
정보보호를 위한 능동적 스토리지 가상화 시스템 설계

조경옥* · 한승조**

The Design of Active Storage Virtualization System for Information Protection

Kyoung-ok Cho* · Seung-jo Han**

요 약

현대 사회에서는 정보 시스템을 이용한 업무의 편의성과 효율성은 높아지고 있지만, 네트워크의 발달로 인한 악성코드, 시스템 해킹, 내부자 정보유출 등의 역기능이 날로 대두되고 있다. 이로 인하여 시스템의 복구와 관리에 막대한 인력과 비용이 소요되고 있다. 기존의 시스템은 두 가지 측면에서 바이러스, 악성코드를 감시하고 치료하는 보안 솔루션과 컴퓨터의 시스템감시, 관리, 복구, 백업 등 유지보수를 하는 네트워크 관리 솔루션으로 나눌 수 있다. 본 논문에서는 Active Write Filter 메커니즘, NFS기반의 기술을 응용하여 기존 시스템의 사용자 데이터 등의 보전 문제점을 보완하여 정보보호 및 불법 저작물 등 지적재산권의 문제 해결이 가능한 시스템을 설계하였다.

ABSTRACT

In contemporary society, though convenience and efficiency of work using information system is growing high, adverse effect problems of malignant code, system hacking, information leak by insiders due to the development of the network are raising their head daily. Because of this, enormous work forces and expenses for the recovery and management of system is needed. The existing system can be divided into two aspects: security solution which surveils and treats virus and malignant codes, and network management solution which observes the system of computer, and practices maintenance and repair such as management, recovery, backup. This treatise applied Active Write Filter mechanism and the technology based on NFS and complemented the maintenance problems of user data of the existing system and designed the system which enables solving problems of intellectual property right such as information protection and illegal work.

키워드

백업, 복구, Write Filter, 파일시스템, 정보보호

Key word

Backup, Recovery, Write Filter, NFS(Network File System), Protection

* 조선대학교 정보통신공학과 박사과정 (sign57421@gmail.com)

** 조선대학교 정보통신공학과 교수

접수일자 : 2010. 08. 05

심사완료일자 : 2010. 08. 12

I. 서 론

인터넷 환경의 급속한 발전과 유비쿼터스 컴퓨팅 환경으로의 진화로 네트워크는 없어서는 안 될 경제·사회의 중요한 원동력이 되고 있다[1]. 현재 기업과 공공기관, 교육기관 등 사회 전반에 걸쳐 컴퓨터 및 서버를 이용한 인트라넷, 교육 시스템, 네트워크, 웹서비스 등이 구축되어 있다. 2009 모든 업무나 행정에 있어서 컴퓨터는 없어서는 안 되는 필수 요소로 업무 효율 및 작업 능력, 서비스 개선 등에 많은 도움이 되고 있다.

하지만 정보전산화, 네트워크 구축 등 인프라의 증가는 많은 부작용을 가지고 있으며, 특히 바이러스, 악성코드, 해킹 툴 등의 비인가자에 의한 시스템 손상이나, 불법 소프트웨어 사용으로 피해가 증가하고 있는 추세이다. 이러한 불법 침해로 인하여 시스템의 복구와 관리에 막대한 인력과 비용이 소요되어 기관에 많은 손실을 입히고 있다.

현재 이를 관리하기 위한 시스템이 설치 운영되고 있으며 크게 백업 시스템과 네트워크 관리 시스템으로 나눌 수 있다.

백업 시스템은 컴퓨터에 설치되어 있는 OS 및 응용 프로그램을 이미지화하여 파일로 저장하고, 필요시 이미지 파일을 이용하여 덮어쓰우는 방식을 사용한다 [2-3]. 기존 백업 시스템은 초기 설치 환경으로의 복구는 가능하나 응용프로그램 추가, 작업 내용, 문서 파일, 자료 등의 변경 사항을 백업하거나 복구하기에는 어려움이 따르고 능동적으로 활용하기는 어려운 실정이다.

네트워크 관리 시스템은 네트워크 환경에서 기관내의 컴퓨터 시스템을 관리, 유지, 보수 하는데 있어서 효율적인 운영 환경을 제공 하지만 운영 관리상의 문제점으로 인하여 사용자의 욕구 충족과 더 나은 성능을 제공하기 위한 새로운 기술이 필요하다고 할 수 있다 [4-6].

본 논문에서는 기존 시스템의 문제점인 위험요소를 제거하는 방식이 아니라 AWF(Active Write Filter) 메커니즘을 이용하여 컴퓨터시스템에 수록되는 모든 데이터에 대하여 재 부팅시 자동으로 데이터 기록에 대한 취소 명령을 내림으로써 유해한 코드를 자동 제거할

수 있도록 하며, 사용자가 직접 작성한 데이터에 대하여서는 Write Filter에 대한 예외사항으로 처리함으로써 백신 없이도 유해코드에 대한 방어 및 항상 최적으로 시스템 환경을 유지가 가능한 시스템을 구현하고자 한다.

2장에서는 기존에 시스템을 소개하고 이에 대한 문제점을 제시하고, 3장에서는 제안하는 AWF 메커니즘과, NFS기술의 기법에 의한 시스템 설계를 설명한다. 4장에서는 본 논문에서 제안된 기법으로 설계된 기술을 구현 및 비교 분석하고, 5장에서는 결론 및 향후 연구방향을 기술한다.

II. 관련 연구

2.1 WF(Write Filter) 메커니즘

Write Filter는 기본적으로 OS 이미지를 보호하기 위해 적용하게 되며, 저장 미디어의 쓰기 액세스 시 발생할 수 있는 섹터 에러를 줄이는 목적으로 사용된다. FBWF(File-Base Write Filter)는 OS 이미지를 보호함으로써 시스템이 부팅 조차 할 수 없는 상태로부터 벗어날 수 있도록 해주며, 사용자의 실수 또는 월/바이러스에 의해 시스템이 임의 변경되는 것을 방지하는 특정 목적을 위해 빌드 된 후 특별히 변경되지 않는 시스템이다[7].

EFW(Enhanced Write Filter)는 보호된 파티션의 쓰기 동작을 Overlay 공간으로 전환하여 하나 이상의 파티션의 쓰기 방지를 하는 기능을 유지하며, 물리 디스크의 파티션과 File System 사이에서 동작하면서 쓰기 액세스를 Overlay 공간으로 전환하는 역할을 한다[8]. 또한, 읽기 액세스 시에는 파티션과 Overlay 공간의 내용을 동시에 읽어 들여 사용자에게 실제 볼륨에 쓰인 것처럼 보이게 하는 기능을 한다. FBWF는 EWF의 발전된 형태로, 쓰기 방지 파티션에서 파일 또는 폴더 단위로 쓰기가 가능한 시스템이다.

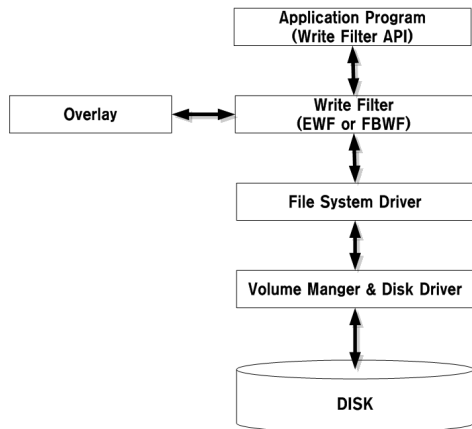


그림 1. Write Filter
Fig. 1 Write Filter

2.2 NFS(Network File System)

로컬 파일시스템처럼 이용할 수 있는 프로토콜로 Sun Microsystems에서 제작한 NFS가 대표적인 예이다 [9]. 네트워크 파일시스템을 이용해서 원격의 파일시스템을 마운트할 경우 상위 계층에서 마운트 지점 아래에 위치한 파일을 시스템 콜을 통해 접근하면 네트워크 파일시스템이 시스템 콜의 요청을 받아서 직접 네트워크로 파일을 수신하여 처리한 후 그 결과를 시스템 콜의 결과로 보낸다. 하지만 NFS의 성능 그리고 관리의 어려움 등의 문제로 NAS(Network Attached Storage) Appliance를 사용하는 경우가 있다. 또한 마운트포인트가 늘어남에 따라 발생하는 성능과 관리상의 어려움 등이 문제점으로 제기 되고 있다. 이에 따라 SAN(Storage Area Network)이나 iSCSI와 같은 다양한 제품들이 개발되고 있으나 이는 시스템의 확장에 따라 매우 높은 비용이 필요하게 된다[10].

2.3 iSCSI

iSCSI(SCSI over IP Networks)는 기존 IP네트워크를 스토리지 네트워크에 통합하고자 하는 목적에 의하여 개발되었으며, 원격지에서 일반 스토리지 I/O를 위해 TCP/IP 기반의 IP네트워크를 통하여 블록 단위의 데이터 전송을 지원하는 표준 SCSI프로토콜이다[11]. iSCSI는 네트워크를 통하여 원격리에서도 스토리지 관리가 가능하며 Host에서 기존의 IP 네트워크를 통해 접근이

가능하므로 시스템의 활용도가 높아 비용을 절감할 수 있다. iSCSI 스토리지를 통한 I/O시에 클라이언트 동작하는 부분인 SCSI Initiator는 캡슐화 하여 원격지에 있는 실제 저장되는 서버의 스토리지를 SCSI Target에 네트워크 장치를 통해 전달한다.

III. 제안된 AWF 시스템 설계

3.1. AWF 메커니즘, 파티션 제어 기술 및 파티션 제어 기술 설계

3.1.1 AWF 메커니즘

AWF 기술은 순간 복구 기술인 Write Filter 기술을 기반으로 사용자 환경과 상황에 맞게 능동적 복구 환경을 제공할 수 있는 기술로 일반적인 사용자는 대부분 사용자의 데이터(문서, 그림, 데이터) 파일을 Primary 드라이브 내에 있는 바탕화면, 내문서 등에 저장한다. 하지만 기존 순간 복구 기술은 Primary 드라이브 영역내의 모든 파일을 복구하기 때문에 Primary 드라이브에 저장한 파일은 사라지게 된다. 따라서 기존 시스템은 사용자는 Extension 드라이브에 직접 접근하여 데이터를 저장하고 불러오는 행위를 해야 하는 문제점이 있었다.

이런 문제점을 해결하기 위하여 본 논문에서는 기존의 정적인 Write Filter의 성능 및 기능을 향상시킬 수 있는 기술로 가변 상황에 맞게 적용할 수 있고 능동적으로 동작할 수 있는 알고리즘 적용하였다. 그림 2는 AWF 메커니즘을 도시한 그림으로 Real Storage 영역을 파티션을 나누고 각각에 운영체제와 Backup Image를 설치한다. Primary 파티션 영역은 AWF를 켜서 동작하며, 가상 저장 공간(Virtual Storage)을 생성하여 관리한다.

또한, 시스템 복구 기술은 실행영역의 드라이브에 Filter를 켜고 가상 저장공간을 만들어서 부팅 후의 모든 행위를 가상 저장 공간에서 실행한다. 재부팅 후 Filter를 제거하고 새로운 Filter를 생성함으로써 아주 짧은 순간에 시스템을 복구할 수 있다. 이 과정에서 사용자에게 의하여 필요하다고 판단되는 행위는 선택적으로 제거되지 않고, 사용할 수 있는 기술을 적용하여, 기존 기술의 단점을 해결하고자 하였다.

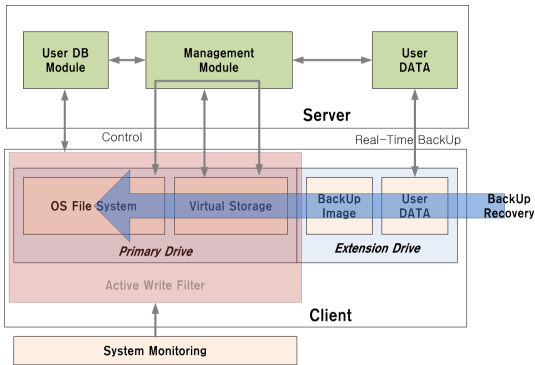


그림 2. Active Write Filter 기술
Fig. 2 Active Write Filter Technology

그림 3은 설계된 AWF의 전반적인 흐름도이다. OS 부팅 과정에서 WF Driver, OS, Active Driver가 로딩된 후 Active Driver는 File, Registry, directory 등의 변경 사항을 후킹 및 모니터링하고, 읽고 쓰기를 제어한다. Active Driver는 백업 및 저장해야할 파일과 재부팅 후 삭제할 파일을 판단하고 제어하는 역할을 수행하며 사용자 파일은 Restore과정(Recovery)을 통하여 저장되고, 웜이나 바이러스, 설치된 프로그램 등은 삭제되어 시스템이 복구된다.

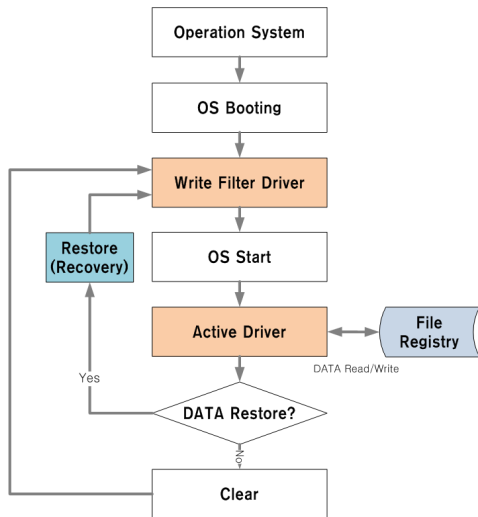


그림 3. AWF의 흐름도
Fig. 3 AWF Write Filter Flowchart

3.1.2. 실시간 네트워크 데이터 백업 기술

실시간 네트워크 데이터 백업 기술은 활성화되어 있는 프로세스에 의해 데이터가 생성 혹은 수정되었을 경우 이를 자동으로 감지하여 서버에 백업을 하는 기술이다. 또한 실시간 네트워크 데이터 백업을 위하여 데이터가 Application에 의해 생성 또는 수정되었는지 판단이 필요하므로 이를 위하여 시스템 모니터링 기술을 활용할 수 있도록 하였으며, 이벤트 검출을 위하여 전단계인 모니터링 드라이버와 드라이버에서 발생하는 이벤트를 비교 분석하는 실행부로 구분하여 설계하였다. 이는 실시간으로 발생한 이벤트의 개수가 엄청나기 때문에 이를 효율적으로 구분하고 정리하는 고속의 로직이 절대적으로 필요하여 표 1의 코드에서는 OS가 디스크 Access에 필요한 이벤트는 부분으로써 이를 통하여 방대한 정보를 효율적으로 걸러낼 수 있도록 하였다.

표 1. 이벤트 검출 코드
Table. 1 Event Identification Code

```

procedure Agent_AFMRename(Sender: TObject; dwOperation: Cardinal;
const szProcess, szFileName, szDestFileName, szUserName: String;
TerminalSessionID: Cardinal; const lpTime: TTimeFields;
ResultCode: Integer);
begin
Add_BackMonitor('Rename', szDestFileName, szProcess);
end;
procedure Agent_AFMWrite(Sender: TObject; dwOperation: Cardinal;
const szProcess, szFileName: String; ResultCode: Integer);
var
FName : string;
begin
if szFileName[Length(szFileName)] <> 'W' then
begin
FName := UpperCase(szProcess);
if (FName = 'SYSTEM') then exit else Add_Monitor('Write', szFileName, szProcess);
if (FName = 'SPOOLSV.EXE') then
begin
if PrintLast = 'Read' then
begin
CopyFile(PrintName, 'c:\spoolw'+IntToStr(PrintPage)+'\SPL');
end;
PrintLast := 'Write';
end;
.
.
.
end;

```

그림 3에서처럼 데이터 저장 이벤트가 발생시 이를 감지하여 사용자의 시스템과 서버에 동시 저장하여 데이터의 유실로 인한 피해를 방지할 수 있도록 하였으며, 수동에 의한 백업 방법도 제공하여 폴더 혹은 파일을 일

괄적으로 백업할 수도 있도록 하였다.

데이터 네트워크 백업과정에서 전수 비교시 시간, 리소스, 트래픽의 낭비가 심해진다. 데이터 백업 기술의 성능 향상을 위하여 MD5 암호화 해시 함수를 이용한 Compare Index Copy 기술을 적용 데이터를 Index화하여 데이터 비교 시간을 단축할 수 있는 알고리즘을 설계하였다. 그림 4는 실시간 네트워크 데이터 백업 기술사용으로 백업을 위한 트래픽이 감소되어 백업 속도 증가, 관리 클라이언트 증가 등의 효과를 기대할 수 있다.

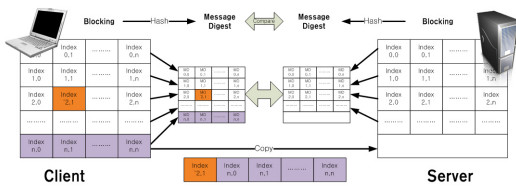


그림 4. 실시간 네트워크 데이터 백업 기술
Fig. 4 Real-time Network Data Backup Technology

표 2는 다음은 클라이언트의 구동부로 백업할 파일을 블록화하여 이를 서버와의 비교작업을 통하여 전송되어야할 블록만을 서버에 보내는 핵심 부분의 코드이다.

표 2. 네트워크 백업 클라이언트 구동 코드
Table. 2 Network Backup Client Drive Code

```

fSrc := FileOpen(fileName, fmOpenRead + fmShareDenyNone);
if fSrc >= 0 then
begin
PBuff := 0;
Index_Table.Last;
while not Index_Table.Bof do
begin
Position := Round(Index_Table.FieldByName('Position').AsFloat);
BSize := Round(Index_Table.FieldByName('Size').AsFloat);
ScanLabel := BytesToFriendlyString(Position)+' / '+BytesToFriendlyString(BSize);
if FileSeek(fSrc, Position, 0) > -1 then
begin
Len := FileRead(fSrc, Buffer^, BSize);
if Len = BSize then
begin
if MD5Print(MD5Pointer(Buffer, Len)) = Index_Table.FieldByName('Data').AsString then
begin
SameSizes := SameSizes+BSize;
end else
.
.
.
end
end
end
end
end

```

3.2. M-iSCSI 기반의 응용 프로그램 모듈화 기술

M-iSCSI(Multiple user iSCSI)기반의 응용 프로그램 모듈화 기술은 서버의 단일 파티션과 유저별로 별도의 임시 파일시스템을 담당하는 파일구조를 가지고 있다. 기존의 NFS가 가지는 동일한 환경을 모든 사용자에게 동일한 형태로 제공하는 부분이 아닌 사용자 개개인의 데이터를 별도의 Thread기술로 control하여 사용자 데이터가 동일한 부분은 서버의 단일 기록장치로부터 참조를 하고 사용자 데이터는 각각의 Thread형 파일시스템에서 운영됨으로써 디스크 자원의 절약과 유지보수의 편리성을 제공한다. 이는 응용 프로그램을 서버기반으로 설치하고 클라이언트 단에서는 독자적인 NFS로 활용함으로써 편리성과 보안성을 확보할 수 있으며 그림 5와 같은 구조로 구성된다. 서버에는 각 클라이언트별 Thread형 파일시스템인 Temp Module이 iSCSI Target를 가지는 파일로 생성되고 가상 모듈을 통하여 클라이언트는 iSCSI Initiator에 의하여 Read/Write가 가능하며 재부팅 후 모듈의 재 할당으로 실 데이터의 변화는 발생하지 않는다.

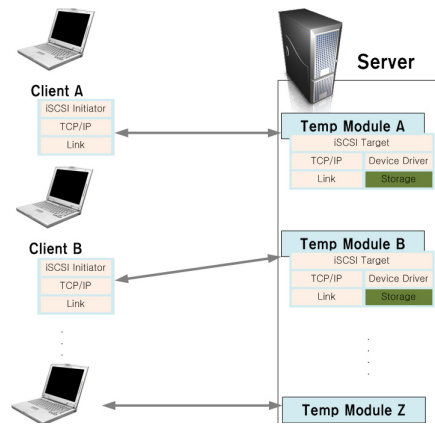


그림 5. M-iSCSI 구조
Fig. 5 M-iSCSI Structure

본 논문에서는 기존의 iSCSI를 이용하는 Single User 용 File System을 Multi User용으로 설계하여, 원본의 파일 시스템과 유저별 가상 파일 시스템을 자동으로 연결하는 Disk Access의 수행과정을 수행하는 Host는 이를 이용하여 응용 프로그램을 자동으로 등록 사용하기 위한 모듈 생성 및 모듈 실행부로 구분하였다.

3.3 제안된 AWF 시스템 설계

Active Write Filter(AWF) 메커니즘과 Multi user iSCSI(M-iSCSI) 및 실시간 모니터링 기술을 이용하여 시스템 복구, OS 복원, 네트워크 환경에서 실시간 데이터 백업, 응용 소프트웨어 관리를 할 수 있는 시스템을 설계하였다. 개방형 네트워크 환경에 정상적인 작업환경을 위협하는 시스템 해킹, 웜/바이러스, 프로그램 오류, 시스템 변경, 내부자 보안, 불법 소프트웨어, 시스템 오작동 등 위협요소를 원천적으로 차단하고, 컴퓨터 시스템을 관리, 유지, 보수를 위한 시스템 설계를 목표로 하여 그림 6과 같이 시스템을 구성하였다.

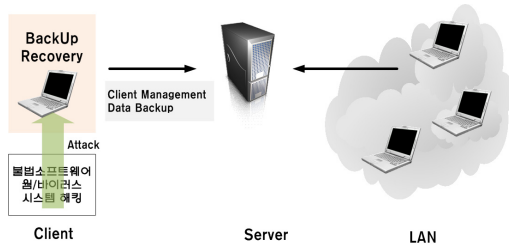


그림 6. 제안된 시스템의 개념도
Fig. 6 Proposal System Schematic Diagram

본 논문에서 제안 하는 핵심 기술은 크게 AWF 메커니즘, 파티션 제어기술, 실시간 네트워크 데이터 백업 기술, M-iSCSI 기반의 응용프로그램 모듈화 기술로 나눌 수 있다. 시스템 구성은 서버와 클라이언트 구조로 나뉘며, 클라이언트는 보호를 위한 개체이고, 서버는 관리와 응용프로그램 모듈, 사용자 데이터 백업을 위한 개체이다. 클라이언트에는 AWF 메커니즘, 파티션 제어기술을 적용하고 서버에는 클라이언트 관리를 위한 User DB Module, Management Module과 M-iSCSI 기반 응용 프로그램 모듈화 기술, 실시간 네트워크 데이터 백업 기술이 적용하였다

IV. 구현 및 비교 분석

4.1 제안된 시스템의 구현

4.1.1 서버

서버는 클라이언트 관리, 데이터 백업, 응용프로그램 지원, 가상화 드라이브 지원 등의 기능을 수행한다.

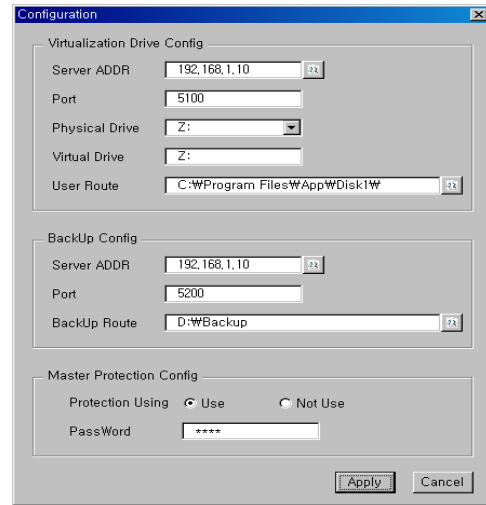


그림 7. 서버 환경설정
Fig. 7 Setting Environmental Server

다음은 서버의 환경 설정의 각 항목을 설명한 것이다.

- ▷ **Virtual** 드라이브 설정: 프로그램 모듈을 사용하기 위한 항목을 설정한다.
- ▷ **BackUp** 설정: 네트워크 백업을 사용하기 위한 항목을 설정한다.
- ▷ **Protection** 설정: 사용자 하여금 개별적으로 보안 기능을 할 수 없도록 설정한다.

그림 8은 사용자를 설정하고, 클라이언트 프로그램이 설치된 PC를 확인할 수 있는 사용자 설정 화면이다. 클라이언트 프로그램을 설치하면 해당 PC의 정보가 자동으로 사용자 정보에 등록되면서 사용자 설정 화면에서 확인할 수 있다.

생성 일자	컴퓨터명	작업 그룹	로그인	IP 주소	설치 OS
2008-09-19 11:30:42	홍보부1	WORK-GROUP	USER	192.168.1.105	Windows XP Home Edition
2008-09-19 12:41:49	홍보부2	WORK-GROUP	USER	192.168.1.141	Windows XP Home Edition
2008-09-19 09:30:49	홍보부3	WORK-GROUP	USER	192.168.1.120	Windows XP Home Edition
2008-09-19 10:41:40	홍보부4	WORK-GROUP	USER	192.168.1.194	Windows XP Home Edition
2008-09-25 10:20:04	차발업1	WORK-GROUP	USER	192.168.1.105	Windows XP Home Edition
2008-09-12 13:54:59	차발업2	WORK-GROUP	USER	192.168.1.101	Windows XP Professional
2008-09-02 21:20:13	차발업3	WORK-GROUP	USER	192.168.1.194	Windows XP Home Edition
2008-09-03 18:36:44	차발업4	WORK-GROUP	USER	192.168.1.194	Windows XP Home Edition
2008-09-03 10:00:34	차발업5	WORK-GROUP	USER	192.168.1.194	Windows XP Professional
2008-09-08 11:22:53	홍보부1	WORK-GROUP	USER	192.168.1.167	Windows XP Professional
2008-09-08 11:26:39	홍보부2	WORK-GROUP	USER	192.168.1.167	Windows XP Professional
2008-09-17 15:40:39	홍보부3	WORK-GROUP	USER	192.168.1.162	Windows XP Professional

그림 8. 서버의 클라이언트 설정
Fig. 8 Client Setting of Server

그림 9는 후킹 예외 프로세스 데이터 관리를 위한 화면으로, 서버 프로그램에서 등록된 프로그램 모듈을 클라이언트 프로그램을 통해 해당 응용 프로그램을 실행할 때, 또는 서버 프로그램의 사용자 데이터 관리에서 등록된 데이터가 클라이언트 프로그램이 설치된 클라이언트에서 적용될 때 데이터 후킹 기술을 사용하여 임의의 위치에 데이터를 저장한다.

또한, 후킹 예외 프로세스 데이터 관리에 실행 파일명 혹은 실행 경로를 등록해 두면 해당 파일명 혹은 경로에서 실행된 데이터는 예외 처리되어 저장되지 않도록 되어 있다.

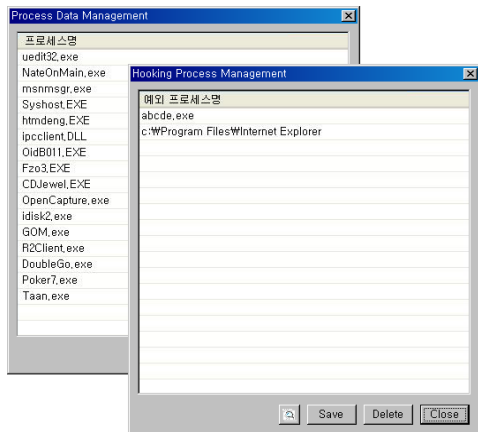


그림 9. 프로세스 데이터 관리
Fig. 9 Process Data Management

4.1.2 클라이언트

클라이언트는 시스템 복구 기능, 드라이브 제어 기능, 후킹에 의한 시스템 모니터링 기술, 웹/바이러스 차단 기능, 응용프로그램 모듈 사용 기능 등을 구현하였다.

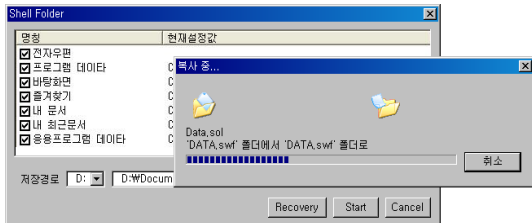


그림 10. 사용자 데이터 동기화
Fig. 10 User Data Synchronization

그림 10은 파티션 제어 기술을 이용하여 Primary 드라이브에 있는 사용자 데이터를 Extension 드라이브와 동기화가 이루어진다.

다음 그림 11은 클라이언트 환경 설정을 위한 화면으로 기본 설정, 백업 설정으로 구성되어 있다.

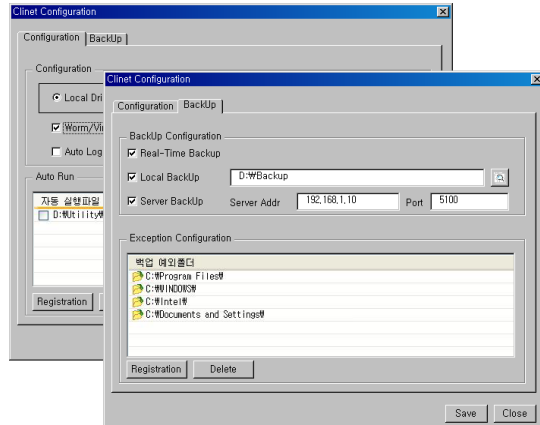


그림 11. 클라이언트 환경설정
Fig. 11 Setting Environmental Client

기본 설정은 외부 장치 사용 설정은 클라이언트 프로그램이 설치된 클라이언트는 프로그램 모듈을 사용하기 위해 로컬 디스크에 프로그램 모듈을 저장하여 사용할 수 있으며, 한번 실행된 응용 프로그램은 그 실행 정보를 로컬 디스크에 백업해 두었다가 다음 실행시에 백업된 정보를 이용하여 응용 프로그램의 실행 속도를 향상시킬 수 있다. 자동 실행은 클라이언트 프로그램이 실행될 때 자동으로 등록된 프로그램을 실행할 수 있도록 하였다. 백업 설정은 자동 실시간 백업 및 예외 설정에서 특정 폴더에 있는 사용자가 필요하지 않는 파일을 예외로 설정 가능하다.

4.2 기존시스템의 비교 분석

4.2.1 AWF

기존의 정적인 Write Filter 기술을 상황에 맞게 적용할 수 있는 능동적으로 동작할 수 있는 알고리즘을 설계하여 실행 영역의 드라이브에 Filter를 씌우고 가상 저장 공간을 만들어서 부팅 후의 모든 행위를 가상 저장 공간에서 수행되며, 재 부팅 후 Filter를 제거하고 새로운 Filter를 생성함으로써 짧은 순간에 시스템을 복구할 수 있다.

또한, 응용 프로그램 설치 후, 사용자 환경 설정 값 등 정당한 레지스트리 변경 및 파일 변경을 모니터링하고, 재부팅 후 이러한 변경된 값을 다시 roading해 줄 수 있는 능동적인 복구가 가능하다.

4.2.2 M-iSCSI 기반의 응용 프로그램 모듈화

서버의 단일 파티션과 클라이언트별 임시 파일시스템을 담당하는 파일구조를 가지고 있으며, NFS가 가지는 환경의 사용자에게 동일한 형태로 제공하는 부분이 아닌 각각의 데이터를 별도의 Thread기법을 사용하여 제어하며 사용자별 데이터가 별도로도 존재한다. 또한, 동일한 부분은 서버의 단일 기록장치로부터 참조를 하고 클라이언트 데이터는 각각의 Thread형 파일시스템에서 운영됨으로써 디스크 자원의 절약과 유지보수의 편리성 제공 가능하다. 이를 이용하여 응용 프로그램을 서버기반으로 설치하고 클라이언트에서는 독자적인 NFS로 활용함으로써 편리성과 보안성을 확보할 수 있다.

표 3. 기존 시스템 비교 분석
Table. 3 Existing System Comparative Analysis

구 분	마이크로소프트 로오피스	DDRS	LANDesk Application Virtualization	제안된 시스템
복구 속도	○	△	×	○
다중시스템복원	×	○	×	×
데이터보존	△	△	×	○
NFS	×	×	×	○
확장성	△	△	△	○
실시간 백업	○	○	×	○
수동 백업	○	○	×	○
데이터 2중화	×	×	×	○

표 3은 제안하는 시스템에서 제공하는 기능들이 기존의 시스템과 비교 한 것이다. 일반적인 시스템은 운영체제의 모든 사항을 복구함으로 사용자 데이터 등의 보전 문제점을 가지고 있으나 제안하는 시스템에서는 AWF 메커니즘을 사용함으로써 이 문제를 해결하였다. 또한 기존의 NFS는 개별적으로 사용자에게 제공되는 공간이지만 이를 다중 사용자에게 하나의 스토리지를 제공하는 메커니즘으로 Virtual Application 기술을 개발하여 향후 다른 시스템에 적용 가능할 것이다.

V. 결론 및 향후 연구 방향

본 논문은 AWF, 파티션 제어 기술, 실시간 네트워크 데이터 백업 기술, 시스템 모니터링 기술 및 응용프로그램 모듈화 기술을 설계하였다. 이로서 기업에서 안정적인 컴퓨터 사용 환경을 제공하여 업무 효율 개선, 컴퓨터 시스템 복구비용과 시간 절감, 안정적인 데이터 백업을 통하여 근무자의 능력 향상의 효과를 기대할 수 있고, 나아가 기업의 생산성 향상과 이윤 증대를 기대할 수 있다.

또한, 컴퓨터 관리 효율도 높일 수 있으며 다양한 사용자가 사용하는 컴퓨터를 관리하기 위하여 많은 애로 사항이 있는 것이 현실이다. 학생들의 불법 소프트웨어, 게임, ActiveX, 애드웨어, 웹/바이러스 등의 문제점이 더욱더 많다. 이러한 문제점을 원천적으로 해결할 수 있는 기술로 불법 소프트웨어 설치 차단, 악성코드로부터 보호, 사용자의 실수로 인한 시스템 보호 등을 제공할 수 있다. 즉, 효율적인 교육환경 제공과 컴퓨터 관리를 위한 인력과 시간 낭비를 줄일 수 있다.

또한, 최근 자산관리 소프트웨어는 공공기관 또는 대기업 등을 중심으로 보편화되어가는 추세이지만 아직까지도 이를 완벽히 관리할 수 있는 제품은 존재하지 않는 상황이며 본 기술과 자산관리를 연동하여 개발할 경우 이러한 문제점들을 완벽히 제공할 수 있는 시스템의 기본 모델로 활용 가능하다.

AWF 기술을 기반으로 단일 복구, 내부자 부정 방지 등의 시스템 향상 및 실시간 네트워크 데이터 백업 기술을 이용하여 백업 서버 동기화가 가능하고, M-iSCSI 및 응용 프로그램 모듈화 기술을 응용하여 서버와 터미널을 이용한 응용 솔루션 활용 가능하다. 나아가 개발 기술을 응용하여 서버용 복구 솔루션, 개인 관리 솔루션을 개발 등 다양한 솔루션으로 응용 가능하다.

참고문헌

- [1] Thomas M.Ruwart, "OSD: A tutorial on Object Storage Devices." Proceedings of the 19th IEEE/10th NASA Goddard Conference on Mass Storage Systems and Technologies. 2002.

- [2] Steve Kleiman, Devang Shah, Bart Smaalders, :
"Programming with Threads", SunSoft Press, A
Prentice Hall Title, 1998.
- [3] T. Westmann, D. Kossmann, S. Helmer, and G.
Moerkotte : "The Implementation of Compressed
Database", SIGMOD Record 29(3), 2000.
- [4] Barillaud, F. Deril, L., M. : Network Management
Using Internet Technologies. Proc. IEEE/IFIP
International Symp. On Integrated Network
Management, San Diego. CA, USA. 1997
- [5] Pell, H.A., Mellquist, P. E.: Web Based System and
Network Management. Internet Draft, Hewlett
Packard. 1996
- [6] Case, j. : Management Information Base for Version 2
of the Simple Network Management Protocol. IETF,
RFC p1907. 1996
- [7] [http://msnd.microsoft.com/en-us/library/ms91-2906.
aspx](http://msnd.microsoft.com/en-us/library/ms91-2906.aspx)
- [8] [http://msnd.microsoft.com/en-us/library/aa940-926
\(Winembedded.5\).aspx](http://msnd.microsoft.com/en-us/library/aa940-926(Winembedded.5).aspx)
- [9] B. Pawlowski, C. Juszczak, P. Staubach, C. Smith, D.
Lebel, and D. Hitz. "NFS Version 3 Design and
Implementation". In Proceedings of the Summer 1994
USENIX Technical Conference, Jun 1994.
- [10] J. Satran and K. Meth, "Internet Small Computer
Systems Interface(iSCSI)", IBM, April 2004
- [11] J. Hufferd, iSCSI: The Universal Storage Connection.
Addison-Wesley, Boston, 2003.



한승조(Seung-jo Han)

1980년 조선대학교 전자공학과
(공학사)
1982년 조선대학교 전자공학과
(공학석사)

1994년 충북대학교 전자계산학과(공학박사)
1986년 6월~1987년 3월 뉴올리언즈대학 객원교수
1995년 2월~1996년 1월 텍사스대학 객원교수
2000년 12월~2002년 3월 버클리대학 객원교수
1998년~현재 조선대학교 정보통신공학과 교수
※관심분야: 통신보안시스템설계, S/W 불법복제방지
시스템, ASIC 설계

저자소개



조경옥(Kyoung-ok Cho)

2003년 광주대학교 컴퓨터전자
통신공학부(공학사)
2005년 조선대학교
정보통신공학과(공학석사)

2007년~현재 : 조선대학교 정보통신공학과 박사과정
※관심분야: DRM, 정보보안, 모바일, 컴퓨터
네트워킹, 불법복제방지시스템