

[Press Release]

September 10th, 2008.

KDDI R&D Laboratories, Inc.

A New Distributed File System for Management of Confidential Information
- Protecting Secret Files by Ultrahigh-Speed Secret Sharing Scheme -

KDDI R&D Laboratories, Inc. has invented a new distributed file system for management of confidential information, which protects secret files from both data leakage and destruction by using a new secret sharing scheme we developed, Ultrahigh-Speed Secret Sharing Scheme.

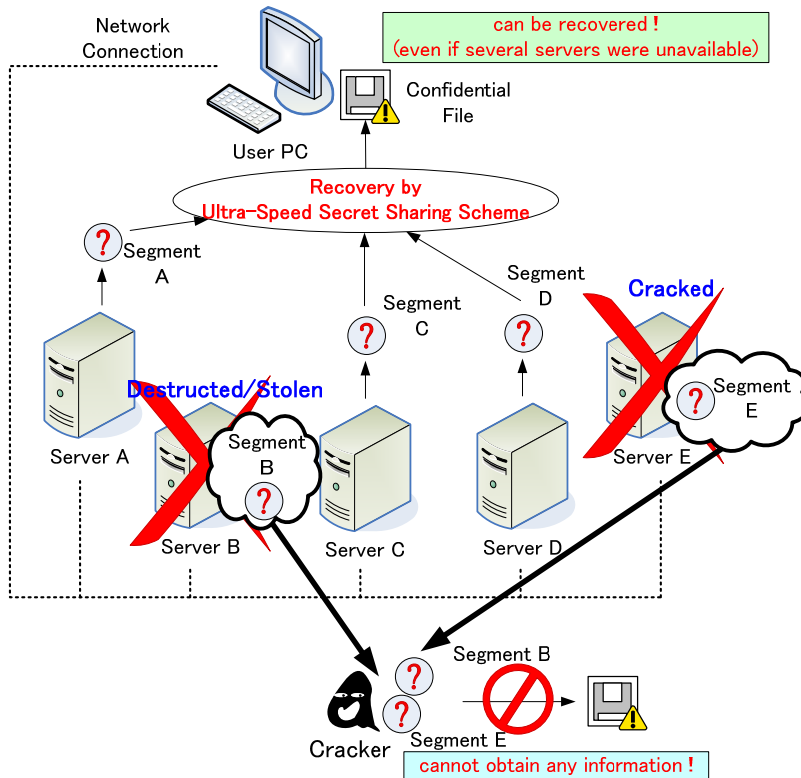
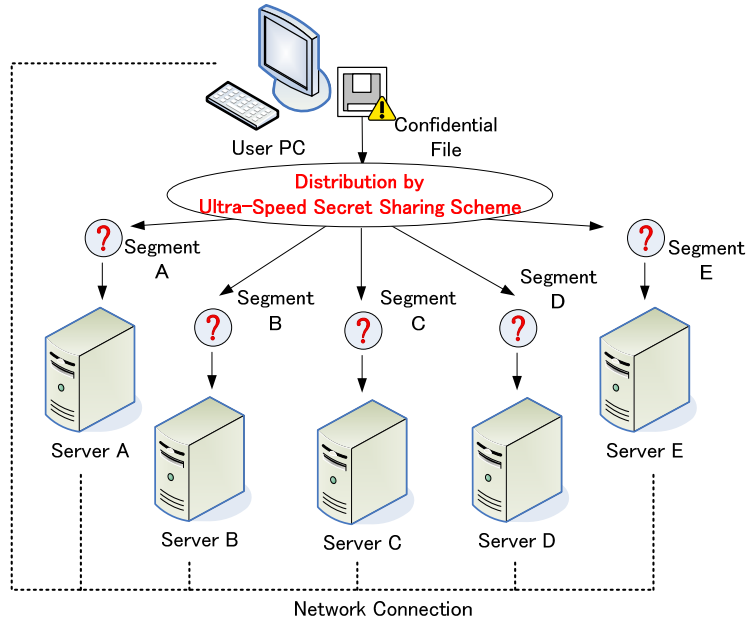
From the backgrounds of effectuation of Private Information Protection Law, rising accidents of information leakage and so on, the technology 'Secret Sharing Scheme'⁽¹⁾ receive a lot of attention, recently. In the conventional method of this technology, heavy computational cost is required to process the secret information. However, in the new method which we developed and used in this distribution system, the ultrahigh-speed processing and the same level security as the conventional method are realized.

By using the developed system, user can realize the high-level security such that any information about the confidential information is not leaked even if one of the distributed servers and storages is cracked by a black hacker. Moreover, the system is also fault tolerant. Even if some of servers are destroyed by disaster, the confidential information can be recovered from survived servers. The developed system works on PCs with Microsoft Windows⁽²⁾ and can be used by easy operations similar to Windows Explore. Also, because of introducing Ultrahigh-Speed Secret Sharing Scheme, the operation in this system is as fast as regular operations to copy files via networks and stress-free operability is achieved.

We will consider promoting the new security solution services using this distributed system. We are also planning to promote licensing the library of Ultrahigh-Speed Secret Sharing Scheme, the core module of this development. We will talk about this Ultrahigh-Speed Secret Sharing Scheme at Information Security Conference 2008 (ICS'08, September 15th~18th, 2008, in Taipei, Taiwan), which is one of the top-level International Conferences about information security.

(Appendix)

- (1) Secret Sharing Schemes : This technology realizes the protection of secret files against both data leakage and destruction. In secret sharing schemes, several information segments which have no information about the secret file are generated (distribution), and the secret file can be recovered only from a certain number of segments (recovery).
- (2) We are planning to develop variations for other Operating Systems, Linux and so on.



Overview of the system