INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

CONTENTS

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT ii

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

http://ijrcm.org.in/

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work**/**manuscript** *anytime* in *M.S. Word format* after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (*FOR ONLINE SUBMISSION, CLICK HERE*).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1.   **COVERING LETTER FOR SUBMISSION**:

                                                                                                                        DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.**

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to their inclusion of names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

http://ijrcm.org.in/

v

NOTES:

a) The whole manuscript has to be in ***ONE MS WORD FILE*** only, which will start from the covering letter, inside the manuscript. ***pdf. version*** *is liable to be rejected without any consideration*.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

   New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) **Abstract alone will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) *The journal gives acknowledgement w.r.t. the receipt of every email within twenty four hours* and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE**: The title of the paper should be **bold typed**, **centered** and **fully capitalised**.

3. **AUTHOR NAME (S) & AFFILIATIONS**: Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.

4. **ACKNOWLEDGMENTS**: Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.

5. **ABSTRACT**: Abstract should be in **fully italicized text**, ranging between **150** to **300 words**. The abstract must be informative and explain the background, aims, methods, results & conclusion in a **SINGLE PARA**. *Abbreviations must be mentioned in full*.

6. **KEYWORDS**: Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations.

7. **JEL CODE**: Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php, however, mentioning JEL Code is not mandatory.

8. **MANUSCRIPT**: Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. *It should be free from any errors i.e.* ***grammatical**, **spelling*** *or* ***punctuation.*** *It must be thoroughly edited at your end*.

9. **HEADINGS**: All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

10. **SUB-HEADINGS**: All the sub-headings must be bold-faced, aligned left and fully capitalised.

11. **MAIN TEXT**:

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESIS (ES)

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

LIMITATIONS

SCOPE FOR FURTHER RESEARCH

REFERENCES

APPENDIX/ANNEXURE

The manuscript should preferably range from ***2000*** *to* ***5000 WORDS***.

12.   **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text*.

13.   **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14.   **ACRONYMS:** These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15.   **REFERENCES:** The list of all references should be alphabetically arranged. *The author (s) should mention only the actually utilised references in the preparation of manuscript* and they are supposed to follow Harvard Style of Referencing. Also check to make sure that everything that you are including in the reference section is duly cited in the paper. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.

- Use (**ed.**) for one editor, and (**ed.s**) for multiple editors.

- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.

- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.

- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.

- For titles in a language other than English, provide an English translation in parenthesis.

- *Headers, footers, endnotes and footnotes should not be used in the document.* However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders after the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.

- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

SPAM ZOMBIE DETECTION SYSTEM

RUTUJA BANKAR
STUDENT
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR

JYOTI DESHMUKH
ASST. PROFESSOR
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR

SWATI DESHPANDE
ASST. PROFESSOR
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR

ABSTRACT

Compromised machines are one of the key security threats on the Internet. The key security threats on internet is compromised machines, which are used to launch security attacks such as spamming and spreading malware, Distributed Denial of Service and identity theft. The compromised machines in the network are identifying using SPOT algorithm. SPOT algorithm is designed on a powerful statistical tool called as Sequential Probability Ratio Test (SPRT). SPOT algorithm is declared as effective and efficient system in automatically detecting compromised machines in network. Spam Zombie Detection and Blocking Mechanism is an online spam zombie detection system in network. Along with the detection it also blocks the zombie system detected within the network. Zombie is defined as a compromised machine within the botnet. SPOT system is mainly implemented over the private mailing system. It also provides the enhanced security mechanism in which if the system which has been hacked gets blocked within the network and the legitimate owner of the system is provided with the secure password changing mechanism so that the possibility of the system getting hacked next time will be reduced. It also provides the strong mechanism which identifies whether the current user is legitimate user of the system or not with the help of some question answer mechanism. The overall proposed system is simply given a name as a Spam Zombie Detection and Blocking Mechanism.

KEYWORDS
spam zombie, security threats, blocking mechanism.

1. INTRODUCTION

In today's computing world, internet plays an important role in our daily lives in almost every aspect. It is the place where we do lot of things just sitting at one place. Internet not only influences the people to do positive works but also influences the people to trouble others by posing many attacks. These attacks are posed by the attackers directly or indirectly. Attacks are generally of two types, one of them is automatic attacks and the other type is manual attacks. Most of the successful attacks are from the automated generated code injected by the attackers. These are very dangerous some of them are Dos, DDos, E-mail Worms, Viruses, Worms, Trojan horses, phishing attacks etc...Attackers control some machines to attack the target machine .These machines are called drones, zombies or compromised machines. Zombies search for the low level secured systems to infect them and can control them through their pre-defined commands to cause an (DDoS) attack. In spamming terminology those are called as spam zombies. It is given that spamming is the major security challenge in the email communication. Report of 2012 march says that more than 75% of all email traffic is occupied by the spam. To detect these spam zombies is tough job for the system administrators.

Spamming is an important threat plaguing the internet from the past decades. More than 75% of traffic is spam and in that 0.4% was malicious. It is done by controlling several hosts to send unwanted messages to some target machines. These compromised machines are called spam zombies. Normally spam is given as UBE/UCE i.e., Unsolicited Bulk or Commercial E-mail. Spam message is an unwanted message to the users because of these reasons. They occupy the network bandwidth, disk space, connection time, money. They could hide viruses inside spam message, can send pornography information and can tempt the users to send their money and the confidential details. E-mail spamming became the major platform for the attackers because of its unique behaviour of low cost and high speed. It is given that spamming is the major resource for the attackers to get the incentives. They are earning around $200 billion dollars per year. In other words it is the cheapest one to one means of communication available today. That is why spamming is attracting the most of the attackers day by day.

There are two types of the botnet architectures that are used for spamming:
1. Centralized Botnet Architecture: Command and Control using IRC channels It is the centralized Command and Control mechanism that makes the use of the Internet Relay Chat channels. One can easily detect and disable this architecture.
2. Peer to Peer based Command and Control architecture: This architecture does not suffer from the single point of failure. Because of the absence of the centralized Command and Control servers, the bots can easily hide their communication. Thus, this architecture is hard to detect and disable.

2. REVIEW OF LITERATURE

ZhenhaiDuan, Peng Chen, Fernando Sanchez ,Yingfei Dong, Mary Stephenson, James Barker mainly focused on the detection of the compromised machines in a network that are involved in the spamming activities, commonly known as spam zombies. He develops an effective spam zombie detection system named SPOT by monitoring outgoing messages of a network. SPOT is designed based on a powerful statistical tool called Sequential Probability Ratio Test, which has bounded false positive and false negative error rates.

Majority of spammers are only active for a short period of time. GuofeiGu, JunjieZhang, and Wenke Lee identified botnet CCchannels in a local area network without any prior knowledge of signature or CC server addresses. Spam Zombie Detection proposes an approach that uses network based anomaly detection. CC servers and infected hosts in the network are identified by this detection approach. This approach is based on the observation that, because of there-programmed activities related to CC, bots within the same botnet will likely demonstrate spatial-temporal correlation and similarity .They engage in coordinated communication, propagation, and attack and fraudulent activities.

M.Vasu, K Munivara Prasad, Dr K VenugopalRao proposed Naive Bayesian approach of the content based method for detecting the spam messages and used SPRT algorithm for identifying the compromised systems in the internet. They compared the results of our approach with existing key word based method and proved that the detection accuracy of spam messages with proposed method improves the detection accuracy of Compromised systems in the internet.

Overview of the state of the art for spam filtering is studied by R.Malarvizhi, K.Saraswathi and the ways of evaluation and comparison of different filtering methods. This research paper mainly contributes to the comprehensive study of spam detection algorithms under the category of content based filtering. Then, the implemented results have been benchmarked to examine how accurately they have been classified into their original categories of spam. Key words: Spam, AdaBoost, KNN, Chi-Square, Black list, White list, Bayesian filters, Cache Architecture.

Ar.ArunachalamV.VevekV.Yogeswaran developed effective spam zombie detection system for detecting compromised machine in a network. SPOT is called Sequential Probability Ratio Test. It is a spam zombie detection system by monitoring outgoing messages, which has bounded false positive and false negative error rates. In addition, they also compare the performance of SPOT with two other spam zombie detection algorithms based on the number and percentage of spam messages forwarded by internal machines, respectively, and show that SPOT outperforms these two detection algorithms.

AmarishChaudhari Ravi Apare proposed the spam zombie detection and blocking with the efficient content filtering and user feedback mechanism is one of the online detection techniques. The system identifies the spam messages and blocks the sender of such messages. Zombie is single compromised machine within the network. The network of such compromised systems is called as a botnet. This system is based on the functionality of SPOT monitoring system which continuously monitors the outgoing messages within the network. The SPOT monitoring system makes the use of the strong statistical tool known as a Sequential Probability Ratio Test.

Manishankar, Sobin E. came up with a novel approach of machine learning to build a tool which predicts an email spam or not with the help of SPOT detection with SPERT algorithm, paper also deals with Zombie attacks and DDOS attacks

3. PROBLEM DEFINITION

Spam Zombie Detection and Blocking Mechanism is an online spam zombie detection system in network. Along with the detection it also blocks the zombie system detected within the network. Zombie is defined as a compromised machine within the botnet. SPOT system is mainly implemented over the private mailing system. It also provides the enhanced security mechanism in which if the system which has been hacked gets blocked within the network and the legitimate owner of the system is provided with the secure password changing mechanism so that the possibility of the system getting hacked next time will be reduced. It also provides the strong mechanism which identifies whether the current user is legitimate user of the system or not with the help of some question answer mechanism. The overall proposed system is simply given a name as a Spam Zombie Detection and Blocking Mechanism.

4. METHODOLOGY

EXISTING SYSTEM

Major security challenge on the Internet is the existence of the large number of compromised machines. Such machines have been increasingly used to launch various security attacks including spamming and spreading malware, DDoS, and identity theft. They are often used to launch various security attacks such as spamming and spreading malware, DDoS, and identity theft.

DETECTING SPAM ZOMBIES BY MONITORING OUTGOING MESSAGES

There is need to control the existing compromised systems over the network that perform the various security attacks. This paper mainly focuses on the detection of the compromised machines that send the spam messages which are also known as spam zombies. This system does not require the spamming global characteristics such as the size of the botnets and the spamming patterns of the botnets. This system has tool with the help of which an administrator can detect the compromised machines automatically. Thus this system is known as an online botnet detection system. Here the name given to this spam zombie detection system is SPOT system which monitors the outgoing messages. The statistical method called Sequential Probability Ratio Test (SPRT) is used to design the SPOT system. The SPRT method is used to test the two hypotheses Spam Zombie Detection and Blocking Mechanism which the machine is compromised and the machine is not compromised. This tool helps to minimize the expected number of observations used to take the decision. Here the user can define the threshold limit for the false positive and false negative probabilities required by the SPRT method. Thus the SPOT system can quickly identify the spam zombies within the network

PROPOSED SYSTEM

SPOT system is mainly implemented over the private mailing system. It also provides the enhanced security mechanism in which if the system which has been hacked gets blocked within the network and the legitimate owner of the system is provided with the secure password changing mechanism so that the possibility of the system getting hacked next time will be reduced. It also provides the strong mechanism which identifies whether the current user is legitimate user of the system or not with the help of some question answer mechanism. The overall proposed system is simply given a name as a Spam Zombie Detection and Blocking Mechanism.

FIG. 1: SYSTEM ARCHITECTURE
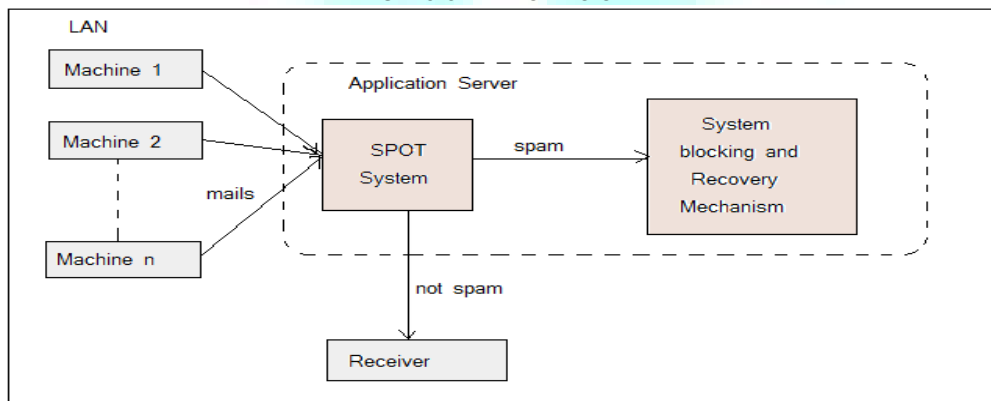
MODULE DESCRIPTION

Account authentication
- In this module to check the mail id and authenticate using OTP generation.
- If these two fields are valid, the account is authenticated.
- Otherwise is not valid.

Sending mails
- In this module a single person to send one or more mails to other person.
- This mails either spam or non spam.
- Spam means the more copies of the single message are send.
- And it contains more than 20 lines.

SPOT detection
- In this module to capture the IP address of the system.

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT   29

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

http://ijrcm.org.in/

- That system mails are applied to filtering process using java based Jasen Scanner.
- In this process, the mail content is filtered.

CT detection

- In this module to set the threshold value Cs
- Cs denotes the fixed length of spam mail.
- Also to count the number of lines in each mail.
- If the each mail, counts are greater than equal to threshold value.
- So, these mails are spam mail.

5. ALGORITHM OF THE PROPOSED METHOD

Spam Zombie Detection Algorithm:

1: An outgoing message arrives at SPOT
2: Get IP address of sending machine m
3: // all following parameters specific to machine m
4: Let n be the message index
5: Let $Xn= 1$ if message is spam, $Xn= 0$ otherwise
6: if ($Xn== 1$) then
7: // spam, Eq. 3
8: $¤n+ = ln\mu1$
$\mu0$
9: else
10: // no spam
11: $¤n+ = ln1-\mu1$
$1-\mu0$
12: end if
13: if ($¤n ¸ B$) then
14: Machine m is compromised. Test terminates for m.
15: else if ($¤n · A$) then
16: Machine m is normal. Test is reset for m.
17: $¤n = 0$
18: Test continues with new observations
19: else
20: Test continues with an additional observation
21: end if

The recovery and blocking functionalities of the system:

1: System is a Zombie.
2: Let n be the number of the important mails.
3: 'que' be security question and 'ans' be given answer,
4: declare total and threshold value
4: if(selectedQuestion==que) == and (ans== answer)then
5: take first 5 important mails subject.
6: for i=0 to i<5
7: choose the correct mail sender
8: If(choose correct sender) then
9: total++
10: endIf
11: endfor
12: if(total>=threshold) then
13: continue with account.
14: change your password.
15: else
16: block account permanently.
17: senders 'mac' block.
18: endelse
19: else
20: enter correct question and password.
21: endelse.

If the system is found as a Zombie system it is blocked temporarily and the user of that system when tries to login then he is informed that the system has been blocked. if the user wants to recover the system then it works as per the above algorithmIf the user fails to answer the questions correctly or enters the wrong username and OTP then the MAC address of the user is blocked so that the user account will be completely blocked.

6. SUMMARY

The proposed system detects the spam mails by monitoring the outgoing mails. The proposed system uses the Sequential Probability Ratio Test algorithm in order to detect the spam zombies. Depending upon the threshold limit given by the user this system minimizes the number of the required observation for detecting the spam zombies. The proposed system also provides the blocking mechanism in which if the system is identified as the spam zombie then the system gets blocked so that it cannot send the spam messages further. Also the proposed system helps to recover the blocked system in case if the system was hacked by an attacker and was used as a spam zombie.

Spam zombies are the major problem in the internet. It is increasing day by day very rapidly. To detect any machine as compromised, we must first classify the messages coming to that particular machine correctly and then detect the machine. In this paper we have implemented the two spam filters based on keyword based and naïve-Bayesian algorithm to classify a message as spam or non-spam and we have shown that Naïve-Bayesian works efficiently and gives more results when we train more number. We proved that detecting a compromised machine depends on false positives and false negatives generated by the deployed spam filter with SPRT algorithm.

REFERENCES
1. AmarishChaudhari Ravi Apare "Spam Zombie Detection and Blocking with Efficient Content Filtering and User Feedback Mechanism" International Journal of Advanced Research in Computer Science and Software EngineeringVolume 4, Issue 7, July 2014
2. Ar.ArunachalamV.VevekV.Yogeswaran"Detecting Spam Zombies Using Spot Tool By Monitoring Outgoing Messages" International Journal of Advanced Research in Computer Science and Software EngineeringVolume 3, Issue 4, April 2013
3. Duan, Z., Chen, P., Sanchez, F., Dong, Y., Stephenson, M., & Barker, J. M. "Detecting spam zombies by monitoring outgoing messages" Dependable and Secure Computing, IEEE Transactions (2012).
4. G. Gu, J. Zhang, and W. Lee. "BotSniffer: Detecting botnet command andcontrol channels in network traffic." In Proceedings of the 15th AnnualNetwork and Distributed System SecuritySymposium (NDSS 2008), SanDiego, CA, Feb. 2008.
5. Hovold, Johan. "Naive Bayes Spam Filtering Using Word-Position-Based Attributes." *CEAS*. 2005.
6. L. Zhuang, J. Dunagan, D. R. Simon, H. J. Wang, I. Osipkov, G. Hulten,and J. D. Tygar. "Characterizing botnets from email spam records." InProc. of 1st Usenix Workshop on Large-Scale Exploits and EmergentThreats, San Francisco, CA, Apr. 2008.
7. M. Xie, H. Yin, and H. Wang."An effective defense against email spamlaundering."In ACM Conference on Computer and Communications Security, October 30 - November 3 2006.
8. M.Vasu, K Munivara Prasad, Dr K VenugopalRao "Detection of Spam messages and Spam zombies in the Internet using Naïve Bayesian and SPRT" American International Journal of Research in Science, Technology, Engineering & Mathematics 2013
9. Manishankar, Sobin E."Spam and Zombie Detection System with Machine Learned Spot Algorithm" International Journal of Science and Research (IJSR) Volume 3 Issue 6, June 2014
10. N. Ianelli and A. Hackworth."Botnets as a vehicle for online crime."InProc. of First International Conference on Forensic Computer Science,2006.
11. R.Malarvizhi, K.Saraswathi"Content-Based Spam Filtering and Detection Algorithms- An Efficient Analysis & Comparison" International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 9- Sep 2013
12. Y. Xie, F. Xu, K. Achan, R. Panigrahy, G. Hulten, and I. Osipkov."Spamming botnets: Signatures and characteristics." In Proc. ACMSIGCOMM, Seattle, WA, Aug. 2008.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other
Journals