from their email only. If email does not exist then it will automatically report an error at the same time.

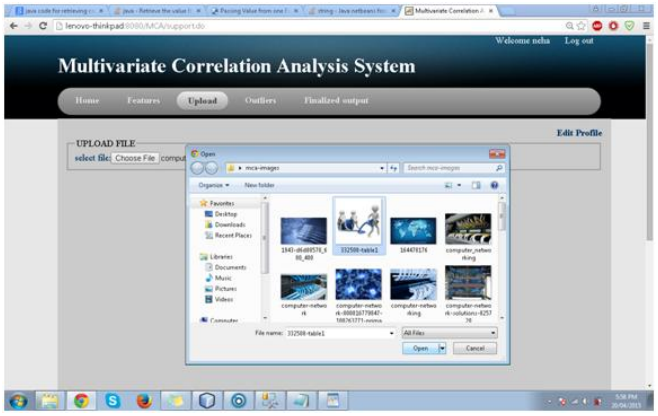

Figure 6: Upload: - User can select the file which he wants to upload by browsing it. After the selection the upload button is used to upload it on the web.

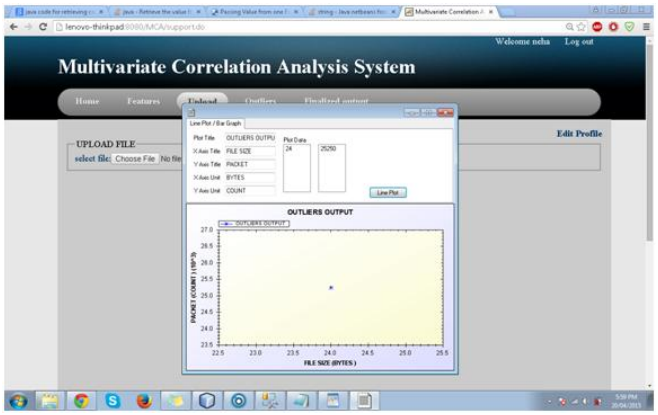

Figure 7: Our system will check the uploaded file by analyzing the report.

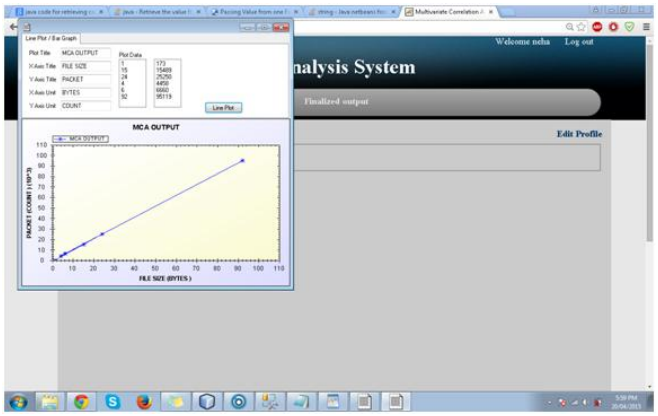

Figure 8: If file does not contain any malicious content it will be uploaded successfully else error can occur & will not be processed any more.

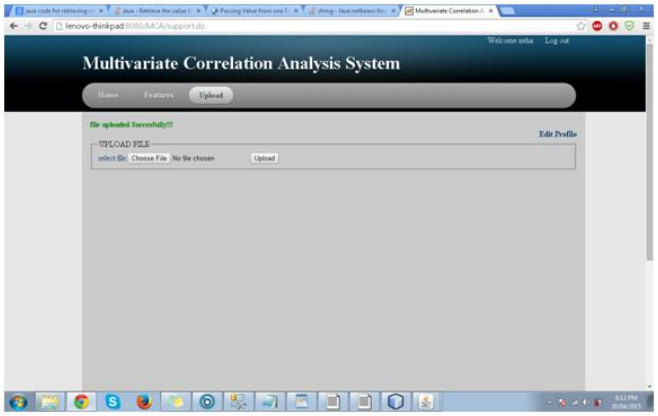

Figure 9

6. Conclusion

With the number of DoS attacks increasing over the past years and many online services are becoming victims of these attacks, it is important that network engineers, designers, and operators build services in the context of defending against DoS attacks. The main intention of DoS attacks is to consume resources, such as memory, CPU processing space, or network bandwidth, in an attempt to make them unreachable to end users by blocking network communication or denying access to services. Thus in this paper a MCA-based DoS attack detection system is developed which is powered by the triangle-area based MCA technique and the anomaly-based detection technique. The MCA technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offers more accurate characterization for network traffic behaviors. The Anomaly-based detection technique facilitates the system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic.

References

[1] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges," Computers & Security, vol. 28, pp. 18-28, 2009.

[2] A. A. Cardenas, J. S. Baras, and V. Ramezani, "Distributed change detection for worms, DDoS and other network attacks," The American Control Conference, Vol.2, pp. 1008-1013, 2004.

[3] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Cost based modelling for fraud and intrusion detection: results from the JAM project," The DARPA Information Survivability Conference and Exposition 2000 (DISCEX '00), Vol.2, pp. 130-144, 2000.

[4] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Triangle- Area-Based Multivariate Correlation Analysis for Effective Denialof- Service Attack Detection," The 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, United Kingdom, 2012, pp. 33-40.

[5] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Denialof- Service Attack Detection Based on

Multivariate Correlation Analysis," Neural Information Processing, 2011, pp. 756-765.

[6] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R. P. Liu, "RePIDS: A multi tier Real-time Payload-based Intrusion Detection System," Computer networks, vol. 57, pp. 811-824, 2013.

[7] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011