Sensitive Data Detection System in Chat Messages Using Data Mining

Divyashree G[1], ShivaKumar Swamy N[2]
[1, 2] Department of CSE
[1, 2] RRIT, Bangalore

Abstract- *Instant Messaging Systems (IMS) generically cannot detect many deceptive phishing attacks; hence they are Vulnerable for cyber frauds. To overcome, we proposes an Active-Phishing Detection System (APDs), developed using Data Mining (Rule-based) and Ontology. APDs monitor the user's psychology and predict type of the detected phishing activity with an alert to achieve zero-minute phishing attacks. Nowadays all illegal activities are happened using the communications in instant messages. Present frameworks for instant messenger have control over suspicious words but not in depth. It means present system could not find out all suspicious words. The proposed system is a framework, which predicts and highlights code words and short form of suspicious words with the help of association rule mining techniques and ontology concepts. Thus this proposed framework detects suspicious messages from instant messaging systems in early stage and helps to identify and predict the type of cyber threat activity and traces the offender details.*

Keywords- Instant Messaging (IM), Social Networking Sites (SNS), Active Phishing Detection System(APDs).Cloud computing, Load balancing, Energy efficiency, Green computing.

I. INTRODUCTION

The APDs, dynamically predicts any potential deceptive phishing attacks, when instant messages are exchanged between users of an IMS. Currently, IMS lacks a stronger mechanism to deal with phishing at content-level. Few researchers proposed various methods to detect phishing attacks [1] [2]. The emails of Google are categorized into Primary, Social, Updates, an Forums, ignoring the issues of phishing attacks. Recently, leaked news of PRISM-NSA as one of the largest surveillance programs monitoring the Networks exploiting against cyber international law. Social networks are essentially networks formed individuals, groups and organizations. Social network analysis is about analyzing the behaviours of individuals, groups and organizations and determines its behaviour patterns .Social network analysis is becoming an important tool for counter terrorism applications.

Internet evolutions led to the growth of innumerable cybercrimes. Criminals adapted to send suspicious messages via mobile phones, Instant Messengers and Social Networking Sites, which is difficult to trace their criminal activities dynamically. The E-crime department must be improvised with\ the development of technology to find criminals. Many of the Instant Messaging Systems (IMS) developed restricted their limit for sending messages, video and audio conferencing. They are not well equipped to detect online suspicious messages. Social Networking Sites (SNS) are web-based services that facilitates individual to construct a profile, which is either public or semi-public. SNS contains list of users with whom we can share a connection, view their activities in network and also converse. SNS users communicate by messages, blogs, chatting with video and music files. SNS plays very important role in human life. It is becoming a main communication media among the individuals and organizations. The other advantages include keeping contact with friends and family members. For entrepreneurs, it acts as a resource to set up a global presence. Employers nowadays use SNS as useful and effective recruitment tool. Some SNS provides low cost of advertising for business owners. However with all these advantages, SNS also have many disadvantages such as information is public, security problem, cyber bullying and misuse and abuse of SNS platform.

The medium of Instant Messaging on the Internet is a well-established means by which users can quickly and effectively communicate with one another. Long utilized by the public as a quick form of free communication, data mining tasks have not been attempted over Instant Messaging. Additionally, on a corporate or government level, people are just beginning to take notice of the potential that IM provides in terms of the type of information that can be collected from these networks. Many large Instant Messaging networks are of their own generally open to the public after registration, including Time Warner, Yahoo and Microsoft.

II. PROPOSED ACTIVE-PHISHING DETECTION SYSTEM

Operational Framework of APDs is shown in Fig. 1. The APDs algorithm initiates the steps to capture the phishing words that are exchanged between the users and then stores them into database for identifying phishing words using pre-defined phishing rules. The APD algorithm is shown in Fig. 2.

In APDs, the Monitoring system program identifies the culprit details of Phisher and report to the victim client. Steps of algorithm are illustrated as follows:

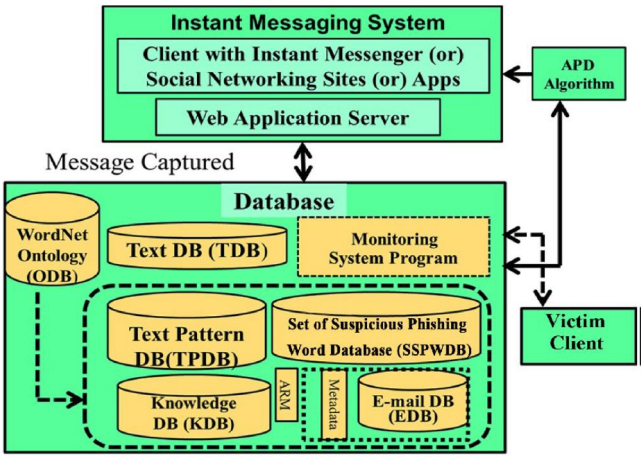

Fig. 1. Proposed Framework (APDs) to detect phishing messages from Instant Messaging Systems (IMS).

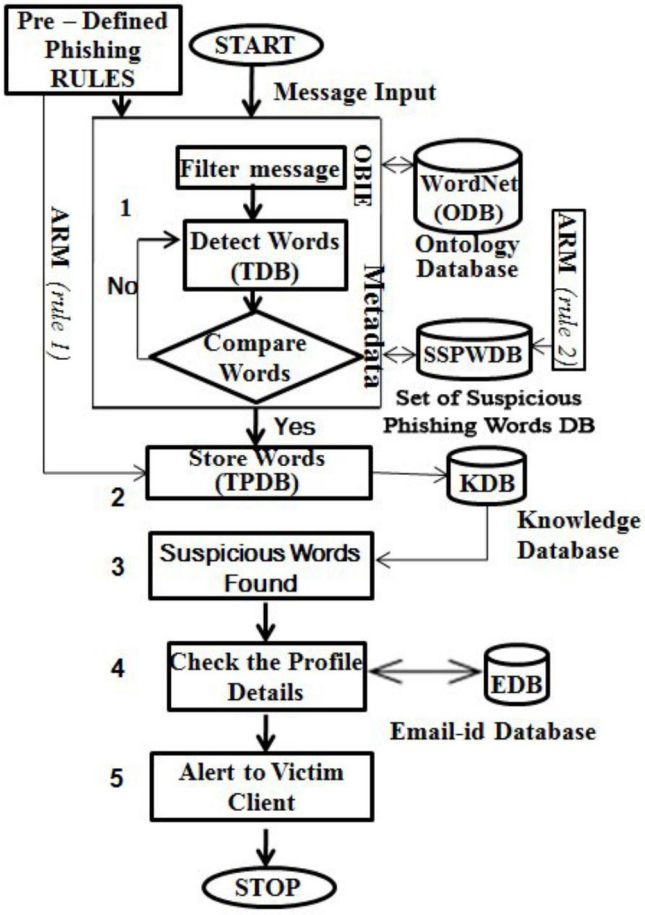

Fig. 2. Schematic cum algorithmic representation for proposed Framework named as APD algorithm.

1. In this step, the phishing words are identified by using GSHL and Tree Alignment Algorithms as discussed in [4]. These messages are stored in Text database (TDB), where unnecessary words are filtered using Ontology Based Information Extraction technique (OBIE) (stemming, N-gram technique, ignore words).
2. The frequently recurring words are extracted from the TDB dynamically using Association rule mining technique [8] and SSPWDB (pre-defined rules) guided with Ontology database (ODB), later these words are pushed to TPDB. The metadata is a gist of information related to instant messages.
3. Once the Phishing words are detected, the message is considered as suspicious, as given in Table I (rule 1). The KDB maintains the detected stem words along with the domain (i.e. type of Phishing activity).
4. Profile details are traced from EDB, which are provide during the creation of an email id, with the aid of Relational Wrapper Algorithm [9].
5. The email- id through which the phishing words are sent is tracked using metadata, and the victim is alerted.

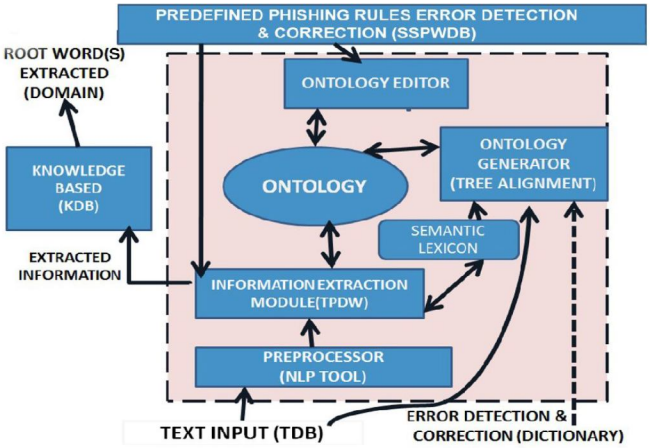

Fig. 3. Proposed OBIE Framework to detect phishing words from Instant Messaging System(IMS).

The given Text Input (TDB) is converted to pure textual format by the pre-processor component using NLP tools. The information extraction techniques filter unnecessary words from unstructured text. The stem words that are found and stored in TPDB, are guided by ontology internally by the Ontology Generator component using Tree Alignment algorithm. During this process it makes use of semantic lexicon (WordNet) and Error detection and Correction, for stem words that are extracted and builds a Tree with empty root node initially. The input given from pre-defined phishing rules (SSPWDB) to Ontology Editor is again mapped with the Ontology Generator by identifying the exact Domain for the empty root node. Finally the root word(s) along with stem words are stored in knowledge database (KDB). The experimental results obtained for predicting the type of phishing activity detected from IMS are shown that Taxonomic Structure of words mapped fro Pattern Database

(TPDB) with pre-defined phishing axioms (SSPWDB).The experimental results obtained for predicting the type of phishing activity detected from IMS using OBIE framework of Fig. 3.

III. PROPOSED FRAMEWORK

Now a days all illegal activities make use of the used in communications of instant messages. Present framework for instant messenger have control over suspicious words but not completely.

Thus existing system has several limitations as follows.

- Cybercrimes have raised day by day, but the social networks are not having mechanisms to restrict them.
- Offenders can easily convey their messages through the insecure social networks and internet.
- Blackmails are also sent from one person to another person that could not be traced out.
- Short form messages and code word messages in social networks are still worsen the case of disclosing the illegal activity. Proposed system has the below mentioned salient features as objectives.
- System tries to provide security for the stored chat messages by using encryption technique. Then it will find suspicious words by decrypting stored messages.
- Detects the suspicious words from the message even the message is in short form or code form.
- This determination of illegal activities is analyzed with the help of ontology. Even new code words that are not available in predefined database are also extracted with the help of data mining techniques and added into ontology database.
- If the system finds some cyber threat it will report with the offender's personal details to E-crime department.
- System's performance can also be evaluated with the help of execution of user generated content called test bed.

Thus the proposed system is a framework that predicts and highlights such suspicious messages along with suspected threat activity with offender's personal details. All the instant messages will be faced by the system for any supposed cipher thread activity. This new framework uses association rule mining algorithm and ontology based information extraction technique which initiates the steps to capture and store the instant messages that are communicated between the users and identifies suspicious messages with predefined knowledge such as the keywords murder, kill and theft and so on. In addition the system also verifies code words and short form suspicious words. The system also uses encryption/decryption methods to enhance security to the messages and figure out any suspicious messages present over there.

This proposed framework has the following components:

- Data collection system
- Suspicious word detection system

Both data collection and suspicious word detection systems have normal functionalities that are given by all instant messengers such as login module, change password etc.,

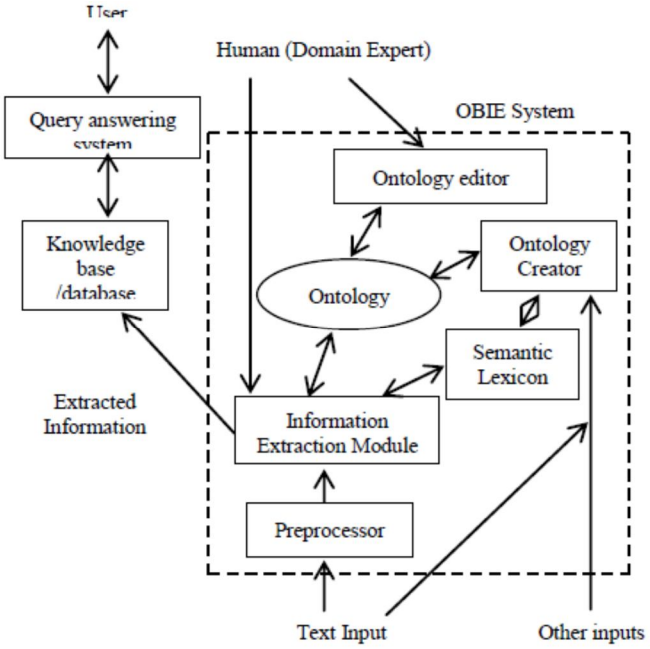

Fig.4. General OBIE architecture

A. Ontology management

Since ontologies are widely used to represent knowledge or meaning they are often seen as providing the backbone for the semantic web. In this framework, ontology database is created with suspicious word list such as murder, kidnap, terrorist, corruption and robbery. These processes can be implemented by OBIE [17] (Ontology Based Information Extraction).OBIE has recently emerged as a subfield of information extraction. Here ontologies – which provide formal and explicit specifications of conceptualizations - play a crucial role in the IE process. Because of the use of ontologies, this field is related to knowledge representation and has the potential to assist the development of the semantic web. General OBIE architecture can be constructed as shown in below Fig 1. This architecture depicts ontology editor, ontology creator and IE module as major parts of ontology. Pre-processing of the text is important before IE. Semantic lexicon also acts major role in ontology creator. Thus the user

can effectively extracts relevant information with the help of OBIE system.

B. Encryption / Decryption Module

System will encrypt the messages and store it in the database. Suspicious word detection can be done on the decrypted message along with short form and code words.

C. Suspicious word detection

Here, filtering of unnecessary words from messages is done; during this process, the suspicious words such as murder, kidnap, terrorist, corruption and robbery are identified using data mining techniques.

D. Short form management

A separate database will be maintained with short forms of suspicious words such as politician names, country names and short form of suspicious word such as kl (kill), att (attack), bom (bomb) and money .Again by using same detection algorithm these suspicious words are detected.

E. Code word management

Comparing several messages communicated within a same group can identify code words. If same word was used by different people in conversation within a group along with known suspicious words in database then these words are considered as code words and also added to suspicious list to detect suspicious words in future.

F. Ontology Update

New suspicious words that are not already in database are founded with the help of code words detection method and will be added back in ontology. Thus ontology used here is fully updated then and there. This ontology update helps in finding suspicious words in efficient manner and it saves time in detecting suspicious words in future.

G. Offender's information module

After finding suspicious words from the conversation system can easily figure out the offenders names along with their personal details and IP address of their systems. This information is displayed with the help of database which was originated while creating the chat id.

IV. CONCLUSION

Framework of proposed system aids the E-crime department to identify suspicious words from cyber messages and trace the suspected culprits. Currently existing Instant Messengers and Social Networking Sites lack these features of capturing significant suspicious patterns of threat activity from dynamic messages and find relationships among people, places and things during online chat, as offenders have adapted to it. The User Generated Content (UGC) testbed is proven to be useful, for monitoring terror and suspicious crimes in cyberspace which provides national and international security. We used simple English terms like kill, murder, etc.

ACKNOWLEDGMENT

We would like to thank Management of RRIT for providing such a healthy environment for the successful completion of this work and express my gratitude to Mr. ShivaKumar Swamy N (Associate Professor, RRIT, Bangalore) for providing continuous support and encouragement.

REFERENCES

[1] Mahmoud Khonji, Youssef Iraqi, and A. Jones, "Phishing detection: A Literature Survey," IEEE Vol 15, 2013.

[2] Mohd Mahmood Ali, and Lakshmi Rajamani, "Deceptive phishing detection system: From audio and text messages in instant messengers using data mining approach," IEEE, 2012.

[3] [Online] APWG - www.antiphishing.org, accessed on 2014.

[4] Mohd. Mahmood Ali, and L. Rajamani, "Framework for surveillance of instant messages," IJITST, Inderscience publisher, 2013.

[5] [Online] Ontology Portal - www.ontologyportal.org, accessed on 2014.

[6] Jer Lang Hong, "Data Extraction for Deep Web using WordNet," IEEE Transaction on Systems, Man and Cybernetics, 2011.

[7] C.D. Manning, P. Raghavan, Hinrich Schutze, Introduction to Information Retrieval, 2004.

[8] R. Srikant, and R. Agarwal, "Mining quantitative association rules in large relational tables," In Proceedings of the ACM - Special Interest Group on Management of Data (ACM SIGMOD), 1996, pp.1-12.

[9] Sunitha Ramanujam, and et al., "A Relational Wrapper for RDF Reification," E. Ferrari et al. (Eds.): TM 2009, IFIP AICT 300, pp.196-214, IFIP International Federation for Information Processing in 2009.

[10] D.Boyd and N.B.Ellison, "Social Network Sites: Definition, History and Scholorship", Journel of Computer Mediated Communication, vol.13 no.1-2, Nov 2007.

[11] J.S.Mclllwain, "Organised crime: A social network approach", Crime Law and Social Change, vol. 32, pp.301-323, 1999.

[12] F.J.Fu, J.Chai and S.Wangl., "Multi-factor analysis of terrorist activities based on social network", Business Intelligence and Financial Engineering (BIFE), 2012 5th International Conference on 18-21 Aug 2012, pp. 476-480, 2012.

[13] Michael Robertson, Yin Pan, and Bo Yuan, "A Social Approach to Security: Using Social Networks to help detect malicious web content," published by IEEE in 2010.

[14] Available:http://www.digitaltrends.com/socialmedia/facebook-scans-chats-and-comments-looking-for-criminal-behavior/ (2012).

[15] Appavu, and et al.,"Data mining based intelligent analysis of threatening e-mail," published by Elsevier in knowledge-based systems in 2009.

[16] John Resig and AnkurTeredesai, "A Framework for Mining Instant Messaging Services" in proceedings of the 2004 SIAM Lake Buena Vista - ejohn.org Date: 2011-04-19.

[17] Khan. F. M., Fisher. T. A., Shuler. L, Wu. T and Pottenger. W.M . "Mining chat rooms conversations for social and semantic interactions" from citeseerx.ist.psu.edu/ doi=10.1.1.19.9358.

[18] Kolenda. T, Hansen. L and Larsen. J "Signal detection using ica: application to chat room topic spotting" from citeseerx.ist.psu.edu/ doi=10.1.1.11.8457.

[19] S. M. Nirkhi, Dr. R. V. Dharaskar, Dr. V. M. Thakre, "Analysis of online messages for identity tracing in cybercrime investigation", IEEE publication, pp. 300-305, 2012.

[20] Zheng R, Li J, Chen H, Huang Z., "A framework for authorship identification of online messages: writing-style features and classification techniques". Journal of the American Society for Information Science and Technology, February, 57(3), pp.378– 93, 2006.

[21] Mohd Mahmood Ali and Lakshmi Rajamani, "APD: ARM Deceptive Phishing Detector System Phishing Detection in Instant Messengers using Data mining Approach" in Springer-Verlag Berlin Heidelberg 2012 :ObCom 2011, part I, CCIS 269, pp.490-502, 2012.

[22] Sharath Kumar and Sanjay Singh, "Detection of user cluster with suspicious activity in online social networking sites" in IEEE publication, pp. 220-225, 2013.

[23] Farkhund Iqbal, Benjamin C.M.Fung, MouradDebbabi, "Mining Criminal Networks from Chat Log" in IEEE/WIC/ACM International Conference, pp.332-337, 2012.

[24] Mohd Mahmood Ali, KhajaMoizuddinMohd and Lakshmi Rajamani, "Framework for surveillance of Instant Messages in Instant Messengers and Social networking sites using Data Mining and Ontology" in proceedings of the 2014 IEEE Students' Technology Symposium, pp.297-302,2014.

[25] G.A. Miller and C. Fel;baum "WordNet: A Lexical database for the English Language". Available at: http://wordnet.princeton.edu [online],2006.