International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 11; November 2017; Page No. 7744-7746
DOI: http://dx.doi.org/10.24327/ijcar.2017.7746.1217

Research Article

# ENHANCED INSTANCE MESSAGING FOR PERVASIVE COMMUNICATION IN MOBILE COMPUTING

**Manogna P and Yashwanth Reddy A**

Department of CSE, Sree Dattha Group of Institutions, Hyderabad Telangana, India

**A R T I C L E I N F O**

***Article History:***

Received 16th August, 2017
Received in revised form 25th September, 2017
Accepted 3rd October, 2017
Published online 28th November, 2017

***Key words:***

Nth- Degree Truncated Polynomial Ring Unit (NTRU), Message, Security, Encryption, Decryption, IM, Spam.

**A B S T R A C T**

The First IM system created by Mirabilis (a pioneer of online chatting that revolutionized communication over the Internet), dubbed ICQ (I seek you), in 1996 which achieved widespread adoption quickly among netizens. Although other instant messaging (IM) systems have surpassed ICQ in popularity, the medium of IM remains a popular form of technologized communication. The major drawback has been the vulnerabilities associated with IM technology. These vulnerabilities have created so many security issues. For efficient activity in each message encryption and decryption. We propose Spam Abstraction Scheme, which considers e-mail layout structure to represent e-mails. We present a procedure to generate the e-mail abstraction using HTML content in e-mail (especially anchor and image tags), and this newly devised abstraction can more effectively capture the near-duplicate phenomenon of spams. Moreover, we design a complete spam detection system that considers other Spam Checking Criteria's besides Content-based filtrations.

*Copyright©2017* ***Manogna P and Yashwanth Reddy A.*** *This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.*

## INTRODUCTION

From the past 20 years Internet has set the rapid force of how, where and the way we communicate. E-mail has become a mainstream form of communication and has replaced the traditional letters. In last couple of decades people have started using Internet regularly. The need of live and sensible way of communication over Internet has increased rapidly. The start of Instant Messaging came about in 1996. Instant Messenger is client software that allows person to person interactive communication in real-time provided both users have the same software. Such communication is called 'chat'. Company named Mirablis, Ltd., introduced ICQ, instant messaging utility. ICQ, in shorthand language is "I seek you". Instant messaging (IM) is a real-time communication service which allows a user to send a message, usually based on text, to other users. Nowadays we depend more and more on information from the Internet, and are increasingly not satisfied with accessing the Internet using personal computers or office workstations. Hence, accessing the Internet by portable and wireless devices has been becoming popular.

Today in business communications IM System plays the major role, such as observing the status of staff, real-time chatting, getting business opportunities and so on. The enterprise applications lay more emphasis on the security of the system; therefore, considering the efficiency issue, existing work use the SHA-1 digest algorithm, AES symmetric encryption algorithm, RSA asymmetric encryption algorithm and RSA signature algorithm, with Bouncy Castle Crypto package, to design a security policy to secure the IM system.

In this paper, we propose Spam Tree Abstraction Scheme, which considers e-mail layout structure to represent e-mails. We present a procedure to generate the e-mail abstraction using HTML content in e-mail (especially anchor and image tags), and this newly devised abstraction can more effectively capture the near-duplicate phenomenon of spams. Moreover, we design a complete spam detection system that considers other Spam Checking Criteria's besides Content-based filtrations.

### *Back ground*

### *How IM works*

It's a very simple which works with its name. It delivers the user's message to his desired contact instantly. The message delivery is instant provided users contact person is online. The client software allows user to maintain a list of contacts that he wants to communicate. User can send messages to any of the contacts in his list. Such list is referred to as a buddy list or contact list. This works like the E-mail management system. This contact list is nothing but e-mail ID of a contact. User can also block a particular contact or everyone who is not on his contact list from sending an instant message. Setting the appropriate privacy settings does this.

**Corresponding author:* **Manogna P**
Department of CSE, Sree Dattha Group of Institutions, Hyderabad Telangana, India

When user logs on Instant messenger service he can see the presence of the friends on his contact list and vice versa. User can show his availability via Instant Messenger. Sometimes user is online but is busy and do not wish to respond to any instant messages. In such situations user can change his status to 'Busy' or 'Not available'. This allows the person who is trying to contact user know the reasoning behind the non-availability of user. User can also choose to be invisible while being online. This enables him to watch his contacts without giving his status.

Various communication means are available using instant messaging. User can have an individual chat session or have a conference with multiple users. With use of web camera and voice an interactive web conference can be held using instant messaging.

***IM Service providers***

Among the various vendors for instant messaging, America online (AOL), Yahoo and Microsoft are some of the major vendors in providing instant messaging for consumers.

- MSN Messenger – MSN has about 9 million subscriptions. Besides the subscribers, MSN Messenger can be downloaded free of charge by anyone with an access to Internet.
- Yahoo Instant Messenger – Just like MSN, Yahoo provides the Messenger services free of charge to anyone who wants it. Simply go to their web site and download the Yahoo Messenger. Both Yahoo and MSN support instant text and voice messages, communication face-to-face via web cameras, and affordable PC-to-phone calls anywhere in the world.

***Drawbacks of IM***

Insecure Communication is the main drawback of IM. Businesses are required to protect information related to their customers, vendors and their own trade secret. Several specific issues come up with insecure communications in commercial sector.

- Identity Theft – This is a technological nightmare for an individual who has to live it. In identity theft an individual's identity is stolen and is used by an identity thief to conduct various monetary transactions. The person who's identity has been stolen is not aware of these transactions. By the time an individual becomes aware of such theft bad record in the system is already established. Such crime can be easily committed. Confidential information such as your bank account number, social security number, credit card information should not be shared during IM session.
- Cyber stalking - Crime such as Cyber stalking is becoming very common. In this case stalker stalks a victim on Internet. Use of E-mail or other forms of electronic communication is used by stalker as means of stalking. Presence is the most popular feature of IM. IM gives away the presence of user. This makes it easier to stalk the person online.

Currently users expect high level of security while doing Instant messaging. Some familiar problems are: data confidentiality while transmitting, data and application access must be controlled, data integrity, loss of device must have limited impact, and non repudiations.

***Confidentiality:*** only the valid communicating users can view the messages.

***Integrity:*** the messages can't be tampered by the intruders. The system should be able to find out such alteration.

***Non-repudiation:*** no party can deny the receiving or transmitting the data communicating between them.

***Authentication:*** each party has to have the ability to authenticate the other party.

***Authorization:*** it has to be ensured that, a party performing the transaction is entitled to perform that transaction or not.

***Security:*** It is where the messages are encrypted/decrypted using NTRU/PKCS for secure communications

***Spam Detection Process***

In message sending operations of the detection of unwanted or unspecified words in given message. The primary idea of the near-duplicate matching scheme for spam detection is to maintain a known spam database, formed by user feedback, to block subsequent spams with similar content. Collaborative filtering indicates that user knowledge of what spam may subsequently appear is collected to detect following spams.

```
Procedure of Matching Handler
Input: EA: the email abstraction of a testing email,
       S_th: the score threshold for determining spams
Output: the detection result
1  var f_level; // the final level which exact matching is processed
2  var candSet; // the set for tentative info of candidate spams
3  // Approximate Matching Phase
4  Find the corresponding SpTree in SpTable with EA.tag_length;
5  Traverse directly to the targeted leaf node based on the types of tags
   at positions 2^l;
6  for (each subsequence in the leaf node)
7    if (EA.tag_length == subsequence.tag_length)
8      candSet.insert (subsequence.info);
9  // Exact Matching Phase
10 nowNode = SpTree.root;
11 for (i = 0 to f_level)
12   for (each subsequence in candSet)
13     if (subsequence.hash_value ==
         EA.current_subsequence.hash_value)
14       if (subsequence!= EA.current_subsequence)
15         candSet.delete (subsequence.info);
16     else candSet.delete (subsequence.info);
17   nowNode = the corresponding child node;
18 sum = the sum of S_R of all candidate spams in candSet;
19 if (sum > S_th) return spam;
20 else           return ham;
End
```

**Figure 1** Extracting spam detection in Secure message

Overall, there are three key points of this type of spam detection approach we have to be concerned about. First, an effective representation of e-mail (i.e., e-mail abstraction) is essential. Since a large set of reported spams has to be stored in the known spam database, the storage size of e-mail abstraction should be small. Moreover, the email abstraction should capture the near-duplicate phenomenon of spams, and should avoid accidental deletion of non spam e-mails (also known as hams). Second, every incoming e-mail has to be matched with the large database, meaning that the near-duplicate matching process should be substantially efficient.

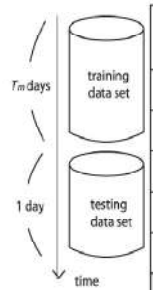
***Performance Analysis***

In this section we conduct several experiments to explore its efficiency and detection results. The real spam data sets used in the experiments are from the

e-mail servers of Computer Center in National Taiwan

University, which has over 30,000 students. Since the ground truth of real e-mail streams is unavailable, spams are extracted from the well-known existing system, Spam Assassin. 3 Concerning hams, we not only include public data sets (around 4,000 e-mails) provided by SpamAssassin,4 but also obtain from volunteers. There are about 60,000 spams per day and a set of 7,000 or so hams in the data set. Note that numerous related works have evaluated the proposed methods with static databases. However, to access the performance of spam detection system with near-duplicate matching scheme, real e-mail streams are more appropriate than static data sets. Therefore, in this paper, we use university-scale e-mail streams as the experimental data sets to better simulate the e-mail environment.

***Accuracy Evaluation:*** The most important requirement for a spam detection system is the capability to resist malicious attack that evolves continuously. The minority of e-mails are in Japanese, French, and so forth. Since Chinese is a non-alphabetic language and English is an alphabetic one, the data set used in the experiments can verify the effectiveness of spam detection system with different kinds of languages to a certain extent.




| $T_m$(days) | | Cosdes | | MultiDigest | | Digest | | Density | |
|---|---|---|---|---|---|---|---|---|---|
| | | 2007 Sep. | 2009 Feb. | 2007 Sep. | 2009 Feb. | 2007 Sep. | 2009 Feb. | 2007 Sep. | 2009 Feb. |
| 1 | TP(%) | 97.15 | 96.34 | 99.62 | 99.71 | 99.30 | 99.34 | 82.46 | 79.33 |
| | FP(%) | 0.21 | 0.24 | 94.71 | 95.40 | 89.04 | 89.14 | 12.99 | 13.11 |
| 2 | TP(%) | 93.37 | 95.09 | 99.71 | 99.63 | 99.64 | 99.08 | 81.09 | 82.81 |
| | FP(%) | 0.33 | 0.36 | 94.92 | 95.48 | 89.21 | 89.34 | 13.36 | 13.66 |
| 3 | TP(%) | 96.62 | 97.05 | 99.80 | 99.73 | 99.75 | 99.39 | 81.34 | 81.67 |
| | FP(%) | 0.46 | 0.49 | 95.04 | 95.61 | 89.32 | 89.48 | 14.07 | 14.41 |
| 4 | TP(%) | 97.59 | 95.60 | 99.82 | 99.81 | 99.80 | 99.16 | 84.11 | 83.27 |
| | FP(%) | 0.56 | 0.60 | 95.25 | 95.73 | 89.66 | 89.74 | 14.87 | 15.12 |
| 5 | TP(%) | 97.94 | 96.09 | 99.74 | 99.77 | 99.72 | 99.28 | 83.36 | 85.09 |
| | FP(%) | 0.68 | 0.71 | 95.38 | 95.84 | 89.88 | 90.03 | 15.38 | 15.83 |
| Average | TP(%) | 96.47 | | 99.75 | | 99.39 | | 82.85 | |
| | FP(%) | 0.46 | | 95.33 | | 89.48 | | 14.28 | |

**Figure 2** Performance of detection results

The detection results are produced by inserting spams within Tm days first, and then the following one-day spams are tested. Note that each spam is inserted into the database after the process of matching. On the other hand, the entire set of hams is tested in each situation. True positive rate (i.e., TP, a real spam is classified as a spam) and false positive rate.

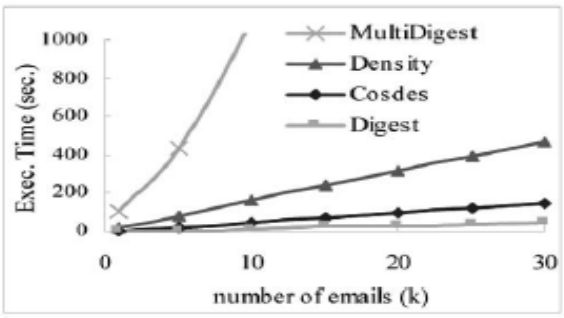



**Figure 3** Email abstraction with spam detection results

In the succeeding experiments, we initially examine the efficiency of near-duplicate matching. Owing to the fact that each incoming e-mail has to be matched with a huge spam database, the efficiency of near-duplicate matching is crucial to a collaborative spam detection system. On evaluation of matching performance, we consider the situation of matching with the number of e-mails varied while there are identical e-mails in the database.

## CONCLUSION

Instant messaging (IM) is a real-time communication service which allows a user to send a message, usually based on text, to other users. The major drawback has been the vulnerabilities associated with IM technology which creates several security issues. In this paper, we explore a more sophisticated and robust e-mail abstraction scheme, which considers e-mail layout structure to represent e-mails. The specific procedure SAG is proposed to generate the e-mail abstraction using HTML content in e-mail, and this newly-devised abstraction can more effectively capture the near-duplicate phenomenon of spams. Moreover, we design a complete spam detection system that considers other Spam Checking Criteria's besides Content-based filtrations.

## References

1. M. Fabri, D. Moore and D. Hobbs, “Empathy and Enjoyment in Instant Messaging,” IEEE International Workshop on Human- Computer Interaction, Sept. 2005.
2. Bird, Drew. “Instant Messaging: Corporate Productivity Tool or Cool Toy? “. *Intranet Journal*, May 1, 2003.
3. Hallett, Tony. “IM creates ‘rampant security risk’”. ZDNet UK. February 5, 2003.
4. Desmond, John. “Report: Secure IM Alternatives Growing”. eSecurity Planet: Trends. June 12, 2003.
5. Bird, Drew “Choosing an Instant Messaging System”. Instant Messaging Planet. July 16, 2003.
6. http://en.wikipedia.org/wiki/NTRUEncrypt
7. J. Hoffstein, J. Pipher, J. H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem,” Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998, pp. 267-288.
8. Sameer Hasan Al-Bakri, M. L. Mat Kiah, A. A. Zaidan, B. B. Zaidan and Gazi Mahabubul Alam: “Securing peer-to-peer mobile communications using public key cryptography: New security strategy”, *International Journal of the Physical Sciences* Vol. 6(4), pp. 930-938, 18 February, 2011.
9. Xiaoyu Shen; Zhenjun Du; Rong Chen: “Research on NTRU Algorithm for Mobile Java Security”, in International Conference Scalable Computing and Communications; Eighth International Conference on Embedded Computing (SCALCOM-EMBEDDEDCOM'09), 2009. page(s): 366 – 369
10. Chi-Yao Tseng, Pin-Chieh Sung, and Ming-Syan Chen,” Cosdes: A Collaborative Spam Detection System with a Novel E-Mail Abstraction Scheme”, IEEE Transactions On Knowledge And Data Engineering, Vol. 23, No. 5, May 2011.