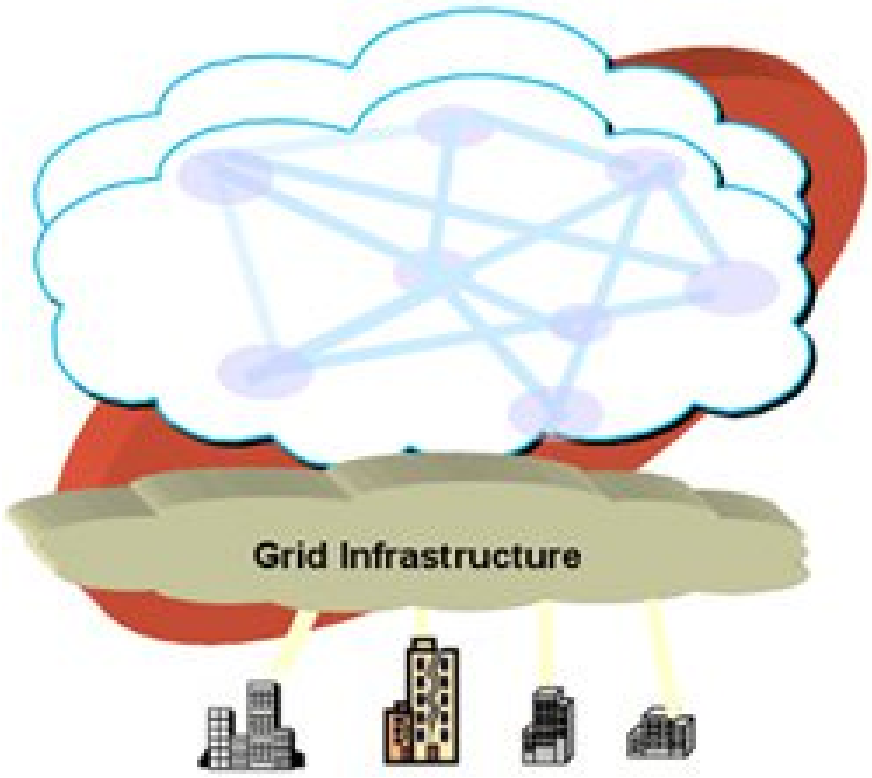
New weapons against malicious code are 'cloud' computing.

The 'cloud computing' model of remote server-based data processing and results returned to the PC will incorporate 10 antivirus engines and two hackers to detect hackers to prevent the malicious code.



The remote "cloud computing" data processing model and returning results to the PC will combine 10 anti-virus machines and two hackers to detect hackers so as not to let the malicious code slip.

Researchers at the University of Michigan (USA) said their CloudAV service is a multi-layer shield that works in tandem so that this class virus is prevented in another class.

To use CloudAV, users will install a monitoring program (host agent) on the computer (running Windows, Linux, FreeBSD) or mobile device. The program controls new files and software that are written to disk, a cache created for previously analyzed files to reduce network load. New files that are not recognized in the cache will be sent to the analytics server (in about 1.3 seconds).

In the last 6 months of testing, CloudAV has detected 98% of 7,220 malicious samples. The single anti-virus engine only managed 83%. Researchers say this will not replace the antivirus program on the workstation, but a

combined solution to increase prevention.

Currently, each individual antivirus program on the PC still reveals many limitations and cannot scan the intrusion code, while installing many programs will slow down the computer, causing inconvenience to users. In addition, there is a time period between when the threat appears until the antivirus program is updated, so the risk is huge.