Detecting Malicious Email Accounts On Social Media

Santhosh Nunna, Nagurbabu Kaladi, S.Jancy

***ABSTRACT---** In this area, we have introduced the scheme for detecting malicious communication over the network and for maintaining the pipeline until the communication ends. Targeted malicious emails (TME) is the method for detecting the malicious email in the computer network, this scheme has a unique protocol for detecting the fault. Methods have two variant namely Spam Analyzing and ClamAV with the classifier of random forest which has a strong mathematical model in TME. The dynamical process will take everything under detection process, Filtering will extract the feature into an alternative. Threats are filtered from the communication by using the protocol which was developed. We develop a unique scheme for auditing the network continuously till the network is idle.*

***Keywords** — Information, email, threats, Administration, Malicious*

I. INTRODUCTION

In today's situation, everyone should have an account in any of the website or application. In those cases, hackers or fraudster have taken this situation as their opportunities. In Online social network, there are many areas like Facebook, Instagram and so on. Here everyone will be inactive, hackers will create a fake account to take interaction with the people who are their target. People who is using the Facebook or Instagram for their business promotion, will do more things like creating a profile, details of own, etc., hackers will create a fake id to give request to that id, and they will aim them as like customer. Finally, they will send the malicious message to the people after accepting the request from the people. Malicious persons know the situation of the people in social media so that they can attack the people easily by knowing the situation [15,16]. Facebook is to connect the families, friends, etc. in our proposed system we have used the TME for detecting the malicious account and the information which is traveling from one place to another place. This scheme will act like protocol, every information or mail will be auditing before it gets to mail. This scheme will have methods like a request with permission or analyzing the person before accepting. Some hackers will install the virus filled an application to the computer or to the network connected server that system will act as a hacker for a long time without knowing us. In these cases, our proposed system will detect the fake application and removing it completely from the system. TME is the concept which was used in many areas for the malicious system. The mathematical model is always heavy to satisfy but here we have used the concept with mathematical formula weight for a quality outcome, we have used some datasets for testing the scheme for building it in future [1]. In the existing system, they have used only to stop the malicious mail or application. It doesn't have any concept to specify the person who is making these dangers in the network. Our system will help the whole network until it is in Idle [2]. The transmission control protocol is only for reducing the traffic in the network also distributed protocol will affect the entire system quickly or slowly. Various attacks will be detected by TME in communication. Our proposed system will help everything inside the network to get safer from hackers or malicious mail [3], [4]. As we surveyed, more operations are getting spoiled because of the fake id or malicious mail.so we satisfied this area as well.

II. RELATED WORK

OSN is very important for the people and they do not have any about the detection methods for the malicious account [4]. Wherever peoples crowd is high, we can expect the dangers of a malicious person in any way. Understanding the malicious account in Facebook or Instagram is very useful. It has some types for denoting the dangers namely, spam information, Phishing and virus social structure [5]. In Facebook or any social media network, grouping is very high, in those cases, we should be safe [14]. Verification is very important, giving full information without knowing anyone is also a malicious [6]. The relationship between user and hacker in OSN is very useful on the survey and some detection methods are very important in the networked area [7]. Telecommunication fraud is happening in more areas till now without any solution, here it has some rules before calling the person also has some algorithm [8]. Financial activities are very important, creating an account before sending the amount, hackers are creating a loophole for stealing the amount from the people without knowing them, these activities are very high nowadays [9]. Intrusion detection on twitter spammer is a very good example for our proposed system. It gives more example of detection system [10]. Some concept is using the extraction for whole usage with spammer detection [11], [12], [13].

Revised Manuscript Received on July 10, 2019.

Santhosh Nunna, Student, School of Computing, Sathyabama Institute of Science & Technology. Chennai, T.N, India. (E-mail: nunnas136@gmail.com)

Nagurbabu Kaladi, Assistant Professor, School of computing, Sathyabama Institute of Science & Technology. Chennai, T.N, India. (E-mail: jancyphd16@gmail.com)

S.Jancy, School of computing, Sathyabama Institute of Science & Technology. Chennai, T.N, India.

Retrieval Number: B11060782S319/19©BEIESP
DOI : 10.35940/ijrte.B1106.0782S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

III. PROPOSED SYSTEM

In our scheme, we have proposed a TME concept in depth to verify the message sent to the user from the administrator, if it happens on, then every message will be in secured and non spammer. Each concept that was proposed by the scheme will act as a protocol then it will take some mathematical terms to calculate the assumption using Bayes theorem and naïve classifier.

Dataset and Feature extraction

Here dataset, as shown in Table.1, has been taken for the calculation and comparison for the results which was taking to best. Method of the dataset has two names, one is the response vector another one is feature matrix. Here we would like to satisfy this scheme for golf players, every player will get an email from the server which is in a much-secured manner. Dataset has humidity, temperature and so on. So that players will get the message like yes means they can play, if it is no, they cannot play on that day. Each calculation was made use of Bayes theorem.

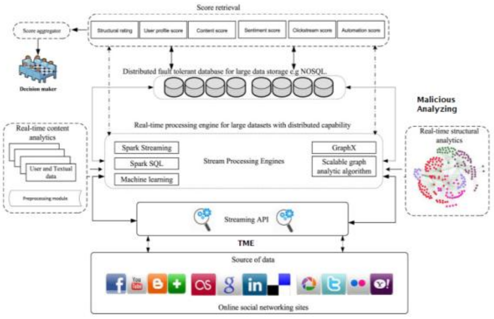
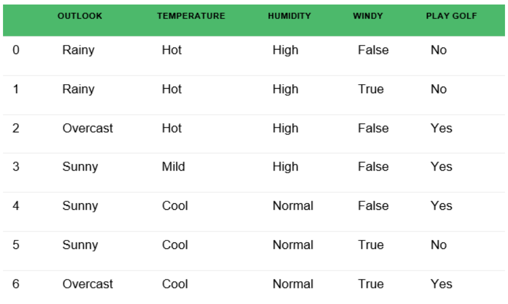

Score retrieval
Score aggregator
Structural rating
User profile score
Content score
Sentiment score
Clickstream score
Automation score
Decision maker
Distributed fault tolerant database for large data storage e.g NOSQL
Malicious Analyzing
Real-time processing engine for large datasets with distributed capability
Real-time content analytics
User and Textual data
Preprocessing module
Spark Streaming
Spark SQL
Machine learning
Stream Processing Engines
GraphX
Scalable graph analytic algorithm
Real-time structural analytics
Streaming API
TME
Source of data
Online social networking sites

Fig. 1 Proposed Scheme

In Fig.1, an email will be preprocessed by classifiers and the scheme. Here once the dataset was prepared then feature extraction will make a classifier to satisfy the area through the mathematical model. It uses some probability for choosing the best like YES or NO. These messages would be handled and maintained in an automated scheme. Every system has been used by some special model but here it is unique to expose. Finally, TME or Non-TME will be satisfied. This system uses some classifiers and theorem as follows.



	OUTLOOK	TEMPERATURE	HUMIDITY	WINDY	PLAY GOLF
0	Rainy	Hot	High	False	No
1	Rainy	Hot	High	True	No
2	Overcast	Hot	High	False	Yes
3	Sunny	Mild	High	False	Yes
4	Sunny	Cool	Normal	False	Yes
5	Sunny	Cool	Normal	True	No
6	Overcast	Cool	Normal	True	Yes

Table.1 Dataset

Naive Bayes classifiers

Here this classifier will be using this data for formation and process. Temperature, humidity, status are very important. So that classifier is using the probability concept to filter everything out of all data. The status will automatically go to the system by TME security. Before satisfies the data, it will move on to theorem for the process.

Bayes' Theorem

This theorem is used for filtering the area and data. A and B is the event, here formula shows the concept for filtering the event out of all events which were placed in an area**.**

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

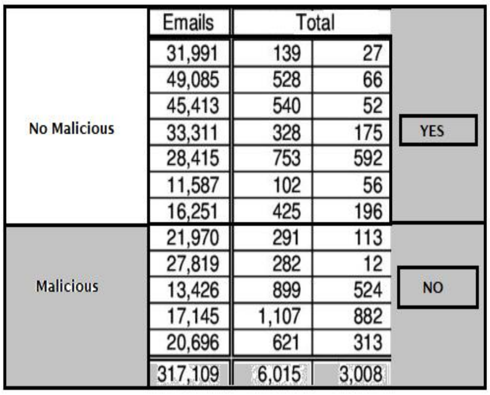
By doing this method we can get the results as soon as possible, also useful for handling the data on the server side as well. This formula was using the Table. 1 data for filtering and formation. Every data will move from theorem to calculation.

Assumption

After data was filtered, it comes out for calculation and resulting, below formula will use all filtered data for resulting it in the secured way after some steps it will notify the data to the user at fast.

$$P(y|x_1,...,x_n) = \frac{P(x_1|y)P(x_2|y)...P(x_n|y)P(y)}{P(x_1)P(x_2)...P(x_n)}$$

In Table. 2, Out of all data, it may vary the result as per YES or NO. If the user is expecting YES, then the calculation will move up to different types. If it is no second type is faster because it may get filtered from the first type using the formula.

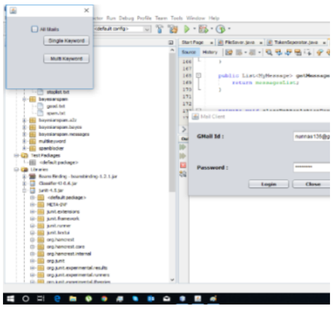


	Emails	Total		
No Malicious	31,991	139	27	YES
	49,085	528	66	
	45,413	540	52	
	33,311	328	175	
	28,415	753	592	
	11,587	102	56	
	16,251	425	196	
Malicious	21,970	291	113	NO
	27,819	282	12	
	13,426	899	524	
	17,145	1,107	882	
	20,696	621	313	
	317,109	6,015	3,008	

Table.2 Calculation

Here we can detect the mail which has malicious and which has not malicious.so our calculation was successful in this case.

IV. EXPERIMENTAL RESULTS



GMail Id : nunnas136@g

Password : ********

Fig. 2 Username and Password

In Fig.2 shows the username and password page for secured access, after logging into the system we can filter by giving the command like Yes or Not. Whatever command gives, it will be showing the result.

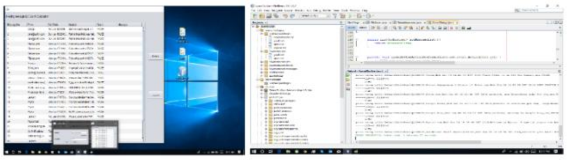


Fig. 3 Execution and Output

In the execution part, we can see the output as well. Here we have achieved the dataset by using the mathematical formula. Finally, it has a good result. Using this concept we can also achieve the banking service area for protecting the user and message.

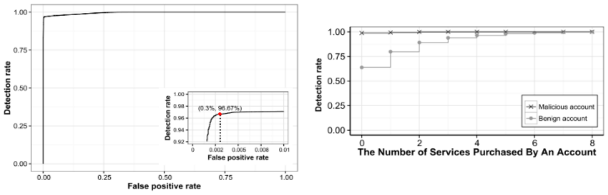


Fig. 4 Existing Graph

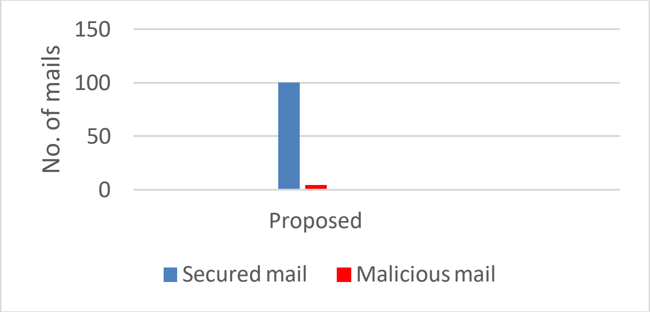


Fig. 5 Execution Graph

In Fig. 5, we have compared the existing model as shown in Fig. 4 with proposed method by detecting malicious mail. When comparing, we have reduced the number of malicious account or malicious mail from the fraudster. By comparing all this model with existing, we have achieved the system as good. As we compared existing has more number of malicious mail but in our proposed scheme we have reduced more number of malicious mail by implementing the secure synchronization using mathematical models.

V. CONCLUSION

More usage is occurring in Social media network as same to this, there is number of attacks are also occurring. To solve these issues and complexity, we have proposed the special scheme for protecting the area which is getting affected by a spammer in the social network. The result was achieved by the naïve classifier and implemented by Bayes theorem. In future work, this method can be used in banking region for securing the user message.

REFERENCES

1. NagaratnHarikant, Suma V, “Risk Analysis in Facebook Based On User Anomalous Behaviors” ICICCS 2017.
2. Santa Barbara, Pittsburgh “COMPA: “Detecting Compromised Accounts on Social Networks”.
3. Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, Ben Y. Zhao “Detecting and Characterizing Social Spam Campaigns” IMC’10, November 1–3, 2010.
4. Prateek Dewan, Ponnurangam Kumaraguru, “Towards Automatic Real Time Identification of Malicious Posts on Facebook” 2015 Thirteenth Annual Conference on Privacy, Security and Trust (PST)
5. Tao Stein, Erdong Chen, Karan Mangla “Facebook Immune System” ACM Jan 1, 2011.
6. M.A. Devmane, Dr. N.K.Rana “Detection and Prevention of Profile Cloning in Online Social Networks” ICRAI E – 2014.
7. Yasmeen Sultana, Prof. B.I.Khodanpur,”Detecting the Malicious Application using FRAppE” ICICCS 2017.
8. F.Wu,J.Shu,Y.Huang,andZ.Yuan,‘‘Social spammer and spam message co-detection in microblogging with social context regularization,’’in Proc. 24th ACM Int. Conf. Inf. Knowl. Manag., 2015.
9. Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, ‘‘Twitter spammer detection using data stream clustering,’’ Inf. Sci., Sep. 2014.
10. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, ‘‘Detecting and characterizing social spam campaigns,’’ in Proc. 10th ACM SIGCOMM Conf. Internet Meas., 2010.
11. S. Lee and J. Kim, ‘‘Warningbird: Detecting suspicious URLS in twitter stream,’’ in Proc. NDSS2012.
12. C. Yang, R. C. Harkreader, and G. Gu, ‘‘Die free or live hard? empirical evaluation and new design for fighting evolving twitter spammers,’’ in Proc. Int. Workshop Recent Adv. Intrusion Detection, 2011.
13. A.Abdallah,M.A.Maarof,andA.Zainal,‘‘Frauddetectionsystem :Asurvey,’’J. Netw. Comput. Oct. 2016.
14. Palagati Harish, Dr.R.Subhashini and K.Priya, “Intruder Detection by Extracting Semantic Content from Surveillance Videos” IEEE International Conference on Green Computing, Communication and Electrical Engineering on march 6th to 8th in NGP Institiute of Technology, Coimbatore, 2014
15. R.Subhashini and V. Jawahar Senthil Kumar, “A Framework for Efficient Information Retrieval using NLP Techniques“, Proceedings of the International conference on Advances in Communication Network and Computing, CNC 2011, CCIS 142, pp. 391–393, 2011, Springer-Verlag Berlin Heidelberg 2011,ACEEE, Bangalore
16. R.Subhashini and V. Jawahar Senthil Kumar, “Shallow NLP Techniques for Noun Phrase Extraction”, Presented in the International Conference on Trendz in Information Sciences & Computing (TISC - 2010) in association with Cognizant Technology Solutions and IEEE from 17th to 19th of December, 2010, Sathyabama University, Chennai.
17. Karthika, J. K., V. Maria Anu, and A. Veeramuthu. &quot;AN EFFICIENT ATTRIBUTE BASED CRYPTOGRAPHIC ALGORITHM FOR SECURING TRUSTWORTHY STORAGE AND AUDITING FOR HEALTHCARE BIG DATA IN CLOUD, 2006.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication