iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: http://doi.org/10.22214/ijraset.2020.7067

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

Safety Measures using Spam Mail Discovery and Filtering Network Safety

Ramiya S[1], Karthik P[2]
[1]*Student. Department of Computer Science Prist University Thanjavur, M.C.A.,*
[2]*Assistent Professor, Department of Computer Science Prist University Thanjavur.*

Abstract: Securing the message in a social network is a big task for us. There are many types of intruder watching with eagle eyes to attack the system. The client's private messages were stolen by the hackers and it makes the client to be in a depressed mood. Another headache in email is spam messages. Lots of spam message was sent. Recently, Google's Gmail facing this problem. The Gmail system can't filter it properly. To avoid this entire "con" in email system the proposed system has been implemented. Each mail will have its own code to be verified the message.

I. INTRODUCTION

In the network security contains various protocol, rules, policies and practical adapt to observe and avert the illegal action and threat of a network and it's accessible sources. Network security can stop, the computer viruses if it has been activated. The users are encouraged to assign an ID and secret key or other authentication information which is private, only can be accessed by the user only. With that secret key or authentication information, they can access to the information within their authority, not even the administration has the rights to break the security access of their client.

The network is often private, like within a cooperation. The most common method of protecting a network resource is by assigning it a name and password. However, as we say, spam is another major disadvantage found in the mail system. Bulk amount of spam mail has sent to a user, this makes lots of trouble for the clients. For this, a tool will be applied which will be very useful and efficient in the work.

II. PROBLEM STATEMENT

Unnecessary junk mail and spam mail causes irritation to the clients. This problem also arises with duplication of mail. Internet merchant will send mail regarding their work to attract new customers. Secondly, the threat of being hacked the server of the mailing system still exist. This is what happen to the Yahoo mail system. For thus lots of clients worried about their privacy. The intruder also sends viruses through the mail to hack someone's personal system to gather or erase his/ her information or data. By this lots of clients have been affected by this issues.

A. Unnecessary junk mail and spam mail is finds a lot.
B. Duplicate mails found.
C. The threat of being hacked.
D. Sending a virus through the mail.

III.PROPOSED SYSTEM

Here we are going to apply the security system more strictly to filter for spam mails and also to avoid duplication. By improving the security system to this level, surely give a big success and more clients will be attracted. Redundancy will be reduced to a certain level so that only important mail will have duplication, not all the mails. The viruses spreading through the mail should completely being avert totally. This would be possible by verifying the mails at two levels. For this reason the tool we are going to apply in the mail system help us. It will work simultaneously to fulfil all the function that has been mentioned.

A. Unnecessary junk mail and spam mail have been filtered.
B. Redundancy will be maintained appropriately.
C. The threat of being hacked will be reduced
D. Sending virus through mail decreased.

©IJRASET: All Rights are Reserved

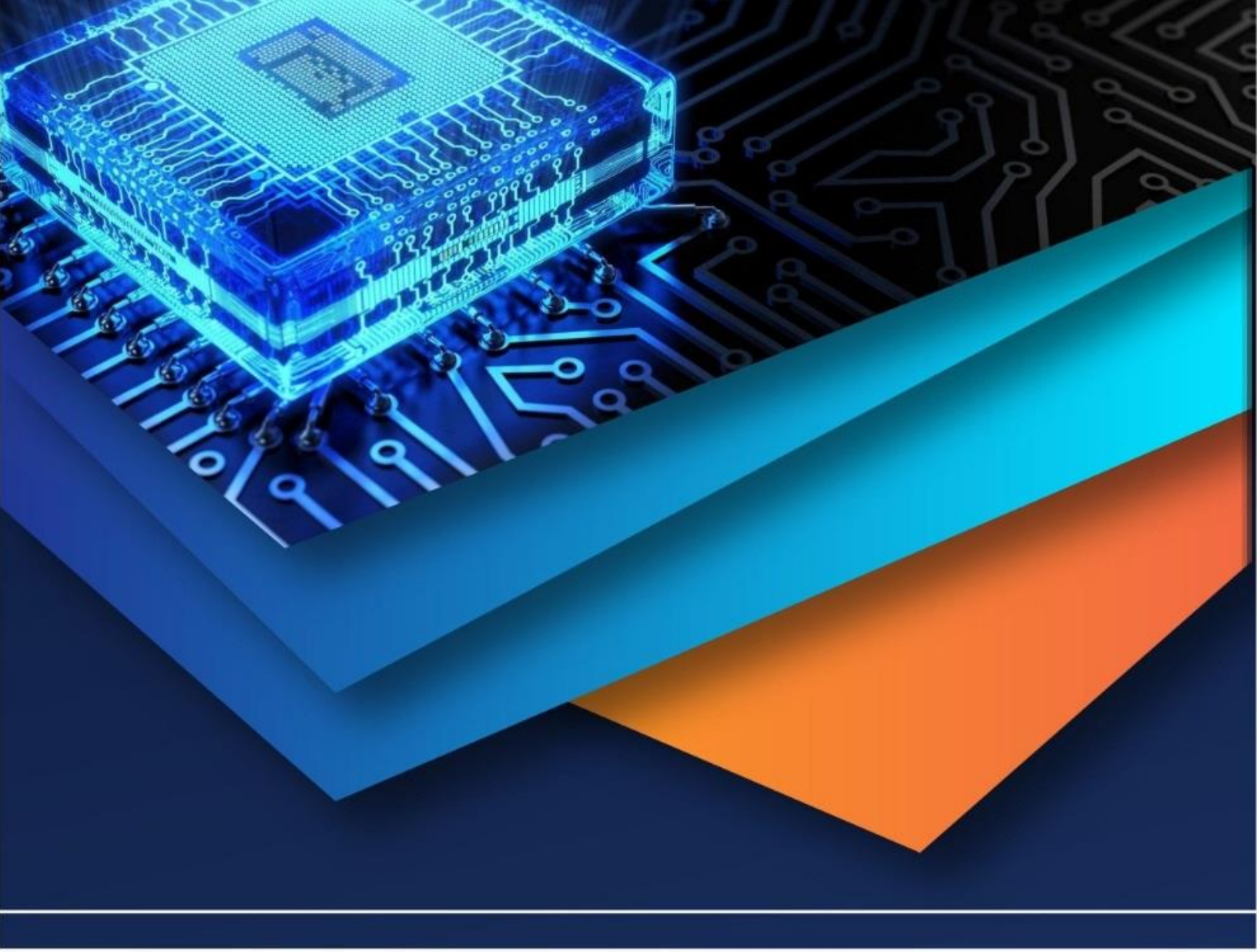
IV. CONCLUSION

This tool also can be implemented to detect picture and advertising spam as this one is completely based on the content spam filtering. This tool will be very helpful to overcome the problem facing through the mailing system. This tool helps to reduce the redundancy and spam filtering failure. And as a final point, apart from spam attacks quite a lot of other attacks can also be paying attention along with the protecting procedures.

REFERENCES

[1] C. MacFarlane, (2003), "FTC Measures False Claims Inherent in Random Spam," Federal Trade Commission, http://www.ftc.gov/opa/2003/04/spamrpt.shtm, Accessed Jul. 20, 2011.
[2] L. Nosrati & A. Nemaney Pour, "Dynamic Concept Drift Detection for Spam Email Filtering," Proceedings of ACEEE 2nd International Conference on Advances Information and Communication Technologies (ICT 2011), Amsterdam, Netherlands, pp. 124-126, Dec. 2011.
[3] A. Ramachandran, D. Dagon & N. Feamster, "Can DNS-Based Blacklists Keep Up with Bots?," The Third Conference on Email and Anti-Spam (CEAS 2006), California, USA, pp.1- 2, Jul. 2006.
[4] J. Goodman, "Spam: Technologies and Policies," White Paper, Microsoft research, pp.1- 19, Feb. 2004. International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012 62
[5] A.Ramachandran & N. Feamster, "Understanding the Network-Level Behavior of Spammers," Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM 2006), Pisa, Italy, pp. 291-302, Sep. 2006.
[6] E. Harris, (2003), "Greylisting: The Next Step in the Spam Control War," White Paper, http://projects.puremagic.com/greylisting/whitepaper.html, Accessed Dec. 20, 2011.
[7] J.R. Levine, "Experience with Greylisting," Proceedings of Second Conference on Email and Anti-Spam (CEAS 2005), CA, USA, pp. 1-2, Jul. 2005.
[8] P. Graham, "Better Bayesian filtering," MIT Spam Conference, Jun. 2003..
[9] H. Yin & Z. Chaoyang, "An Improved Bayesian Algorithm for Filtering Spam E-Mail," IEEE 2nd International Symposium on Intelligence Information Processing and Trusted Computing(IPTC 2011), Huangzhou, China, pp. 87-90, Oct. 2011.
[10] A. Ciltik & T. Gungor, (2008), "Time-efficient spam e-mail filtering using n-gram models," Elsevier,Pattern Recognition Letters, Vol. 29, No. 1, pp. 19-33.
[11] M.Lakshmi Lecturer in PG Dept.of.Computer Science & Applications, Bharathidasan university constituent college for Women Orathanadu-614625 International Journal of Engineering and Techniques - Volume 4 Issue 1, Jan – Feb 2018.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)