(54) Title of the invention : A SYSTEM AND METHOD FOR DETECTING AND RESPONDING TO BOTNET ATTACKS

(51) International classification	:H04L0009000000, H04L0043160000, H04L0067020000, H04W0076150000, G06F0021550000
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
  1)**Chitkara University**
    Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------
  2)**Bluest Mettle Solutions Private Limited**
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
  1)**MISHRA, Rahul**
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------
  2)**PANDEY, Sakshi**
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------
  3)**SHARMA, Bhanu**
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :
The present invention discloses a system (100) for detecting and responding to one or more botnet attacks. The system (100) comprises a server (106) that establishes secure communication channels with computing devices (110), along with a processor (102) and memory (104) containing a set of instructions. The set of instructions cause the processor to scan network traffic between computing devices (110) and networks (108). The scanned network traffic is then compared with a database of known network traffic associated with botnet attacks. Based on this comparison, the system (100) detects the presence or absence of botnet attacks in the network traffic and responds accordingly. Additionally, upon detecting the presence of botnet attacks, the system (100) generates and transmits alert signals to the computing devices (110).

No. of Pages : 26 No. of Claims : 10