(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년03월20일
(11) 등록번호 10-2091787
(24) 등록일자 2020년03월16일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01)
(52) CPC특허분류
G06F 21/56 (2013.01)
(21) 출원번호 10-2018-0061144
(22) 출원일자 2018년05월29일
심사청구일자 2018년05월29일
(65) 공개번호 10-2019-0135752
(43) 공개일자 2019년12월09일
(56) 선행기술조사문헌
김형규외 4인, '$UsnJrnl 기반 랜섬웨어 암호화 패턴 유형화 및 탐지모델', 디지털 포렌식 연구 11(3) pp.71-80, 2017.12.*
이규빈외 2인, '랜섬웨어 동적 분석을 위한 시그니처 추출 및 선정 방법', 정보과학회 컴퓨팅의 실제 논문지 24(2) pp.99-104, 2018.02*
KR1020180001896 A*
KR1020170088160 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단

(72) 발명자
이희조
배정한
이충인

(74) 대리인
특허법인엠에이피에스

전체 청구항 수 : 총 8 항 심사관 : 윤혜숙

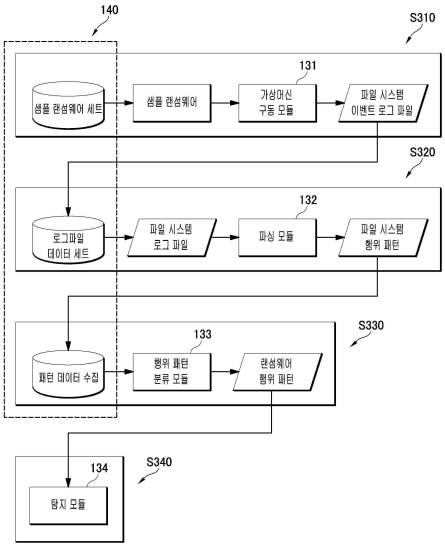
(54) 발명의 명칭 **파일 시스템에서의 랜섬웨어 탐지 방법 및 그 장치**

(57) 요 약

본 발명의 일 실시예에 따른 파일시스템에서의 랜섬웨어 탐지 방법은, 파일시스템 내 파일의 이벤트 발생에 따른 로그 파일이 기록되는 기록모듈을 이용하여 파일의 랜섬웨어를 탐지하는 랜섬웨어 탐지장치에 의해 수행되는 파일시스템에서의 랜섬웨어 탐지 방법에 있어서, 가상환경에서 샘플 랜섬웨어를 실행하고, 상기 샘플 랜섬웨어에

(뒷면에 계속)

대 표 도 - 도2



의한 파일시스템 행위를 기 설정된 행위 모델링 코드에 따라 로그 파일로 상기 기록모듈에 저장하는 샘플 랜섬웨어 실행 단계; 상기 기록 모듈에서 로그 파일을 파싱하여 각 파일에서 발생된 행위들에 대해 파일 변경 기록 분석을 수행하여 연속된 행위 모델링 코드로 이루어진 코드열로 변환하는 기록 분석 단계; 기 설정된 랜섬웨어 행위 규칙에 기초하여 상기 변환된 코드열을 분석하여 정상 프로그램과 분류되는 랜섬웨어 행위 패턴을 수집하는 패턴 분류 단계; 및 상기 랜섬웨어 행위 패턴을 이용하여 실제 환경에서 랜섬웨어를 탐지하는 탐지 단계를 포함할 수 있다.

이 발명을 지원한 국가연구개발사업

과제고유번호	20150005650031001
부처명	과학기술정보통신부
연구관리전문기관	정보통신기술진흥센터
연구사업명	정보보호핵심원천기술개발사업
연구과제명	IoT 소프트웨어 보안 취약점 자동 분석 기술 개발
기 여 율	1/1
주관기관	고려대학교 산학협력단
연구기간	2017.06.01 ~ 2018.05.31

명 세 서

청구범위

청구항 1

파일시스템 내 파일의 이벤트 발생에 따른 로그 파일이 기록되는 기록모듈을 이용하여 파일의 랜섬웨어를 탐지하는 랜섬웨어 탐지장치에 의해 수행되는 파일시스템에서의 랜섬웨어 탐지 방법에 있어서,

가상환경에서 샘플 랜섬웨어를 실행하고, 상기 샘플 랜섬웨어에 의한 파일시스템 행위를 기 설정된 행위 모델링 코드에 따라 로그 파일로 상기 기록모듈에 저장하는 샘플 랜섬웨어 실행 단계;

상기 기록 모듈에서 로그 파일을 파싱하여 각 파일에서 발생된 행위들에 대해 파일 변경 기록 분석을 수행하여 연속된 행위 모델링 코드로 이루어진 코드열로 변환하는 기록 분석 단계;

기 설정된 랜섬웨어 행위 규칙에 기초하여 상기 변환된 코드열을 분석하여 정상 프로그램과 분류되는 랜섬웨어 행위 패턴을 수집하는 패턴 분류 단계; 및

상기 랜섬웨어 행위 패턴을 이용하여 실제 환경에서 랜섬웨어를 탐지하는 탐지 단계를 포함하되,

상기 패턴 분류 단계는,

상기 코드열에서 상기 랜섬웨어 행위 규칙에 기초하여 각 파일에 대한 행위 패턴 그룹을 추출하고, 상기 행위 패턴 그룹에서 복수의 행위로 이루어진 행위 패턴을 분류한 후 행위별 빈도수, 행위 패턴별 빈도수를 체크하는 단계;

랜섬웨어에 감염되지 않은 정상 프로그램에서 나타나는 행위별 빈도수와 또는 행위 패턴별 빈도수가 기 설정된 횟수 이상 나타나는 행위 패턴을 분류하는 단계; 및

상기 행위 패턴 그룹에서 기 설정된 횟수 이상 나타나는 행위별 빈도수 또는 행위 패턴별 빈도수를 상기 정상 프로그램에서 나타나는 행위별 빈도수 또는 행위 패턴별 빈도수와 비교하고, 두 빈도수의 차이값에 따라 행위 또는 행위 패턴 별로 가중치를 부여하여 랜섬웨어 행위 패턴을 산출하는 단계를 포함하는 것인, 파일 시스템에서의 랜섬웨어 탐지 방법.

청구항 2

제 1 항에 있어서,

상기 행위 모델링 코드는,

파일 생성(Create, C), 파일 삭제(Delete, D), 파일명 변경을 포함한 파일 이동(Move, M) 및 파일 갱신(Update, U)으로 분류 및 정의하는 것인, 파일 시스템에서의 랜섬웨어 탐지 방법.

청구항 3

제 2 항에 있어서,

상기 랜섬웨어 행위 규칙은,

모든 파일의 변경 행위가 단일 파일에 대한 행위로 정의되는 제1 규칙,

상기 파일 생성(C)과 파일 삭제(D)는 하나의 쌍으로 존재하는 행위로 정의되는 제2 규칙,

상기 파일 생성(C)이 존재하지 않으면 상기 파일 이동(M) 및 파일 갱신(U)은 파일 삭제(D)에 후속되는 행위로 출현되지 않는다고 정의되는 제3 규칙,

상기 파일 갱신(U)이 행위 패턴의 선두부에 존재하는 경우에 무시하도록 정의되는 제4 규칙 및

기 설정된 개수 이상의 행위 패턴 그룹에 대해 복수의 행위로 이루어진 행위 패턴의 반복으로 나타내도록 정의되는 제5 규칙을 포함하는 것인, 파일 시스템에서의 랜섬웨어 탐지 방법.

청구항 4

제 3 항에 있어서,

상기 패턴 분류 단계는,

상기 랜섬웨어 행위 규칙을 적용하여 CDM, CDU, CMD, CUD, DCM, DCU, MMM 및 MUM의 행위 패턴을 랜섬웨어 행위 패턴으로 분류하는 것인, 파일 시스템에서의 랜섬웨어 탐지 방법.

청구항 5

삭제

청구항 6

제 1 항에 있어서,

상기 샘플 랜섬웨어 실행시 행위패턴그룹에서 발생된 행위 패턴별 빈도수가 랜섬웨어에 감염되지 않은 정상 프로그램에서 나타나는 행위 패턴별 빈도수와 차이가 클수록 가중치를 높게 설정하는 것인, 파일 시스템에서의 랜섬웨어 탐지 방법.

청구항 7

제 1 항에 있어서,

상기 탐지 단계는,

상기 파일 시스템 행위가 기 설정된 발생개수가 될 때마다 각 파일 별로 행위 패턴 그룹을 분석하여 상기 랜섬웨어 행위 패턴과 일치하는 행위 패턴이 존재하는 지를 판단하는 단계;

상기 랜섬웨어 행위 패턴과 일치하는 행위 패턴이 존재하는 경우, 해당 행위 패턴에 부여된 가중치를 기 설정된 기준값에 합산하여 탐지수치를 증가시키는 단계; 및

상기 탐지 수치가 기설정된 임계수치 이상인 경우, 상기 행위 패턴을 랜섬웨어 행위 패턴으로 판단하여 랜섬웨어 탐지를 수행하는 단계를 포함하는 것인, 파일 시스템에서의 랜섬웨어 탐지 방법.

청구항 8

파일시스템 내 파일의 이벤트 발생에 따른 로그 파일이 기록되는 기록모듈을 이용하여 파일의 랜섬웨어를 탐지하는 파일 시스템에서의 랜섬웨어 탐지장치에 있어서,

파일 시스템에서의 랜섬웨어 탐지 방법을 수행하기 위한 프로그램이 기록된 메모리; 및

상기 프로그램을 실행하기 위한 프로세서를 포함하며,

상기 프로세서는, 상기 프로그램의 실행에 의해,

가상환경에서 샘플 랜섬웨어를 실행하여 파일시스템 행위를 기 설정된 행위 모델링 코드에 따라 로그 파일로 상기 기록모듈에 저장하고, 상기 기록 모듈에서 로그 파일을 파싱하여 각 파일에서 발생된 행위들에 대해 파일 변경 기록 분석을 수행하여 연속된 행위 모델링 코드로 이루어진 코드열로 변환한 후 기 설정된 랜섬웨어 행위 규칙에 기초하여 상기 변환된 코드열을 분석하여 정상 프로그램과 분류되는 랜섬웨어 행위 패턴을 수집하며, 상기 수집된 랜섬웨어 행위 패턴을 이용하여 실제 환경에서 랜섬웨어를 탐지하되,

상기 코드열에서 상기 랜섬웨어 행위 규칙에 기초하여 각 파일에 대한 행위 패턴 그룹을 추출하고, 상기 행위 패턴 그룹에서 복수의 행위로 이루어진 행위 패턴을 분류한 후 행위별 빈도수, 행위 패턴별 빈도수를 체크하고, 랜섬웨어에 감염되지 않은 정상 프로그램에서 나타나는 행위별 빈도수와 또는 행위 패턴별 빈도수가 기 설정된 횟수 이상 나타나는 행위 패턴을 분류하며, 상기 행위 패턴 그룹에서 기 설정된 횟수 이상 나타나는 행위별 빈도수 또는 행위 패턴별 빈도수를 상기 정상 프로그램에서 나타나는 행위별 빈도수 또는 행위 패턴별 빈도수와 비교하고, 두 빈도수의 차이값에 따라 행위 또는 행위 패턴 별로 가중치를 부여하여 랜섬웨어 행위 패턴을 산출하는 것인, 파일 시스템에서의 랜섬웨어 탐지 장치.

청구항 9

제 8 항에 있어서,

상기 프로그램은,

상기 샘플 랜섬웨어를 실행하기 위한 가상 환경을 구현하는 가상머신 구동 모듈;

상기 기록모듈에서 파일시스템의 로그파일을 파싱하는 파싱 모듈;

파일시스템 행위에 대한 파일 변경 기록 분석을 통해 각 파일에 대한 행위 패턴 그룹을 추출하고, 상기 행위 패턴 그룹에서 복수의 행위로 이루어진 행위 패턴을 분류한 후 상기 랜섬웨어 행위 규칙에 기초하여 상기 랜섬웨어 행위 패턴을 수집하는 행위 패턴 분류 모듈; 및

상기 랜섬웨어 행위 패턴을 이용하여 랜섬웨어 탐지를 수행하는 탐지 모듈을 포함하는 것인, 파일 시스템에서의 랜섬웨어 탐지 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 컴퓨터 사용 환경에서 랜섬웨어에 대한 탐지를 수행하여 파일시스템 내의 파일들이 암호화되는 위협으로부터 파일들을 보호하기 위한 파일시스템에서의 랜섬웨어 탐지 방법 및 그 장치에 관한 것이다.

배 경 기 술

[0002] 랜섬웨어는 사용자의 컴퓨터에 접근하여 사용자가 보유한 사진, 문서, 음악 및 영상 그리고 컴퓨터 데이터베이스 등을 암호화 하여 비트코인을 요구하는 악성코드로써 2016년 기준 13만 명의 피해자와 피해액이 3000억원 이상인 것으로 추정된다.

[0003] 초기의 랜섬웨어는 윈도우 운영체제를 중심으로 배포되었으나 오늘날 랜섬웨어는 리눅스 웹서버 및 안드로이드 모바일 기기의 데이터까지 감염할 수 있다. 특히 최근 등장한 랜섬웨어는 개인의 민감한 정보를 암호화 시킨 후 주소록상의 지인에게 배포하겠다는 협박을 통해 비용을 지불하도록 유도하고 있다. 이러한 랜섬웨어들은 비트코인이 가진 추적 불가한 은닉성과 익명성, 환전의 신속성, 변종 개발의 용이성에 유혹 당한 공격자들에 의해 지금 현재도 계속 진화 중에 있다.

[0004] 랜섬웨어는 기본적으로 데이터를 암호화 하는 Encryption Ransomware, 사용자 화면을 장악하는 Lock Screen Ransomware, 부트영역을 훼손하는 Master Boot Record (MBR) Ransomware, 안드로이드 기기를 대상으로 하는 Mobile device ransomware (Android)로 크게 나눌 수 있으며, 2017년 국내에 보고된 랜섬웨어는 275종에 이른다.

[0005] 이러한 랜섬웨어는 2013년 Locky, Cryptolocker 랜섬웨어의 등장을 시작으로 최근까지도 전 세계 컴퓨터 사용자들을 위협하고 있다. 따라서, 랜섬웨어를 탐지하고 예방할 수 있는 기술은 컴퓨터 보안에 있어 없어서는 안되는 중요한 요소 중의 하나로 자리매김하고 있다.

[0006] 랜섬웨어 탐지 기술과 관련된 연구는 전 세계적으로 활발하게 이루어지고 있으며, 크게 랜섬웨어의 정적 분석 탐지 기법과 동적 분석 탐지 기법으로 분류할 수 있다.

[0007] 랜섬웨어의 정적 분석 탐지 기법은 이미 랜섬웨어로 분류된 악성 소프트웨어의 소스 코드 및 시그니처를 이용하여 탐지를 수행하는 방법으로서, 향후 이와 유사한 랜섬웨어가 동작하는 경우 쉽고 빠르게 찾아낼 수 있는 장점이 있다. 그러나, 랜섬웨어의 정적 분석 탐지 기법은 이미 알려진 랜섬웨어의 경우에 탐지가 가능하며, 신종/변종 랜섬웨어의 경우에 탐지가 힘들다는 한계점이 있다.

[0008] 랜섬웨어의 동적 분석 탐지 기법은 랜섬웨어의 행위 패턴 분석에 기반하여 랜섬웨어가 동작할 때 나타나는 특징들을 분석하고, 이를 이용하여 탐지하는 방법으로서, 랜섬웨어의 공통된 행위들을 타겟으로 하기 때문에 신종/변종 랜섬웨어의 출현 시에 탐지가 가능하다는 장점이 있다. 그러나, 랜섬웨어의 동적 분석 탐지 기법은 패턴 모니터링에 소비되는 리소스가 정적 분석 탐지 기법에 비해 커서 컴퓨팅 파워가 작은 단말에서는 해당 기법을 적용하기 힘들고, 분석된 행위 패턴을 우회할 수 있는 랜섬웨어가 출현할 경우에 미탐지 발생 가능성이 있다는 문제점이 있다.

[0009] 이와 같이, 랜섬웨어로 감염으로 인한 피해를 예방하기 위해 다양한 랜섬웨어 탐지 솔루션이 등장하고 있다. 그러나, 종래의 랜섬웨어 탐지 기법들은 기법의 특성에 맞는 상황에서는 유용하게 될 수 있지만, 일부 상황에서는 신종 랜섬웨어 혹은 변종 랜섬웨어를 탐지하는데 한계점이 있다. 이는 랜섬웨어 공격자들에게 악용되어 새로운 공격 기법을 제시하게 하고, 새로운 위협이 가해지게 되므로 이를 방어하기 위한 새로운 방어기법이 필요하다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) 대한민국등록특허 제10-1817636호 " 랜섬웨어 검출 장치 및 방법 "

(특허문헌 0002) 대한민국등록특허 제10-1685014호 " 컴퓨터 시스템의 랜섬웨어 행위에 대한 선제적인 탐지 차단 방법 및 그 장치 "

발명의 내용

해결하려는 과제

[0011] 본 발명은 전술한 문제점을 해결하기 위하여, 본 발명의 일 실시예에 따라 컴퓨팅 환경 및 컴퓨터 관련 기기 사용 환경에서 파일시스템 내 파일 변경 기록에 대한 분석을 통해 랜섬웨어 행위를 탐지하는 데에 목적이 있다.

[0012] 다만, 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

과제의 해결 수단

[0013] 상기한 기술적 과제를 달성하기 위한 기술적 수단으로서 본 발명의 일 실시예에 따른 파일시스템에서의 랜섬웨어 탐지 방법은, 파일시스템 내 파일의 이벤트 발생에 따른 로그 파일이 기록되는 기록모듈을 이용하여 파일의 랜섬웨어를 탐지하는 랜섬웨어 탐지장치에 의해 수행되는 파일시스템에서의 랜섬웨어 탐지 방법에 있어서, 가상환경에서 샘플 랜섬웨어를 실행하고, 상기 샘플 랜섬웨어에 의한 파일시스템 행위를 기 설정된 행위 모델링 코드에 따라 로그 파일로 상기 기록모듈에 저장하는 샘플 랜섬웨어 실행 단계; 상기 기록 모듈에서 로그 파일을 파싱하여 각 파일에서 발생된 행위들에 대해 파일 변경 기록 분석을 수행하여 연속된 행위 모델링 코드로 이루어진 코드열로 변환하는 기록 분석 단계; 기 설정된 랜섬웨어 행위 규칙에 기초하여 상기 변환된 코드열을 분석하여 정상 프로그램과 분류되는 랜섬웨어 행위 패턴을 수집하는 패턴 분류 단계; 및 상기 랜섬웨어 행위 패턴을 이용하여 실제 환경에서 랜섬웨어를 탐지하는 탐지 단계를 포함하는 것이다.

[0014] 또한, 본 발명의 다른 일 실시예에 따른 파일 시스템에서의 랜섬웨어 탐지장치는, 파일시스템 내 파일의 이벤트 발생에 따른 로그 파일이 기록되는 기록모듈을 이용하여 파일의 랜섬웨어를 탐지하는 파일 시스템에서의 랜섬웨어 탐지장치에 있어서, 파일 시스템에서의 랜섬웨어 탐지 방법을 수행하기 위한 프로그램이 기록된 메모리; 및 상기 프로그램을 실행하기 위한 프로세서를 포함하며, 상기 프로세서는, 상기 프로그램의 실행에 의해, 가상환경에서 샘플 랜섬웨어를 실행하여 파일시스템 행위를 기 설정된 행위 모델링 코드에 따라 로그 파일로 상기 기록모듈에 저장하고, 상기 기록 모듈에서 로그 파일을 파싱하여 각 파일에서 발생된 행위들에 대해 파일 변경 기록 분석을 수행하여 연속된 행위 모델링 코드로 이루어진 코드열로 변환한 후 기 설정된 랜섬웨어 행위 규칙에 기초하여 상기 변환된 코드열을 분석하여 정상 프로그램과 분류되는 랜섬웨어 행위 패턴을 수집하며, 상기 수집된 랜섬웨어 행위 패턴을 이용하여 실제 환경에서 랜섬웨어를 탐지하는 것이다.

발명의 효과

[0015] 전술한 본 발명의 과제 해결 수단에 의하면, 기존의 랜섬웨어의 행위 패턴 분석에 기반의 랜섬웨어 탐지 방법에 비해 패턴 모니터링에 소비되는 리소스 사용이 적고, 랜섬웨어가 우회할 수 없는 행위들에 대한 패턴화를 진행하여 랜섬웨어 탐지를 수행함으로써 미탐지 발생 가능성을 최소화할 수 있으며, 신종/변종 랜섬웨어에 대한 탐지도 가능하다는 효과가 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 일 실시예에 따른 파일 시스템에서의 랜섬웨어 탐지 장치의 구성을 나타낸 도면이다.

도 2는 도 1의 구성요소인 프로세서의 랜섬웨어 탐지 방법에 대한 수행 과정을 설명하는 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 파일시스템에서의 랜섬웨어 탐지 방법을 설명하는 순서도이다.

도 4는 본 발명의 일 실시예에 따른 파일 시스템에서의 랜섬웨어 탐지 방법의 탐지 단계를 설명하기 위한 도면이다.

도 5는 일반적인 랜섬웨어의 파일 암호화를 위한 행위 패턴을 설명하는 예시도이다.

도 6은 본 발명의 일 실시예에 따른 랜섬웨어 행위 규칙을 통해 추출된 행위 패턴 리스트를 설명하는 도면이다.

도 7은 본 발명의 일 실시예에 따른 랜섬웨어 행위 규칙을 통해 행위 패턴이 형성되는 과정을 유한 상태 기계의 형태로 설명하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0018] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미하며, 하나 또는 그 이상의 다른 특징이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0019] 이하의 실시예는 본 발명의 이해를 돕기 위한 상세한 설명이며, 본 발명의 권리 범위를 제한하는 것이 아니다. 따라서 본 발명과 동일한 기능을 수행하는 동일 범위의 발명 역시 본 발명의 권리 범위에 속할 것이다.

[0020] 도 1은 본 발명의 일 실시예에 따른 파일 시스템에서의 랜섬웨어 탐지 장치의 구성을 나타낸 도면이다.

[0021] 도 1을 참조하면, 파일시스템에서의 랜섬웨어 탐지 장치(100)는 통신 모듈(110), 메모리(120), 프로세서(130) 및 기록모듈(140)을 포함한다.

[0022] 통신 모듈(110)은 통신망과 연동하여 사용자 단말에 통신 인터페이스를 제공하는데, 사용자 단말로부터 전송되는 데이터 요청을 수신하고, 이에 대한 응답으로서 사용자 단말에 데이터를 송신하는 역할을 수행할 수 있다.

[0023] 여기서, 통신 모듈(110)은 다른 네트워크 장치와 유무선 연결을 통해 제어 신호 또는 데이터 신호와 같은 신호를 송수신하기 위해 필요한 하드웨어 및 소프트웨어를 포함하는 장치일 수 있다.

[0024] 메모리(120)는 파일시스템에서의 랜섬웨어 탐지 방법을 수행하기 위한 프로그램이 기록된다. 또한, 프로세서(130)가 처리하는 데이터를 일시적 또는 영구적으로 저장하는 기능을 수행한다. 여기서, 메모리(120)는 휘발성 저장 매체(volatile storage media) 또는 비휘발성 저장 매체(non-volatile storage media)를 포함할 수 있으나, 본 발명의 범위가 이에 한정되는 것은 아니다.

[0025] 프로세서(130)는 일종의 파일시스템에서의 랜섬웨어 탐지 방법을 제공하는 전체 과정을 제어한다. 프로세서(130)가 수행하는 각 단계에 대해서는 도 2 및 도 3을 참조하여 후술하기로 한다.

[0026] 여기서, 프로세서(130)는 프로세서(processor)와 같이 데이터를 처리할 수 있는 모든 종류의 장치를 포함할 수 있다. 여기서, '프로세서(processor)'는, 예를 들어 프로그램 내에 포함된 코드 또는 명령으로 표현된 기능을 수행하기 위해 물리적으로 구조화된 회로를 갖는, 하드웨어에 내장된 데이터 처리 장치를 의미할 수 있다. 이와 같이 하드웨어에 내장된 데이터 처리 장치의 일 예로써, 마이크로프로세서(microprocessor), 중앙처리장치(central processing unit: CPU), 프로세서 코어(processor core), 멀티프로세서(multiprocessor), ASIC(application-specific integrated circuit), FPGA(field programmable gate array) 등의 처리 장치를 망라할 수 있으나, 본 발명의 범위가 이에 한정되는 것은 아니다.

[0027] 기록 모듈(140)은 적어도 하나 이상의 데이터베이스로 구성되고, 샘플 랜섬웨어 세트, 파일 시스템의 행위에 대

한 로그 파일 데이터 세트, 수집된 행위 패턴 데이터 등 랜섬웨어 탐지 방법을 수행하면서 누적되는 데이터가 저장된다.

[0028] 도 2는 도 1의 구성요소인 프로세서의 랜섬웨어 탐지 방법에 대한 수행 과정을 설명하는 흐름도이고, 도 3은 본 발명의 일 실시예에 따른 파일시스템에서의 랜섬웨어 탐지 방법을 설명하는 순서도이다.

[0029] 도 2 및 도 3을 참고하면, 파일시스템에서의 랜섬웨어 탐지 방법은 프로세서(130)에서 파일시스템 내 파일의 이벤트 발생에 따른 로그 파일이 기록되는 기록모듈(140)과 연계하여 파일의 랜섬웨어를 탐지한다. 파일시스템에서의 랜섬웨어 탐지 방법을 수행하기 위한 프로그램은 가상머신 구동 모듈(131), 파싱 모듈(132), 행위 패턴 분류 모듈(133) 및 탐지 모듈(134)을 포함하지만 상술한 모듈들은 본 발명을 설명하기 위한 일 실시예일 뿐, 이에 한정되지 않고 다양한 변형으로 구현될 수 있다. 또한, 상술한 모듈들은 프로세서(130)에 의해 제어될 수 있는 컴퓨터로 판독 가능한 기록매체로서 메모리(120)에 저장된다.

[0030] 먼저, 프로세서(130)는 랜섬웨어 샘플 세트가 저장된 데이터베이스에서 샘플 랜섬웨어를 불러오고, 가상환경 구동 모듈(131)을 통해 가상 환경에서 샘플 랜섬웨어가 실행되도록 함으로써 샘플 랜섬웨어에 의한 파일 시스템의 행위를 기 설정된 행위 모델링 코드에 따라 이벤트 로그 파일로 로그파일 데이터 세트가 저장된 데이터베이스에 저장한다(S310).

[0031] 이때, 행위 모델링 코드는 파일 생성(Create, C), 파일 삭제(Delete, D), 파일명 변경을 포함한 파일 이동(Move, M) 및 파일 갱신(Update, U)으로 분류 및 정의될 수 있다.

[0032] 프로세서(130)의 파싱 모듈(132)은 로그파일 데이터 세트가 저장된 데이터베이스에서 파일시스템의 로그파일을 파싱하고, 각 파일에서 발생된 행위들에 대해 파일 변경 기록 분석을 수행하여 연속된 행위 모델링 코드로 이루어진 코드열로 변환한다(S320). 즉, 프로세서(130)는 랜섬웨어가 파일을 암호화할 때 발생되는 행위들을 모델링하고, 해당 행위들이 파일 시스템의 데이터베이스 상에 얼마나 많이 기록되는지, 어떠한 행위 패턴들이 자주 나타나는지를 분석한다.

[0033] 행위패턴 분류 모듈(133)은 상기 변환된 코드열을 분석하여 복수의 행위로 이루어진 행위 패턴을 분류한 후 기 설정된 랜섬웨어 행위 규칙에 기초하여 정상 프로그램과 분류되는 랜섬웨어 행위 패턴을 패턴 데이터 수집을 위한 데이터베이스에 저장한다(S330).

[0034] 실제로, 파일 시스템의 기록 모듈(140)에는 가상환경 구동모듈(131)을 통해 파일시스템 행위들이, 예를 들면” CCMUDDCMUCUDCUUUMU” 와 같이 연속된 코드열, 즉 문자열로 변환될 수 있다.

[0035] 따라서, 행위 패턴 분류 모듈(133)은 코드열에서 랜섬웨어 행위 규칙에 기초하여 각 파일에 대해 4개 이상의 행위로 이루어진 행위 패턴 그룹을 추출하고, 행위 패턴 그룹에서 복수의 행위로 이루어진 행위 패턴을 분류한 후 행위별 빈도수, 행위 패턴별 빈도수를 체크한다. 또한, 행위 패턴 분류 모듈(133)은 정상 프로그램에서 나타나는 행위별 빈도수와 기 설정된 횟수 이상 나타나는 행위 패턴을 분류할 수 있다.

[0036] 행위패턴 분류 모듈(133)은 행위 패턴 그룹에서 기 설정된 횟수 이상 나타나는 행위별 빈도수 또는 행위 패턴별 빈도수를 정상 프로그램에서 나타나는 행위별 빈도수 또는 행위 패턴별 빈도수와 비교하고, 두 빈도수의 차이값에 따라 행위 또는 행위 패턴 별로 가중치를 부여하여 랜섬웨어 행위 패턴을 산출한다.이때, 랜섬웨어 실행시 발생된 행위 패턴별 빈도수가 정상 프로그램에서 나타나는 행위 패턴별 빈도수와 차이가 클수록 가중치를 높게 설정한다.

[0037] 예를 들어, 행위 패턴 분류 모듈(133)은 랜섬웨어 실행시의 행위 패턴 빈도수와 정상 프로그램 실행시의 행위 패턴 빈도수를 비교했을 때 랜섬웨어 실행 시 특정한 행위 패턴의 빈도 수가 유난히 높게 나타나는 경우, 해당 행위 패턴의 가중치를 높게 부여한다. 그러나, 랜섬웨어 실행시 특정한 행위 패턴의 빈도수가 정상 프로그램에서의 행위 패턴의 빈도수가 유사하게 나타날 경우, 해당 행위 패턴은 가중치를 낮게 부여한다.

[0038] 따라서, 랜섬웨어 실행시 행위 패턴의 빈도수와 정상 프로그램 실행시 행위 패턴의 빈도수 간에 차이가 크다는 것은 해당 행위 패턴이 랜섬웨어에서 특징적으로 많이 발견되었다는 것을 의미이기 때문에 랜섬웨어 행위 패턴으로 수집한다.

[0039] 탐지 모듈(134)은 수집된 랜섬웨어 행위패턴을 이용하여 실제 환경에서 랜섬웨어 탐지를 수행한다(S340).

[0040] 도 4는 본 발명의 일 실시예에 따른 파일 시스템에서의 랜섬웨어 탐지 방법의 탐지 단계를 설명하기 위한 도면으로서, 4개의 파일(file1, file2, file3, file4)이 file 1, 3, 2, 4, 3, 4, 1, 2, 2, 2, 3, 4, 3, 2, 3의 순

서대로 CCDMDUDCMUMMDMC와 같은 행위 패턴을 발생하였다고 가정할 경우, 각 파일들에서 발생한 행위들을 순서대로 정리한 것이다.

[0041] 탐지 모듈(134)은 파일 시스템 행위가 기 설정된 발생개수가 될 때마다 각 파일 별로 행위 패턴 그룹을 분석하여 랜섬웨어 행위 패턴과 일치하는 행위 패턴이 존재하는 지를 판단한다.

[0042] 만일, 랜섬웨어 행위 패턴과 일치하는 행위 패턴이 존재하는 경우, 탐지 모듈(134)은 행위패턴 분류 단계에서 부여된 해당 행위 패턴에 부여된 가중치를 기 설정된 기준값에 합산하여 탐지수치를 증가시키고, 탐지 수치가 기설정된 임계수치 이상이 되면 해당 행위 패턴을 랜섬웨어 행위 패턴으로 판단하여 랜섬웨어 탐지를 수행한다.

[0043] 도 5는 일반적인 랜섬웨어의 파일 암호화를 위한 행위 패턴을 설명하는 예시도이고, 도 6은 본 발명의 일 실시예에 따른 랜섬웨어 행위 규칙을 통해 추출된 행위 패턴 리스트를 설명하는 도면이고, 도 7은 본 발명의 일 실시예에 따른 랜섬웨어 행위 규칙을 통해 행위 패턴이 형성되는 과정을 유한 상태 기계의 형태로 설명하는 도면이다.

[0044] 도 5의 (a)에 도시된 바와 같이, 일반적으로 랜섬웨어는 원본 파일을 읽어와 새롭게 암호화된 파일을 생성하고, 원본 파일을 삭제하는 행위를 하거나, 도 5의 (b)에 도시된 바와 같이, 파일 이동이 3회 나타나므로 MMM의 행위 패턴으로 표현할 수 있다.

[0045] 이러한 랜섬웨어 행위들을 정황화하고 정상 프로그램들과 분류하기 위해 랜섬웨어 행위 규칙을 정의한다. 랜섬웨어 행위 규칙은 모든 파일의 변경 행위가 단일 파일에 대한 행위로 정의되는 제1 규칙, 파일 생성(C)과 파일 삭제(D)의 행위는 하나의 쌍으로 존재하는 행위로 정의되는 제2 규칙, 선두부에 파일 생성(C)이 존재하지 않으면 파일 이동(M) 및 파일 갱신(U)은 파일 삭제(D)에 후속되는 행위로 출현되지 않는다고 정의되는 제3 규칙, 파일 갱신(U)이 행위 패턴의 선두부에 존재하는 경우에 무의미한 것으로 정의되는 제4 규칙 및 4 개 이상의 행위 패턴 그룹에 대해 3개의 행위로 이루어진 행위 패턴의 반복으로 나타내도록 정의되는 제5 규칙으로 이루어진다.

[0046] 랜섬웨어 행위 규칙 중 제1 규칙, 제2 규칙 및 제3 규칙을 적용하면, 도 6에 도시된 바와 같은 행위 패턴 리스트가 추출되고, 이렇게 추출된 행위 패턴 리스트에 제4 규칙 및 제5 규칙을 적용하면 최종적으로 CDM, CDU, CMD, CUD, DCM, DCU, MMM 및 MUM의 8개의 행위 패턴을 랜섬웨어 행위 패턴으로 분류할 수 있다.

[0047] 도 7에 도시된 바와 같이, 랜섬웨어 행위 규칙 중 제4 규칙 및 제5 규칙에 대한 내용을 확인할 수 있고, 이러한 랜섬웨어 행위 패턴이 형성되는 과정을 무한 상태 머신의 형태로 표현하면, CDM, CDU, CMD, CUD, DCM, DCU, MMM 및 MUM의 8개의 행위 패턴들이 모두 출현되는 것을 알 수 있다.

[0048] 이와 같이, 본 발명의 일 실시예에 따른 파일 시스템에서의 랜섬웨어 탐지 방법은 기기개발 시장 및 랜섬웨어 탐지 관련 소프트웨어 개발 시장 등에서 기업 등 보안을 필요로 하는 컴퓨팅 환경에서 사용할 수 있는 랜섬웨어 탐지 관련 백신 및 보안 제품에 적용될 수 있다.

[0049] 이상에서 설명한 본 발명의 실시예에 따른 파일 시스템에서의 랜섬웨어 탐지 방법은, 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행 가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 이러한 기록 매체는 컴퓨터 판독 가능 매체를 포함하며, 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체를 포함하며, 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다.

[0050] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0051] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0052] 100: 파일시스템에서의 랜섬웨어 탐지 장치

110: 통신 모듈 120: 메모리

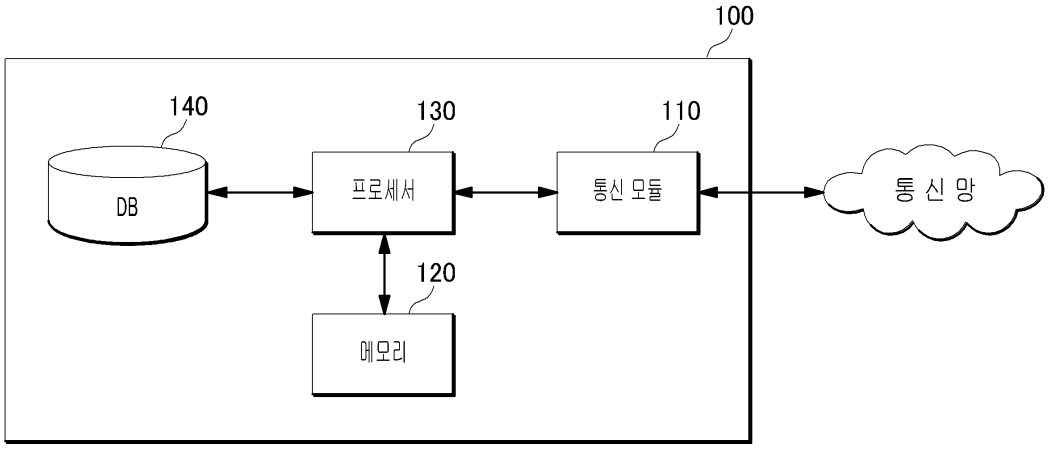
130: 프로세서 140: 기록 모듈

131: 가상머신 구동모듈 132: 파싱 모듈

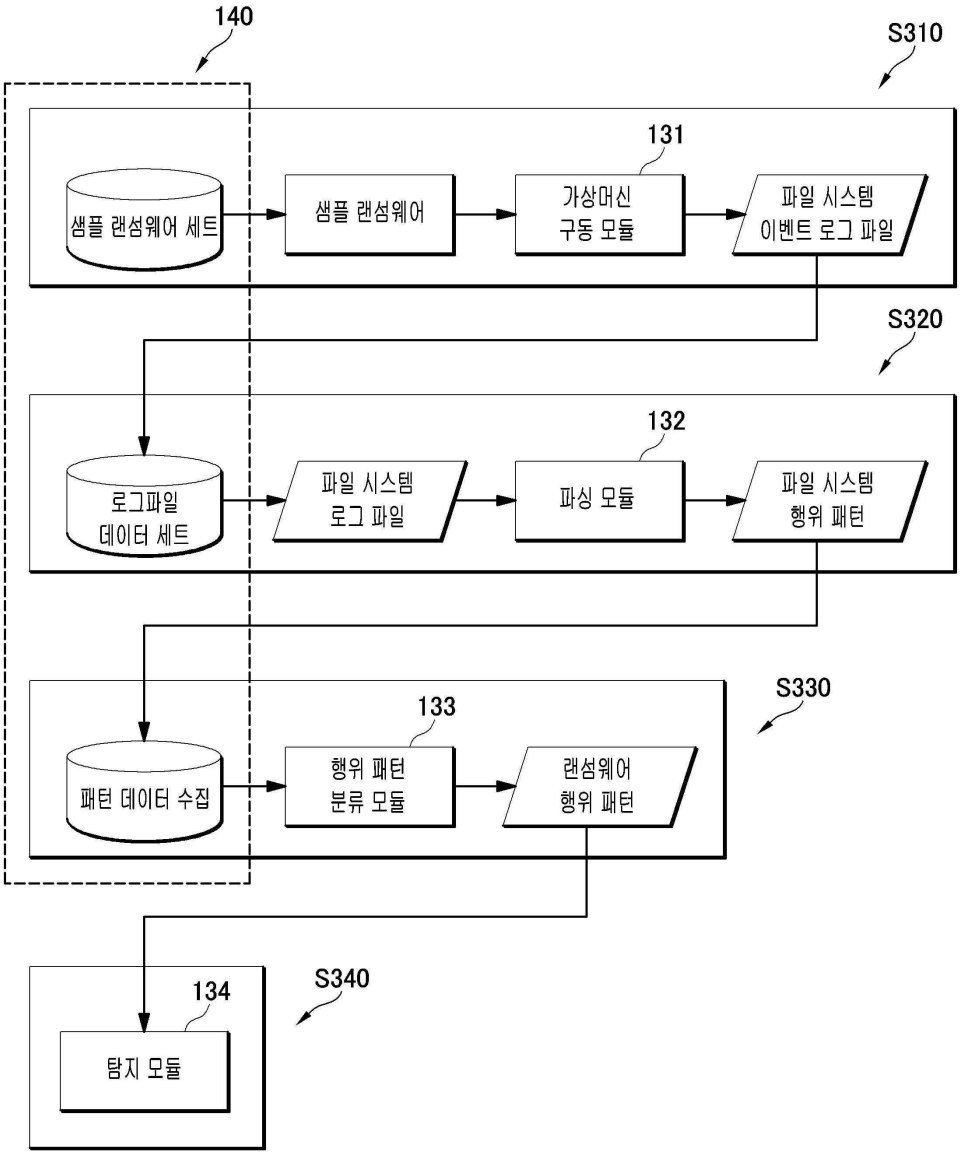
133: 행위패턴 분류 모듈 134: 탐지 모듈

도면

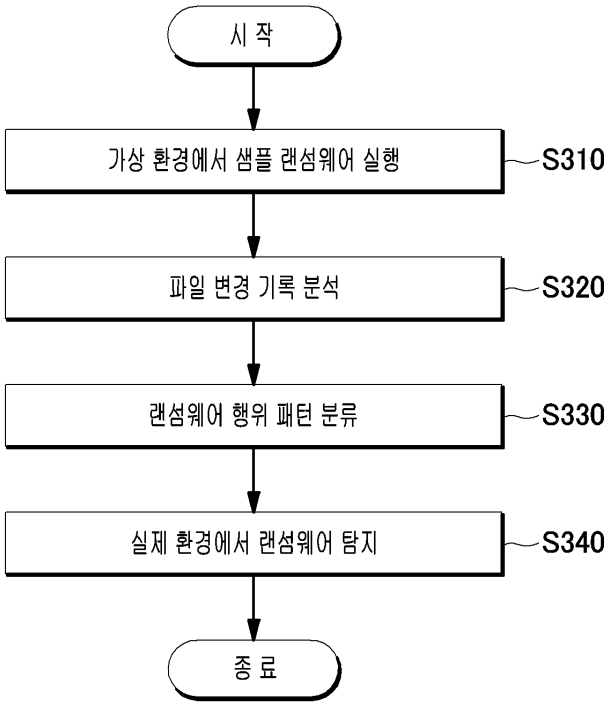
도면1



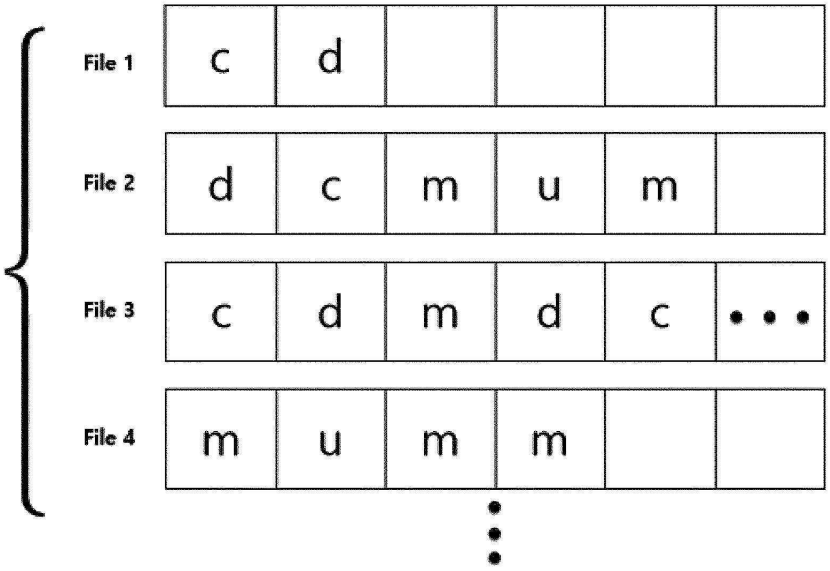
도면2


140
S310
131
샘플 랜섬웨어 세트
샘플 랜섬웨어
가상머신
구동 모듈
파일 시스템
이벤트 로그 파일
S320
132
로그파일
데이터 세트
파일 시스템
로그 파일
파싱 모듈
파일 시스템
행위 패턴
S330
133
패턴 데이터 수집
행위 패턴
분류 모듈
랜섬웨어
행위 패턴
S340
134
탐지 모듈

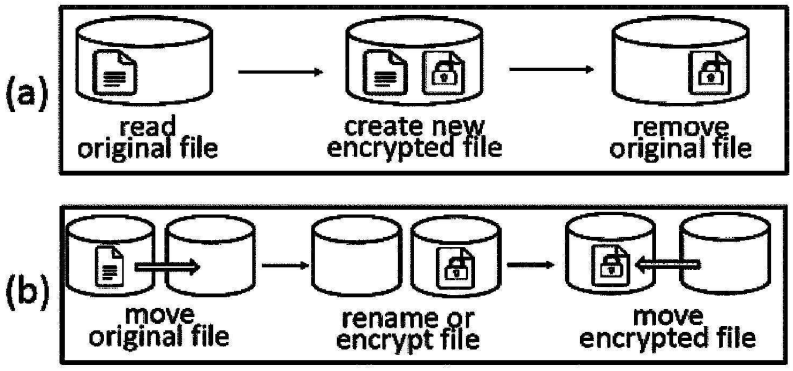
도면3


시 작
가상 환경에서 샘플 랜섬웨어 실행
S310
파일 변경 기록 분석
S320
랜섬웨어 행위 패턴 분류
S330
실제 환경에서 랜섬웨어 탐지
S340
종 료

도면4


File 1
c
d
File 2
d
c
m
u
m
File 3
c
d
m
d
c
File 4
m
u
m
m

도면5



도면6

- 1-gram patterns (two patterns)
  - M,U
- 2-gram patterns (six patterns)
  - CD, DC, MU, UM, MM, UU
- 3-gram patterns (14 patterns)
  - CDM, CMD, DCM, CUD, CDU, DCU, MMM, UUU, MMU, MUM, UMM, UUM, UMU, MUU
- 4 or more-gram patterns (more than 30 patterns)
  - CDMU, CDMM, CMDU, CMDM, CUDU, CUDM, CDUU, CDUM
  - and D, M, U cases

도면7