Expert System: Debugging Using MD5 Process Firewall

Authors : C. U. Om Kumar, S. Kishore, A. Geetha

Abstract : An Operating system (OS) is software that manages computer hardware and software resources by providing services to computer programs. One of the important user expectations of the operating system is to provide the practice of defending information from unauthorized access, disclosure, modification, inspection, recording or destruction. Operating system is always vulnerable to the attacks of malwares such as computer virus, worm, Trojan horse, backdoors, ransomware, spyware, adware, scareware and more. And so the anti-virus software were created for ensuring security against the prominent computer viruses by applying a dictionary based approach. The anti-virus programs are not always guaranteed to provide security against the new viruses proliferating every day. To clarify this issue and to secure the computer system, our proposed expert system concentrates on authorizing the processes as wanted and unwanted by the administrator for execution. The Expert system maintains a database which consists of hash code of the processes which are to be allowed. These hash codes are generated using MD5 message-digest algorithm which is a widely used cryptographic hash function. The administrator approves the wanted processes that are to be executed in the client in a Local Area Network by implementing Client-Server architecture and only the processes that match with the processes in the database table will be executed by which many malicious processes are restricted from infecting the operating system. The add-on advantage of this proposed Expert system is that it limits CPU usage and minimizes resource utilization. Thus data and information security is ensured by our system along with increased performance of the operating system.