(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :10/05/2019

(21) Application No.201941018711 A
(43) Publication Date : 07/06/2019

(54) Title of the invention : SDCC-DEVICE: STRANGELY DETECT AND CONTROL CYBERCRIME DEVICE

(51) International classification :G06F21/00
(31) Priority Document No :NA
(32) Priority Date :NA
(33) Name of priority country :NA
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)Name of Applicant :
1)NAGARJUNA PITTY
Address of Applicant :SENIOR SCIENTIST OFFICER , INDIAN INSTITUTE OF SCIENCE, CV RAMAN RD, BENGALURU 560012 Karnataka India
2)DR. SANTOSH TUKARAM JAGTAP
3)DR. RAJARAJESWARI. P
4)ANITA BAI
5)DR. SHAIK KHAMURUDDEEN
6)DR. L VANKATESHWAR REDDY
7)P. ILA CHANDANA KUMARI
8)PROF.(DR.) BEG RAJ
(72)Name of Inventor :
1)NAGARJUNA PITTY
2)DR. SANTOSH TUKARAM JAGTAP
3)DR. RAJARAJESWARI. P
4)ANITA BAI
5)DR. SHAIK KHAMURUDDEEN
6)DR. L VANKATESHWAR REDDY
7)P. ILA CHANDANA KUMARI
8)PROF.(DR.) BEG RAJ

(57) Abstract :
This invention is to designed and identifies cyber users as a strategy to detect and control cybercrime. The motivation was premised on the fact that every cyber user must create some impressions which are verifiable to identify him. The methodology adopted is the object oriented paradigm of system analysis and design. The crime scenario considered for detection is phasing, identity theft and data theft. The platform for implementation of the system is PHP ,java and Anguler-2. MySQL was used as the database. The hardware used for implementation has inbuilt webcam or attached digital camera for facial image capturing, a Real time-GPS sensor to locate a cyber-user™s position, and a fingerprint scanner. The invention is modeled to provide interfaces to capture the digital signatures, Biometric input, for each information sent to the cyberspace, the user™s fingerprints and facial image as mandatory login parameters, identify and record the geographical location of the user, the MAC address of the system used, the date, time and the kind of action carried out by the user while online, then record security threats for further investigation by cybercrime investigators. The results showed that the system can genuinely identify the cyber user and his/her criminal activities while online. Also this invention is providing the strongest tool to detect the cybercrime with real time. We are used as a first line of defence against this unusual sort of crime Since cybercrime is like a smart key, we can build a smarter keyhole to detect illegal entry. We can do that by detecting attempts to pick the lock. Smart locks can detect smart crimes. Cybercrime detection acts like a smart lock, and so detection of cybercrime (picking the lock) involves monitoring computers, computer networks, and network servers that play important roles in information systems. Sometimes we classify cybercrime using cyber-attack at an advanced cybercrime (high-tech crime) these are sophisticated attacks against computer hardware and software - like online scams (fraud), identity theft, email spam, and phishing. In other words, advanced cybercrime is using a computer to attack other computers.

No. of Pages : 21 No. of Claims : 10