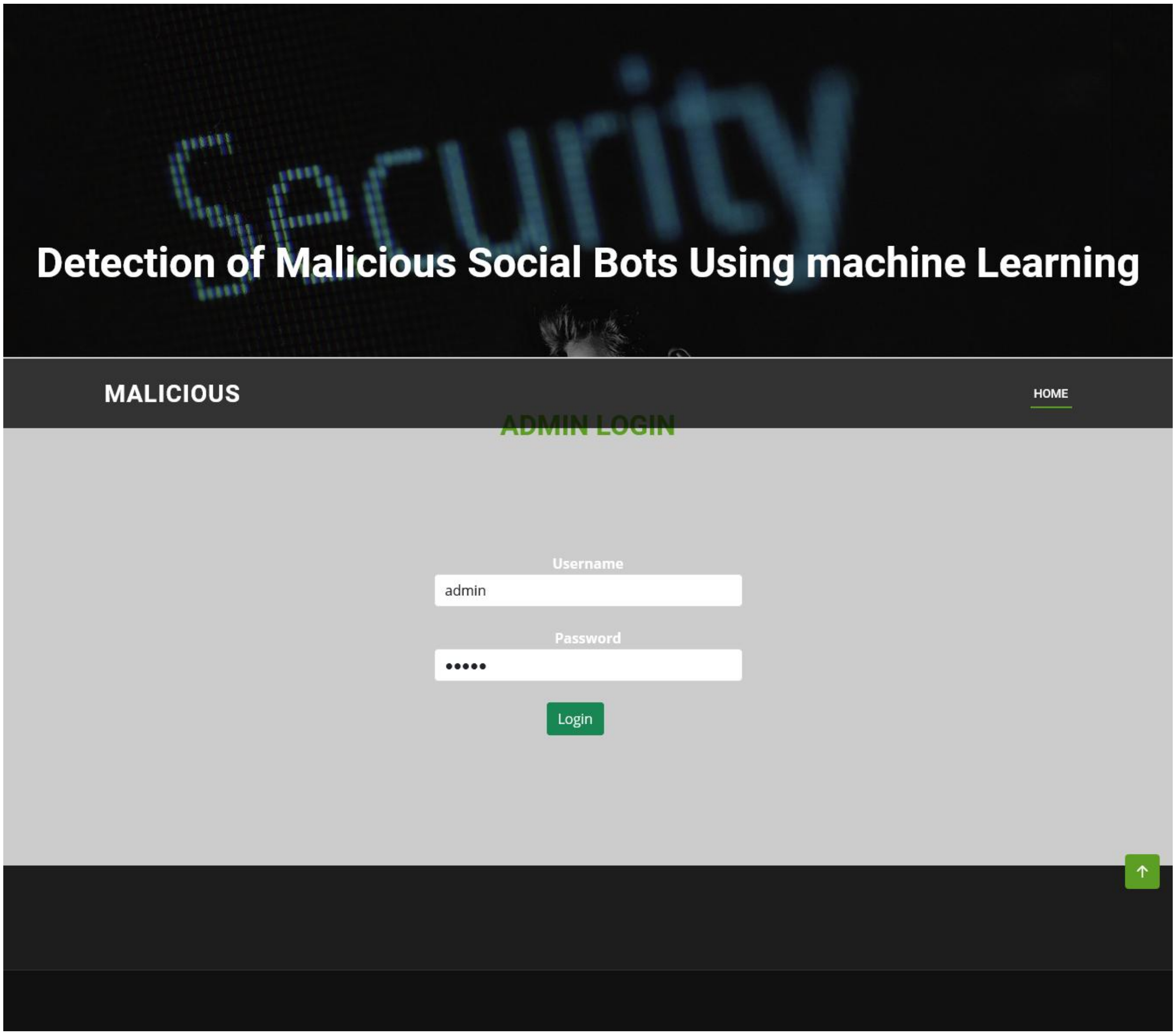
check this https://www.datacamp.com/

@jp

https://www.youtube.com/

@jp

view this video https://www.youtube.com/

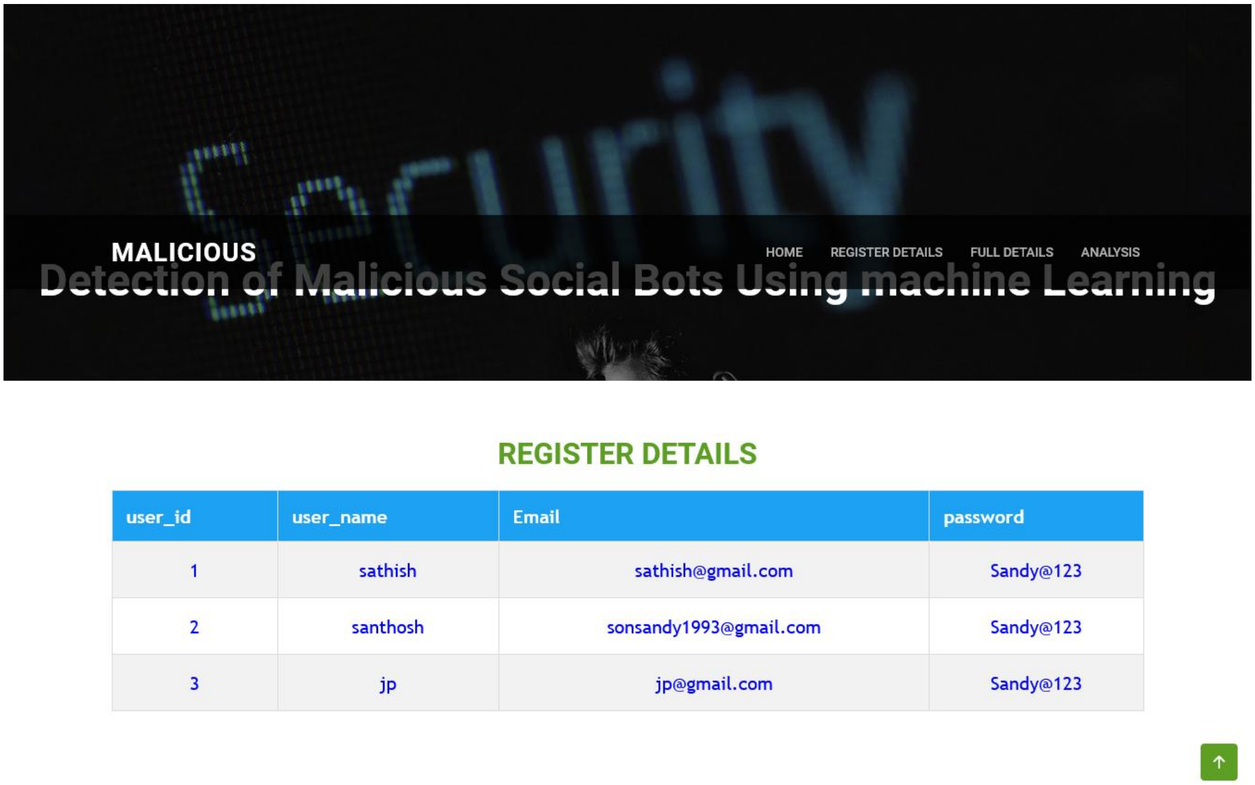


Detection of Malicious Social Bots Using machine Learning

ADMIN LOGIN

Username: admin

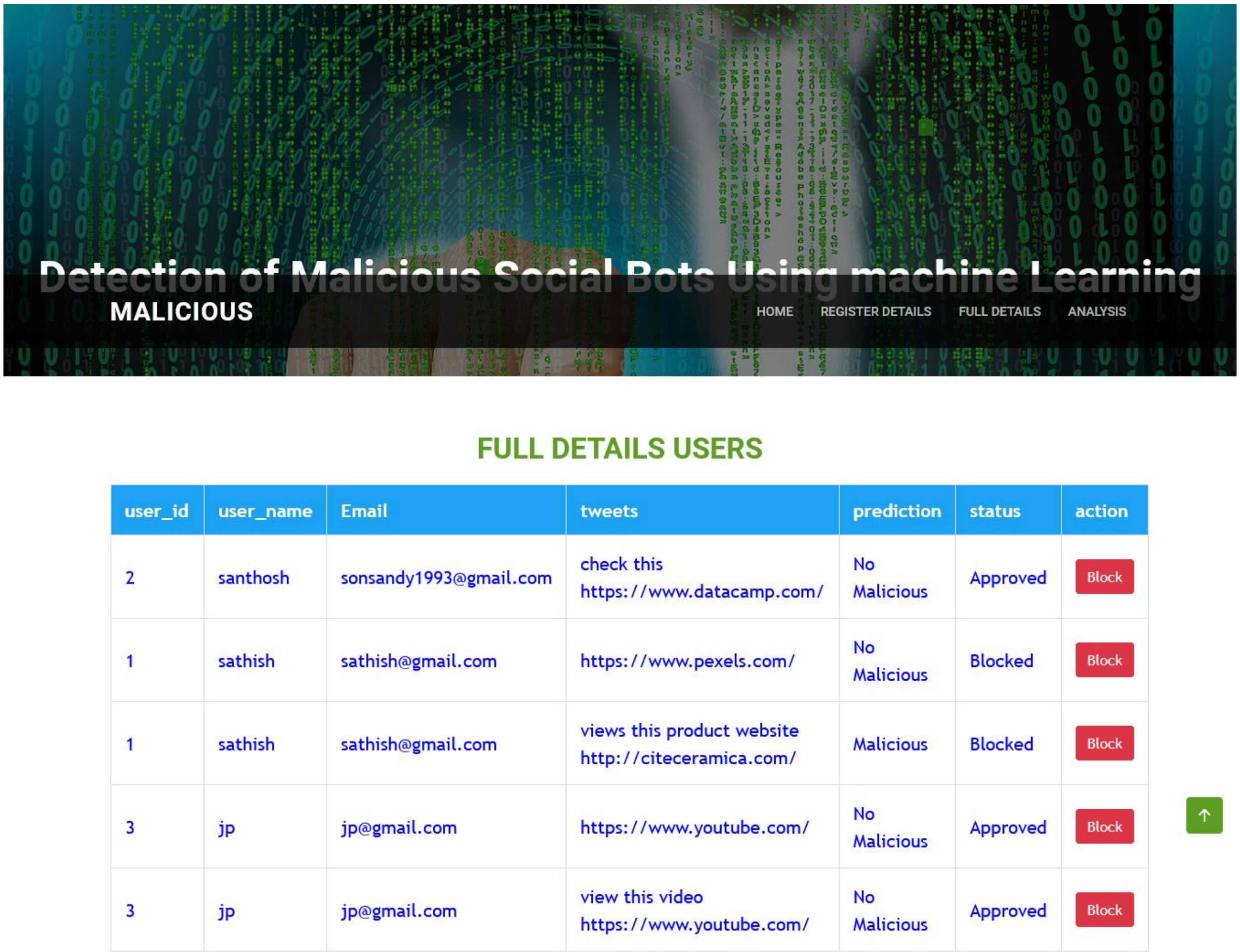
Password: •••••



Detection of Malicious Social Bots Using machine Learning

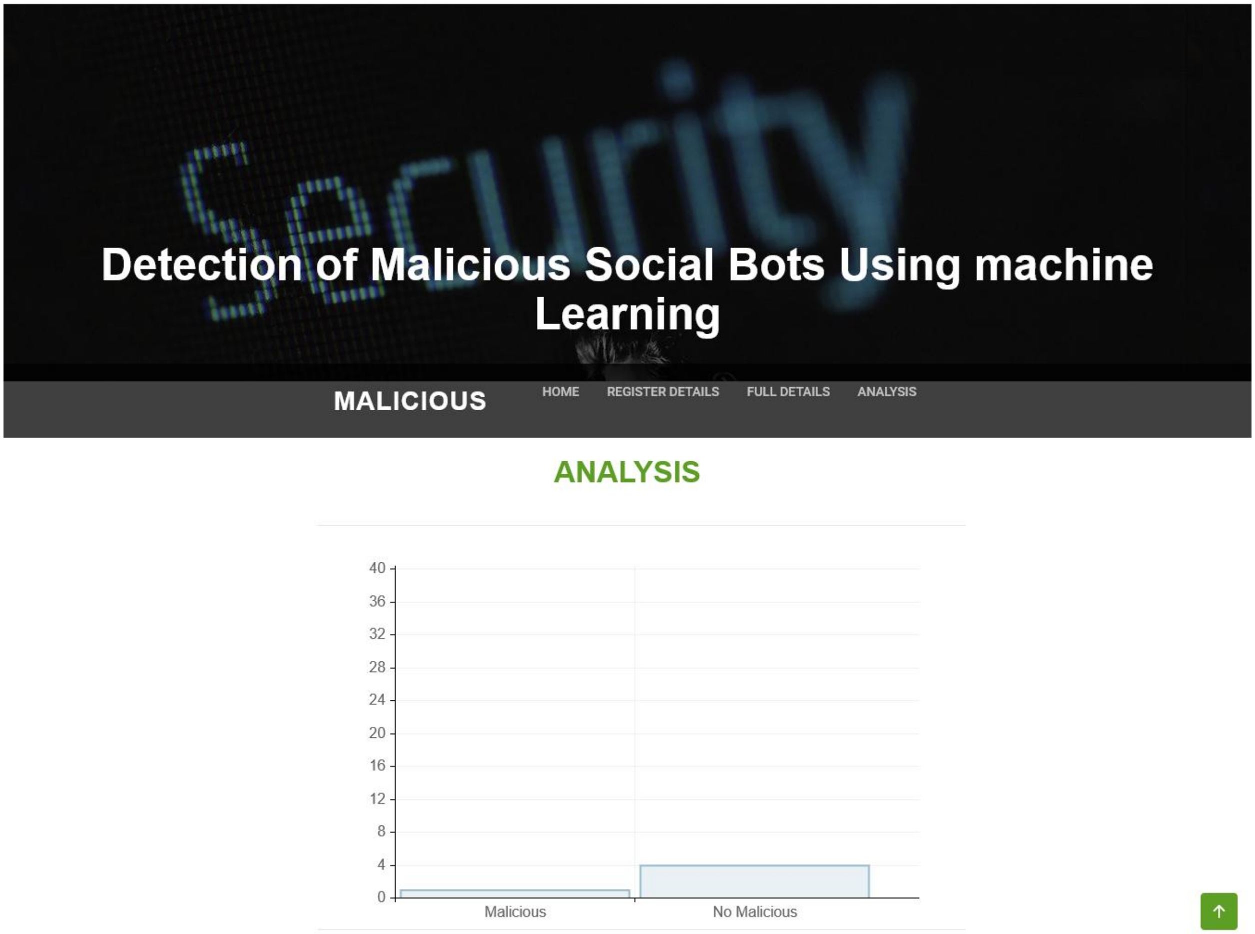
REGISTER DETAILS

user_id	user_name	Email	password
1	sathish	sathish@gmail.com	Sandy@123
2	santhosh	sonsandy1993@gmail.com	Sandy@123
3	jp	jp@gmail.com	Sandy@123



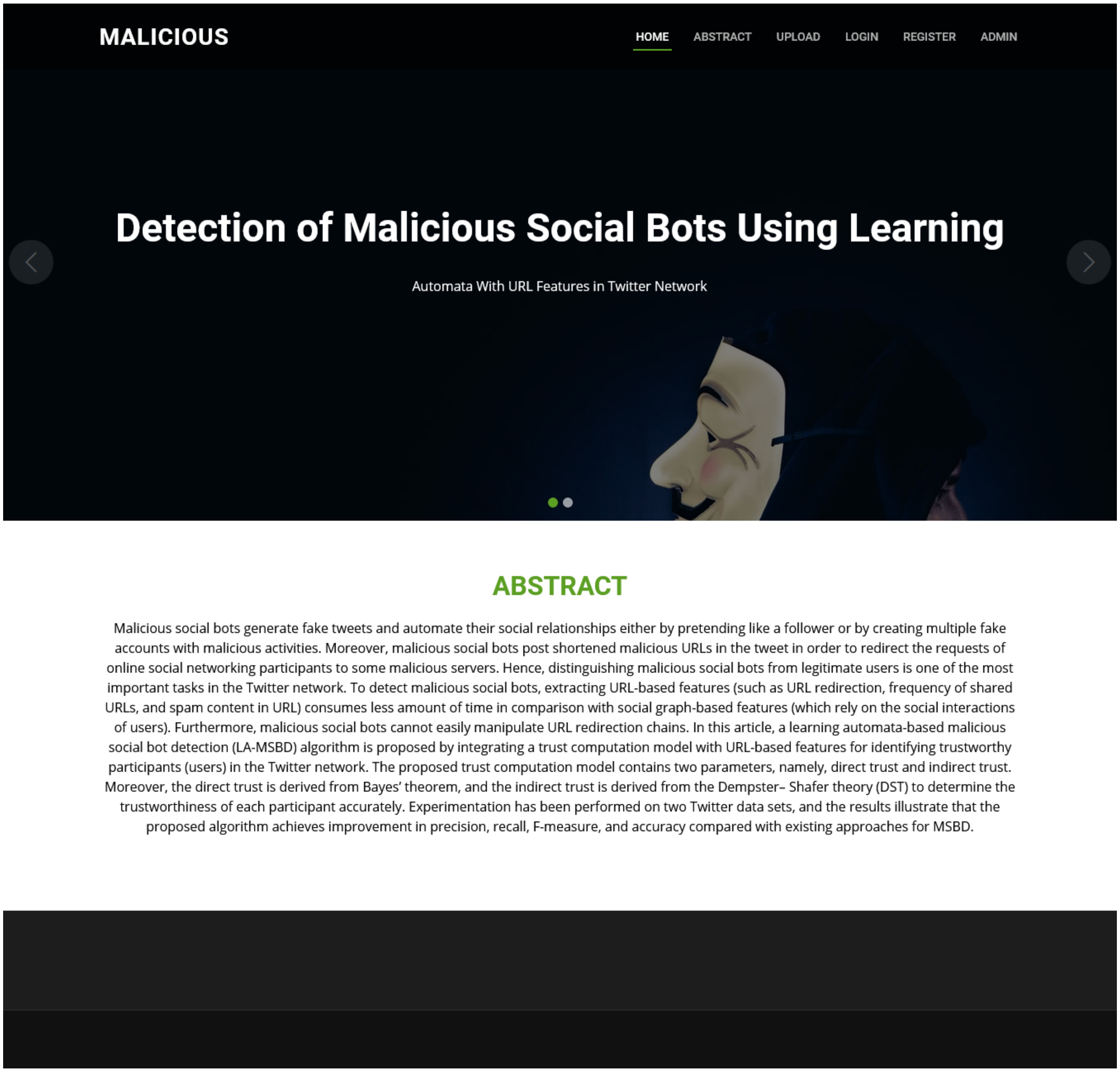
FULL DETAILS USERS

user_id	user_name	Email	tweets	prediction	status	action
2	santhosh	sonsandy1993@gmail.com	check this https://www.datacamp.com/	No Malicious	Approved	Block
1	sathish	sathish@gmail.com	https://www.pexels.com/	No Malicious	Blocked	Block
1	sathish	sathish@gmail.com	views this product website http://citeceramica.com/	Malicious	Blocked	Block
3	jp	jp@gmail.com	https://www.youtube.com/	No Malicious	Approved	Block
3	jp	jp@gmail.com	view this video https://www.youtube.com/	No Malicious	Approved	Block



Detection of Malicious Social Bots Using machine Learning

ANALYSIS



Detection of Malicious Social Bots Using Learning

Automata With URL Features in Twitter Network

ABSTRACT

Malicious social bots generate fake tweets and automate their social relationships either by pretending like a follower or by creating multiple fake accounts with malicious activities. Moreover, malicious social bots post shortened malicious URLs in the tweet in order to redirect the requests of online social networking participants to some malicious servers. Hence, distinguishing malicious social bots from legitimate users is one of the most important tasks in the Twitter network. To detect malicious social bots, extracting URL-based features (such as URL redirection, frequency of shared URLs, and spam content in URL) consumes less amount of time in comparison with social graph-based features (which rely on the social interactions of users). Furthermore, malicious social bots cannot easily manipulate URL redirection chains. In this article, a learning automata-based malicious social bot detection (LA-MSBD) algorithm is proposed by integrating a trust computation model with URL-based features for identifying trustworthy participants (users) in the Twitter network. The proposed trust computation model contains two parameters, namely, direct trust and indirect trust. Moreover, the direct trust is derived from Bayes' theorem, and the indirect trust is derived from the Dempster– Shafer theory (DST) to determine the trustworthiness of each participant accurately. Experimentation has been performed on two Twitter data sets, and the results illustrate that the proposed algorithm achieves improvement in precision, recall, F-measure, and accuracy compared with existing approaches for MSBD.