PROCEEDINGS

NATIONAL CONFERENCE
ON
INNOVATIVE TECHNOLOGIES & ADVANCED COMPUTING

Sep 11th, 2015

Organized by :

PG Department of Computer Applications

Fatima College (Autonomous)

(College with Potential for Excellence)

(Re-Accredited with A-Grade by NAAC)

Madurai-18.

www.fatimacollegemdu.org

NATIONAL CONFERENCE ON INNOVATIVE TECHNOLOGIES AND ADVANCED COMPUTING

NCITAC'15

Edited by

PG Department of Computer Applications

Fatima College
Autonomous
College with Potential for Excellence
Re-Accredicted with "A" Grade by NAAC
Mary Land, Madurai-18.

[3] S.Arivazhagan, R.Newlin Shebiah, S.Selva Nidhyanandhan, L.Ganesan, *"Fruit Recognition using Color and Texture Features"*, Journal of Emerging Trends in Computing and Information Sciences, E-ISSN 2218-6301, VOL. 1, NO. 2, Oct 2010

[4] Woo Chaw Seng, Seyed Hadi Mirisaee, *"A New Method for Fruits Recognition System"*

[5] F.S. Mohamad, A.A. Manaf, S. Chuprat, *"Nearest Neighbor For Histogram-based Feature Extraction"* International Conference on Computational Science, Procedia Computer Science 4 (2011) 1296–1305

[6] Monika Sharma, Vibhuti P N Jaiswal, Amit Goyal, "Fruit Detection with Multiple Features using Fuzzy Logic", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013

[7] Azizi Abdullah, Remco C. Veltkamp, Marco A. Wiering, *"Fixed Partitioning and Salient Points with MPEG-7 Cluster Correlograms for Image Categorization"* ISSN: 0924-3275

23. IMPACT ANALYSIS OF REAL TIME DDOS ATTACK DETECTION AND MITIGATION USING MACHINE LEARNING – G.PREETHA

Assistant Professor, Dept. of Computer Applications, Fatima College, Madurai.

Abstract— Distributed Denial of service (DDoS) attacks is the most devastating attack which tampers the normal functionality of critical services in internet community. DDoS cyber weapon is highly motivated by several aspects including hactivitism, personal revenge, anti-government force, disgruntled employers/customers, ideological and political cause, cyber espionage and so on. IP spoofing is the powerful technique used by attackers to disrupt the availability of services in the internet network by impersonating as a trusted source. Since the spoofed traffic shares the same resources as that of the legitimate one's detection and filtering becomes very essential. The proposed model consists of online monitoring system (OMS), spoofed traffic detection module and interface based rate limiting (IBRL) algorithm. OMS provides DDoS impact