(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :10/06/2020
(21) Application No.202041024434 A
(43) Publication Date : 19/06/2020

(54) Title of the invention : PREDICTION OF THRESHOLD VALUE FOR CLOUD STORAGE SECURITY PARAMETER BY EFFICIENT MEANS OF ASSO GENETIC ALGORITHM

(51) International classification	:H04L 9/08
(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)Dr. K. Anbazhagan
Address of Applicant :Associate Professor Department of Computer Science & Engineering Velammal Institute of Technology, Panchetti, Chennai-601204. Ph:6374775259 rishianbu@gmail.com Tamil Nadu India
2)Dr. P. Deivendran
(72)**Name of Inventor :**
1)Dr. K. Anbazhagan
2)Dr. P. Deivendran
3)Dr. R. Sugumar
4)S. Ezravethamani
5)K. Diala
6)K. Mahendran

(57) Abstract :
Cloud computing is a type of internet-based computing, and it is one of the foundations of the next generation computing. It offers on demand provisioning of resources over the Internet. Cloud computing enables individuals and organization to use various services like software as a service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) over the Internet. Even though cloud attracts lot of attention still there is a prime requirement of security concerns needs to be taken care. This work aims to address the security problem in cloud and predicts the threshold value of cloud security parameter have attained threshold stage when proposed with Proficient Two Level Security Contrivance (PLTC) and Hybrid Cryptography-Steganography Technique(HCST) along with asso genetic algorithm. Cryptography plays major role to secure ATM transmission, E-commerce, digital media privacy and web data transmission or storage. Modern cryptography works for the following concern, repudiation, integrity, authentication and confidentiality. In order to provide robust security to the cloud lightweight cryptographic scheme called signcryption is introduced which is a logical combination of encryption and signature. In the subsequent level of security, encrypted data are Steganographed using Biorthogonal Wavelet Transforms (BWT), along with that embedding and extraction is done with the use of advanced social spider optimization algorithms. In experimental results, the threshold value of cloud security parameter such as Peak signal-to-noise ratio (PSNR) and Normalized Correlation (NC) , Time(ET), Upload Time (UT), outperforms the existing traditional method when used with Enhanced Social Spider Optimization (ESSO) . The scenario of with attacks and without attacks (Noise, Blurring, and Filter) is considered using Enhanced Social Spider Optimization (ESSO), Social Spider Optimization (SSO) algorithms and Cuckoo Search (CS). Experiment results shows that proposed way of predicting the cloud security parameter attains a peak value and efficient compared to other method. Keywords: Cryptography, Steganography, Peak signal-to-noise ratio, Normalized Correlation.

No. of Pages : 20 No. of Claims : 4