금융보안원
FINANCIAL SECURITY INSTITUTE

빅데이터 및 인공지능을 통한 재택근무 시스템의 보안 취약점 개선에 대한 연구

전성호* · 이재덕* · 정민혁** · 김재현***
* 부산대학교 IT응용공학과
** 중소기업은행 IT내부통제팀 대리
*** 한국전력공사 전북본부 ICT운영부 사원

요 약

코로나 19로 인해 기업의 근무환경이 크게 변화하고 있다. 국내 및 해외 유수 기업에서 재택근무를 시행하고 있으며, 최근 금융권에서도 '전자금융감독규정 시행세칙'의 개정으로, 비상시에만 허용되었던 사내 업무망 접속이 상시 허용으로 변경되면서 원격(재택)근무의 수요가 폭발적으로 증가하였다. 이에 맞춰 KISA '비대면 업무환경 도입·운영을 위한 보안가이드', 금융보안원 '금융회사 재택근무 안내서' 등 다양한 가이드라인이 발간되어, 원격(재택)근무 시스템 보안의 지침을 제시해주었다. 그러나 보안적 관점에서 많은 기업들은 기술적으로 준비되기 전에 원격(재택)근무를 시행하게 되었고, 최근 이러한 취약점을 이용하여 원격(재택)근무 시스템을 대상으로 한 보안 사고가 꾸준히 발생하고 있다. 본 논문에서는 스마트워크에도 적용할 수 있는 미래 지향적인 관점으로, 원격(재택)근무 시스템의 현주소와 취약점을 분석하고, 기존 가이드 내 다소 포괄적으로 작성되어 있던 내용을 구체화하거나 추가함으로써 원격(재택)근무 시스템 내 보안을 강화할 수 있는 빅데이터 및 인공지능 기반 보안 모델을 제안한다.

키워드

VPN, 원격(재택)근무, 강화학습, 딥러닝, 이상탐지, 암호화

목 차

I. 서론

1. 연구 배경 및 필요성

코로나19 확산으로 인한 ‘사회적 거리두기’ 시행과 직장 내 확진자가 발생함에 따라 근무장소 폐쇄 등으로 인해 비대면 업무방식이 확산되고 있다. 전 세계적으로 다양한 기업에서 원격(재택)근무를 시행하고 있으며, 이에 국내에서도 원격(재택)근무의 필요성이 급증하고 있다. 하지만 원격(재택)근무는 보안 통제가 소홀할 수밖에 없는 장소에서 수행하게 되므로, 다양한 보안 사고의 위협이 존재한다. 이에 대한 대안으로 통신 데이터를 암호화하여 안전하게 내부망에 접속할 수 있게 도와주는 VPN(가상사설망)이 재택근무의 인프라로 조명받고 있다.

VPN 시스템의 취약점을 이용하여 내부 전산망 및 직원 컴퓨터를 대상으로 한 공격이 발생하고 있다. 최근 국내에서 한국원자력연구원, 한국항공우주산업의 내부 전산망 해킹사고가 보고되었으며, 해외에서도 다양한 VPN 취약점을 이용한 공격 사례가 발표되고 있다. 이에 국내 금융권에서는 금융보안원의 ‘금융회사 재택근무 보안 안내서[1]’를 바탕으로 원격(재택)근무 내 다양한 보안 위협을 대비하기 위한 작업을 수행하고 있다. 하지만 매일 새롭게 최신화되는 취약점 및 보안 사고 사례를 보아, 원격(재택)근무 시스템의 추가적인 보안대책의 필요성이 급증하고 있다.

4차 산업혁명의 핵심 기술 중 하나로 꼽히고 있는 인공지능 기술은 다양한 산업 분야에 깊숙히 자리잡았다. 특히 보안 분야에서는 인공지능을 이용한 보안 모델이 네트워크침입탐지(NIDS), 이상금융거래탐지(FDS), 이상징후탐지(ADS)와 같은 분야에 적용되고 있으며, 현재도 인공지능을 접목한 보안 기법에 대한 연구가 활발하게 이루어지고 있다. 하지만 문제는 해킹 공격 기법에서도 다양하게 인공지능을 접목하여, 고도화하고 있다는 것이다. 따라서 보안대책의 필요성이 급증하고 있는 원격(재택)근무 시스템에도 인공지능 기반 보안 모델의 추가적인 구축이 절실한 상황이다.

2. 연구 목표

본 논문에서 진행한 연구의 목표를 요약하면 다음과 같다.

(1) 현재 금융 및 공공기관에서 사용 중인 원격(재택)근무용 VPN에서 발생 가능한 취약점을 분석한다.

(2) 분석 결과를 토대로 다양하게 발생 가능한 종류의 해킹 공격을 예측하고, 이를 대비할 수 있는 보안 모델을 구축한다.

(3) 외부에 공개되어 있는 샘플 데이터를 이용하여 보안 모델의 성능을 검증한다.

(4) 구축한 보안 모델을 토대로 현재 원격(재택)근무 보안 가이드라인을 개선할 수 있는 방안을 함께 제시한다.

Ⅱ. 기술적 배경지식 및 관련연구

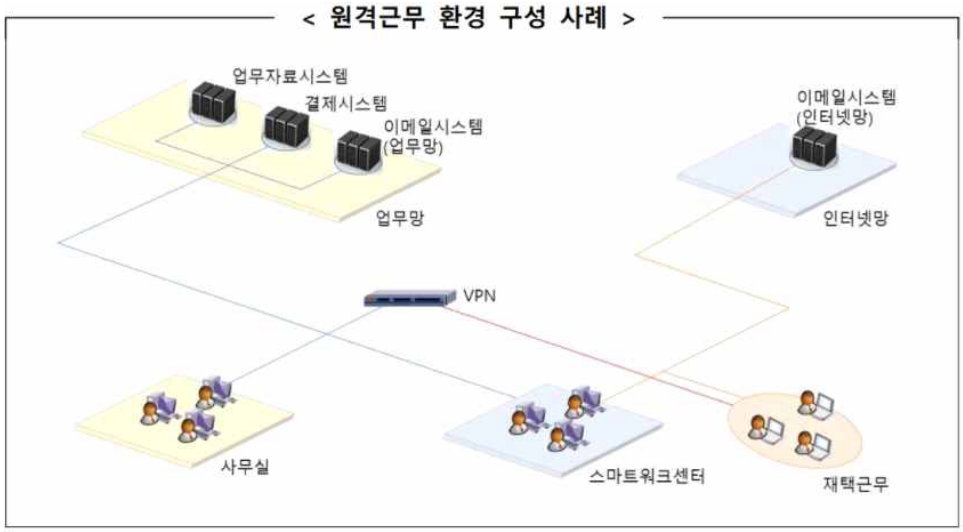
1. 원격(재택)근무 접속 시스템

(1) VPN(가상사설망)

VPN은 공중 네트워크를 통해 정보를 외부에 공개하지 않고 통신할 목적으로 사용하는 사설 통신망이다. VPN에서 네트워크 메시지는 인터넷과 같은 공공망 위에서 터널링(tunneling)이라는 기술을 통해 가상의 전용 네트워크로 구현하게 된다. 터널링이란 송신자와 수신자 간의 데이터를 마치 터널이 뚫려 있는 것처럼 통로를 생성하여 사설망처럼 보안 기능을 제공하는 기술이며, PPTP, L2TP, IPSec 등의 프로토콜을 이용하여 구현하게 된다.

(2) 원격(재택)근무 시스템

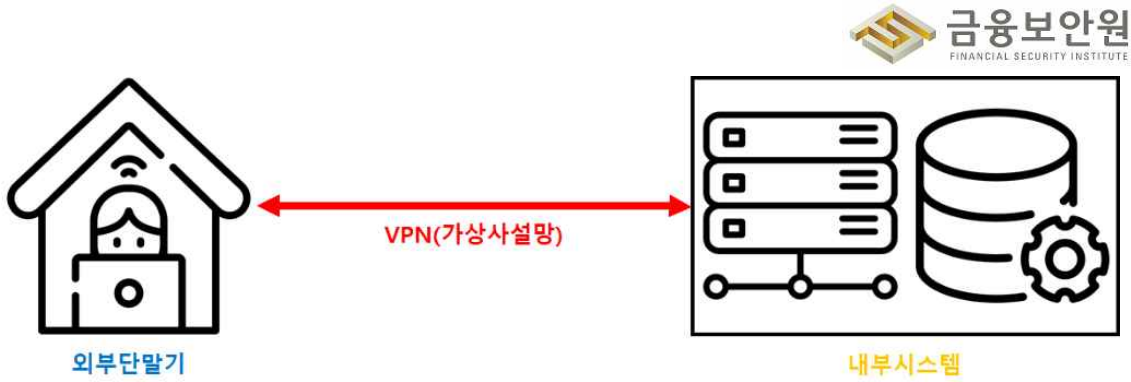
원격(재택)근무 시스템이란 직원이 기업 내 정해진 장소가 아닌 공간에서 내부 시스템에 접속하여 업무를 수행할 수 있도록 하는 시스템이다. 일반적으로 원격(재택)근무 시스템의 경우 인터넷을 통해 내부망에 접속하기 때문에 VPN을 통한 원격 접속 방식을 채택하고 있으며, 접속 방식에 따라 직접 접속 방식과 간접 접속 방식으로 구분된다.



<그림 1> 원격근무 환경 구성 사례[2]

1) 직접 접속 방식

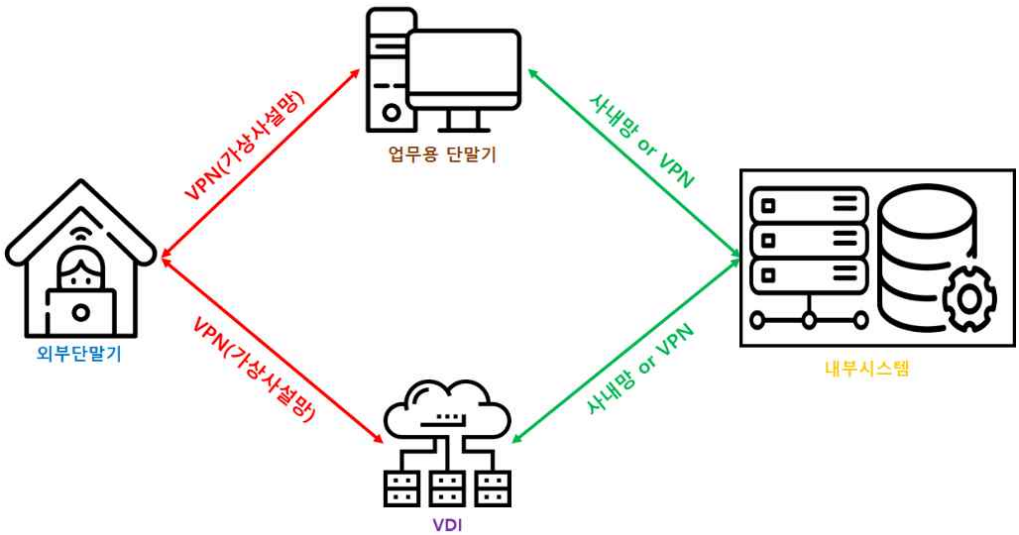
기업 내부 단말기가 아닌 외부 단말기로 내부 시스템에 직접 접속하는 방식이다. 직접 접속 방식은 외부 단말기에서 내부 시스템의 업무를 직접 처리하고, 데이터도 외부 단말기에 저장되기 때문에 간접 접속 방식보다 보안에 취약하다는 단점을 가진다. 따라서 직접 접속 방식을 통해 원격(재택)근무 시스템에 접속하는 경우, 외부 단말기의 종류나 업무 장소를 통제하는 등 보다 강력한 보안대책의 적용이 필수적이다.



<그림 2> 직접 접속 방식

2) 간접 접속 방식

간접 접속 방식은 기업 내부 단말기로 VDI(Virtual Desktop Infrastructure)와 같은 가상 업무용 단말기를 경유 하거나, 원격 접속 프로그램을 통해 기업 내 위치한 업무용 단말기를 경유 하여 내부시스템에 접속하는 방식이다. 간접 접속 방식의 특징은 외부 단말기에서 업무가 직접 처리되지 않고, 업무용 단말기에서 업무가 처리된다. 따라서 외부 단말기에는 데이터가 저장되지 않으며, 단순 화면 이미지만 출력하게 된다. 그리고 간접 접속 방식 중 VDI 시스템을 활용하는 경우, VDI 시스템이 외부 클라우드, 사내망, 업무망 등 다양한 환경에 위치할 수 있고, 각 환경별 VPN 사용 유무의 차이가 존재한다. 이와 같이 VDI를 활용한 간접 접속 방식을 통해 기업별 시스템의 구성에 알맞은 원격(재택)근무 서비스를 제공 할 수 있다.



<그림 3> 간접 접속 방식

2. 현 원격(재택)근무 관련 가이드라인

최근 코로나 19 확산 방지책으로 원격(재택)근무가 화두되고 있다. 이에 따라 NIST SP 800-114 'User's Guide to Telework and Bring Your Own Device(BYOD) Security' [3]가 조명되고 있으며, '전자금융감독규정 시행세칙'의 개정으로 금융권에서도 비상시에만 허용되었던 사내 업무망 접속이 상시 허용으로 변경되면서 원격(재택)근무의 수요가 폭발적으로 증가하였다. 국내에서도 수요에 맞춰 KISA '비대면 업무환경 도입·운영을 위한 보안가이드' [1], 금융보안원 '금융회사 재택근무 안내서' [4] 등 다양한 가이드라인이 발간되었다.

3. 강화학습

2016년 구글 딥마인드에서 발표한 강화학습 모델인 알파고의 등장은 강화학습의 발전을 촉진시켰다.[5] 강화학습은 마르코프 결정 프로세스(Markov Decision Process, MDP)로 표현되는 문제를 푸는 알고리즘이다. 강화학습의 기본적인 구성요소는 다음과 같다.

(1) 에이전트(agent) : 환경(environment)을 탐색하는 주체
(2) 상태(state) : 환경 내부에서 에이전트의 상태
(3) 행위(action) : 특정 상태로 가기 위한 에이전트의 행동
(4) 보상(reward) : 에이전트가 특정 행위를 취했을 시 얻게 되는 보상
(5) 정책(policy) : 에이전트가 상태에서 행위를 취함에 대한 확률분포

마르코프 결정 프로세스에서 에이전트는 자신의 상태를 알게 되고, 주어진 정책에 따른 행동을 취하게 된다. 그 결과 보상과 다음 상태에 대한 정보를 업데이트하게 된다. 이때 보상의 누적 기대값을 가치 함수(value function)라 하며, 이 가치 함수를 최대화하는 정책을 구하는 것이 강화학습의 목표이다. 하지만 강화학습이 실제 환경에 적용되기에는 모든 경우의 수를 정리하여 문제를 풀어야 하는 한계점을 가진다. 따라서 모든 경우의 수를 정리하는 것이 아닌, 모델이 직접 경험하고, 축적된 데이터를 토대로 가치 함수를 순차적으로 업데이트하는 샘플링 기법을 사용한다. 샘플링 기법의 대표적인 종류로는 에피소드(episode) 단위로 보상함수를 업데이트하는 몬테카를로 학습(Monte-Carlo Learning, MC)과 시간(time-step)별로 보상함수를 업데이트하는 시간차 학습(Temporal-Difference Learning, TD)이 있다.[6]

강화학습의 종류로는 가치 기반 강화학습(Value-based Reinforcement Learning)과 정책 기반 강화학습(Policy-based Reinforcement Learning)이 있다. 가치 기반 강화학습에서는 가치함수를 목적함수로 두고, 가치 함수를 최대화하는 행위를 선택하는 것을 목표로 한다. 정책 기반 강화학습은 좋은 정책을 잘 찾는 것을 목표로 하며, 상태에 대한 행위의 분포에서 행위 하나를 샘플링하는 것이 특징이다. 정책 기반 강화학습은 가치 기반 강화학습에 비해 행위에 대하여 연속적인 정책을 알아내기에 용이하다는 장점이 있으며, 현재 로봇 및 자율주행 도메인을 넘어 다양한 영역에도 접목이 되고 있다.

4. A3C

정책 기반 강화학습 알고리즘 중 Actor-Critic 알고리즘은 Actor 네트워크와 Critic 네트워크를 사용한다.[7] Actor는 상태가 주어졌을 때 행동의 분포인 정책을 업데이트하고, Critic은 Actor가 수행한 행위에 대한 평가한다. Actor-Critic 알고리즘은 Replay Buffer를 사용하지 않고, 매 step마다 학습 결과로 얻은 상태, 행위, 보상, 다음 상태를 이용하여 모델을 학습한다. 에이전트의 행동 확률을 학습하는 방법을 policy gradient라 한다. 미분을 통한 정책 업데이트로 최적의 policy를 찾아가고, 가치 함수를 함께 사용함으로써 에이전트의 행동 확률의 안정성을 높이는 것이 Actor-Critic의 특징이다. Actor-Critic 알고리즘은 다음과 같다.

(0) 주요 parameter Θ와 ω를 초기화

(1) Actor update

$$\theta \leftarrow \theta + \alpha \nabla_\theta ln P_\theta(a_t|s_t) Q_w(s_t, a_t)$$

(2) Critic update

$$\omega \leftarrow \omega - \beta \nabla_\omega (R_t + \gamma Q_\omega(s_{t+1}, a_{t+1}) - Q_w(s_t, a_t))^2$$

(3)매 step마다 (1), (2) 반복

Actor-Critic에서 Actor의 기대 출력으로 Advantage를 사용한 알고리즘이 A2C(Advantage Actor-Critic)이다. Advantage는 Q 자리에 Q-V를 대입함으로써, sample의 분산을 낮춘다. A2C는 1-step TD를 사용함으로써 update 속도가 상대적

으로 빠르다는 장점이 있다. A2C의 알고리즘은 다음과 같다.[8]

(0) 주요 parameter Θ와 ω를 초기화

(1) Collect N samples

(2) Actor update

$$\theta \leftarrow \theta + \alpha \nabla_{\omega} \sum_{i=t-N+1}^{t} (lnP_{\theta}(a_i|s_i)(R_i + \gamma_w V(s_{i+1}) - V_w(S_i))$$

(3) Critic update

$$\omega \leftarrow \omega - \beta \nabla_{\omega} \sum_{i=t-N+1}^{t} (R_i + \gamma V_w(s_{i+1}) - V(s_t))^2$$

(4) Clear the batch <Θ update되고 나면 기존 Θ를 파기 후 새로운 policy를 사용>

(5) (1) ~ (4) 과정을 반복하며 batch 형태로 update

A3C(Asynchronous Advantage Actor-Critic) 알고리즘은 A2C 모델의 단점인 sample batch 간 correlation이 발생하는 문제를 해결하기 위해 제안된 모델이다. A3C는 한 개가 아닌 여러 개의 에이전트를 비동기적으로 실행하며, n-step TD 방식을 사용한다는 특징이 있다. 그리고 actor의 목적함수 생성 시 entropy를 추가로 사용함으로써 적극적인 경험을 통해 학습을 진행한다. A3C 알고리즘은 여러 개의 에이전트를 실행시키기 때문에, 다양한 환경에서 얻을 수 있는 데이터로 학습시킬 수 있다는 장점이 있고, 항상 최신 데이터를 사용하여 학습하기 때문에 DQN의 단점을 보완할 수 있다. A3C 알고리즘은 다음과 같다.[8]

(0) 주요 parameter Θ와 ω를 초기화

(1) Collect N samples

(2) Actor update

$$\theta \leftarrow \theta + \alpha \nabla_{\theta} \sum_{i=t-N+1}^{t} (lnP_{\theta}(a_i|s_i)A_i + \lambda H_i(P_{\theta}(a_i|s_i)))$$

(3) Critic update

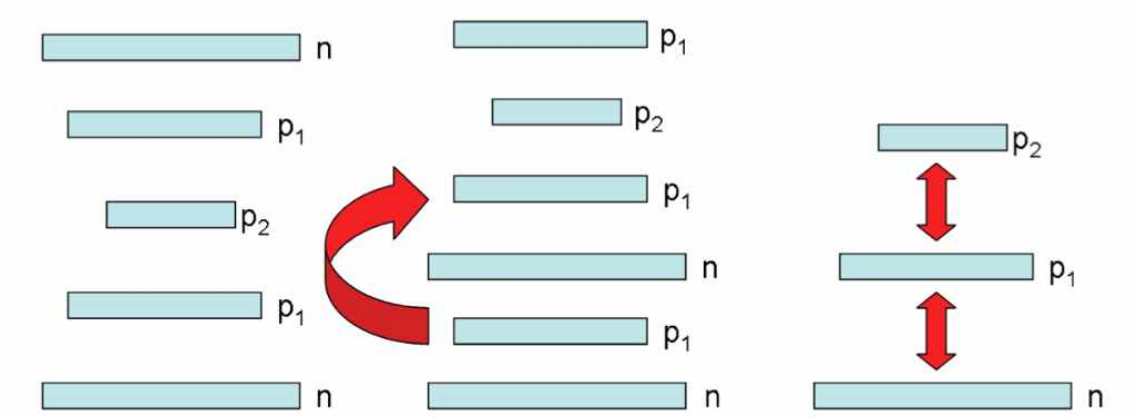
$$\omega \leftarrow \omega - \beta \nabla_{\omega} \sum_{i=t-N+1}^{t} (A_i)^2$$

(4) Clear the batch

(5) 비동기적 worker에 대하여 1)~4) 과정을 반복한다.

5. Autoencoder

Autoencoder는 비지도학습 기반의 딥러닝 모델로, 입력과 출력이 같은 구조를 가지는 네트워크이다.[9] 입력 데이터를 인코더 네트워크에 통과시켜 더 낮은 차원으로 압축된 벡터 z값을 얻은 뒤, 압축된 벡터 z를 디코더 네트워크에 통과시켜 입력 데이터와 동일한 차원의 출력값을 얻는다. 이때 모델은 인코더에 통과된 입력 데이터 x와 디코더를 통과한 출력 데이터 y값의 유사성을 비교하여, 재구성 오류와 정확도를 반환한다. Autoencoder는 이러한 재구성 오류를 최소화하며 입력 데이터의 Feature를 추출한다. 현실 세계에서 라벨링 되지 않은 데이터를 사용해도 학습이 가능한 비지도학습의 특징을 이용하여, 이상탐지(Anomaly Detection) 분야에서도 Autoencoder를 이용한 연구가 활발히 이루어지고 있다.

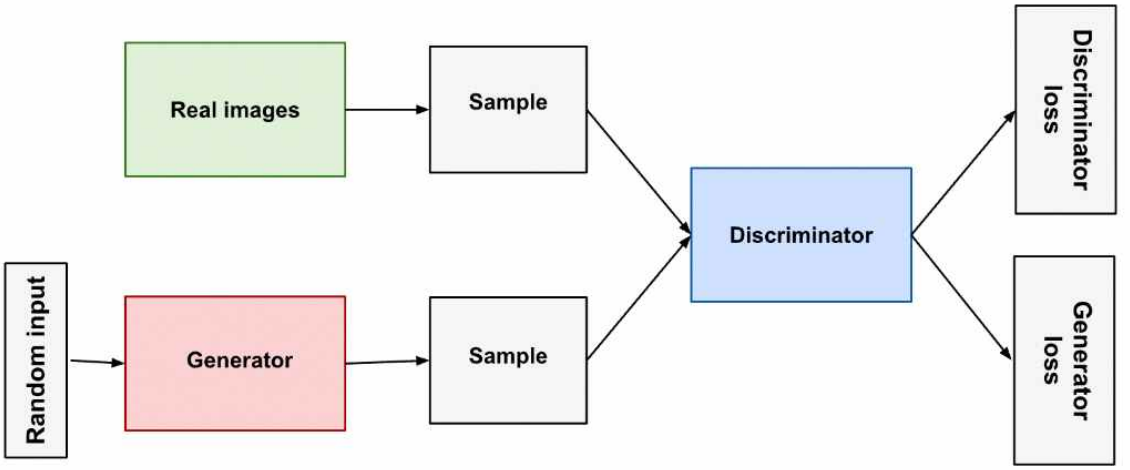


<그림 4> Autoencoder Structure[9]

6. GAN

2014년 이안 굿펠로우(Ian Goodfellow)에 의해 소개된 생성적 적대 신경망(Generative Adversarial Network, GAN)은 생성자(generator)와 판별자(discriminator)

로 구성된다.[10] 생성자는 실제 데이터와 비슷한 위조 데이터를 생성하는 것을 목표로 하고, 판별자는 실제 데이터와 위조 데이터를 구별하는 것을 목표로 한다. 이처럼 GAN은 서로 적대적 관계에 놓여있는 생성자와 판별자가 서로 경쟁하며 발전해 나가는 적대적 학습 기법을 사용한다. GAN은 현재, 이미지 처리 분야에서 활발히 쓰이고 있으며, 이를 넘어 텍스트, 보안과 같은 다양한 영역으로 확대되어 가고 있다. 특히 이상탐지 분야에서 데이터 문제 및 탐지모델로, 전통적 딥러닝 모델의 한계를 극복하기 위해 GAN을 접목한 연구가 활발하게 이루어지고 있다.



<그림 5> GAN Structure[11]

Ⅲ. 개선된 재택근무 보안시스템 모델 설계

1. 현 재택근무 시스템 취약점 분석

(1) 국내 침해 사례

2021년 6월 한국원자력연구원에서 VPN 취약점으로 인해 신원불명의 외부인이 사내 시스템 일부 접속에 성공하는 침해사고가 발생하였다. 한국원자력연구원은 원전, 핵연료봉 등 원자력 기술을 연구하고 개발하는 국가 최대의 핵심 연구기관이다. 해당 사고는 연구원이 해킹메일의 첨부 파일을 개인 컴퓨터에 저장하면서 비롯되었고, 컴퓨터 내 저장되어 있던 VPN 접속용 ID·PW 등의 정보가 해커에게 탈취되었다. 이외에도 방산업체인 대우조선해양과 한국항공우주산업에서도 VPN 취약점을 이용한 침해사고 사례가 보고되기도 하였다.[12]

(2) 해외 침해 사례

2020년 8월 일본 기업 38개사가 해킹으로 인해 VPN ID·PW가 유출되는 피해를 입었다. NISC에 따르면 2020년 8월 범죄 사이트에서 전 세계 약 900개 이상 기업의 VPN 정보가 거래되고 있다고 알려졌다.[13]

2020년 9월 이란 해킹조직은 정보 유출을 목적으로 미국 연방기관 네트워크를 겨냥해 사이버 공격을 단행하였다. 당시 IT기업, 공공기관, 의료기관, 금융사, 보험사, 언론사 등 다양한 기업이 대상이 되었으며,[14] 해킹 조직은 알려진 VPN 취약점들을 활용하여 VPN 시스템에 침입하였다. 이후 관리자 권한을 획득하여 추가 악성 행위를 통해 네트워크에 장기간 머물었고, 정보를 탈취해 다크웹에 판매하기도 하였다. 추가로 2021년 4월 미국 연방기관은 VPN 취약점을 이용한 침해사고가 다시 발생하였다고 보고하였다.[15]

(3) 발생 가능 취약점 및 공격 기법 예측

1) 비인가 프로세스 사용

금융보안원 '금융회사 재택근무 안내서'[4]에는 외부 단말기로 회사에서 제공된 자산이 아닌 개인 단말기를 사용하는 경우 강력한 보안통제를 권고하고 있다. 현재 통제방식으로 IP, MAC, H/W Serial 등을 기준으로 통제하는 방식이 있고, 그중 가장 강력한 통제방식은 사용자 VPN 계정과, 외부 단말기 MAC 주소를 1:1 매칭하여 화이트리스트 방식으로 적용하는 방법이 있다. 하지만 위 방법의 경우 모든 직원 외부 단말기의 정확한 MAC 주소를 수집하는 것은 단말기 도입 시점부터 고려되지 않았다면 적용하기 어렵다는 단점을 가진다. 이외에도 부서 공용 노트북을 사용하거나, 직원 간 단말기 대여, 신규 직원에 의한 단말기 추가 등의 문제로 관리의 용이성이 떨어진다는 한계점이 존재한다.

VPN 접속 시 레지스트리, 프로레스 체크가 정상적으로 이루어지지 않으면, 백도어 사이트에 의한 계정 탈취, 원격 프로그램 및 가상환경을 통한 화면 정보 및 권한 탈취가 발생할 수 있다. 이에 금융권에서는 정상적인 원격(재택)근무 시스템 사용자의 프로세스, 레지스트리 데이터를 빅데이터화 하여 단순 화이트리스트/블랙리스트 방식이 아닌, 보다 강력한 비정상 프로세스 탐지 모델의 구축이 필요하다.

2) 취약하거나 위장된 VPN 어플리케이션 사용

최신 업데이트를 적용하지 않은 취약한 VPN 어플리케이션에는 [표 1]과 같은 취약

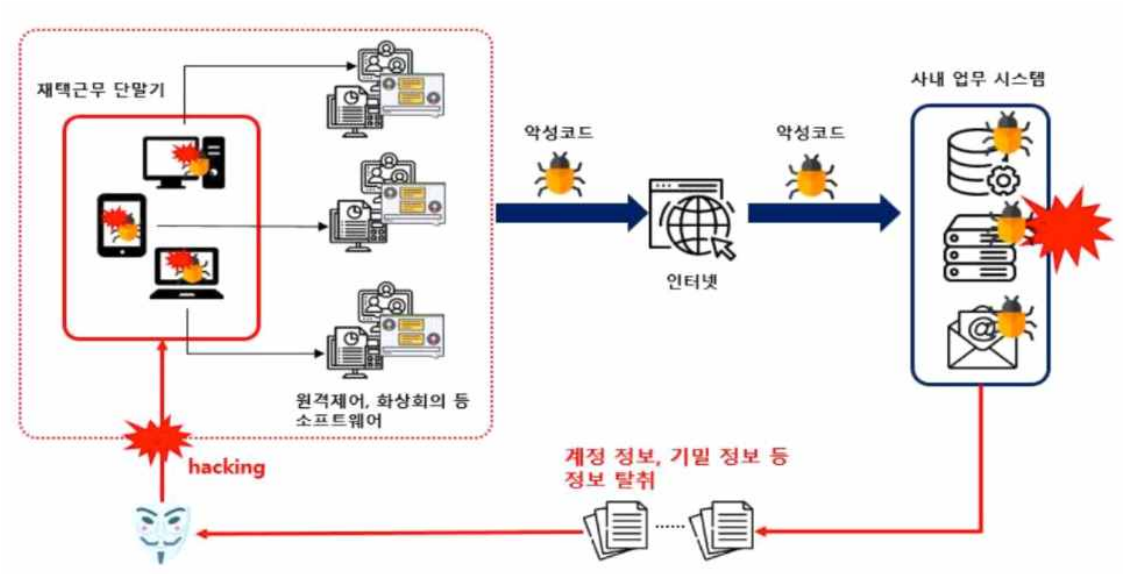
점들이 존재하며, 해커는 이를 이용하여 사내전산망에 침입할 수 있다.

제품	CVE 취약점	내용
Pulse Connect Secure	CVE-2019-11510	비인가 된 공격자가 임의의 파일 읽기 가능
	CVE-2019-11539	인증 된 공격자 명령 삽입, 실행 가능
	CVE-2021-22893	인증되지 않은 사용자가 원격으로 임의 코드 실행 가능
Fortinet	CVE-2018-13379	비인가 된 공격자가 시스템 파일 다운로드 가능
	CVE-2018-13382	비인가 된 공격자가 사용자의 암호를 수정 가능
	CVE-2018-13383	공격자가 라우터에서 실행되는 쉘의 권한을 획득 가능
Palo Alto Networks	CVE-2019-1579	인증되지 않은 사용자가 원격으로 임의 코드 실행 가능

<표 1> VPN 장비의 알려진 취약점[16]

3) 접속 단말 감염을 통한 제어권 탈취

공개된 많은 침해사례를 통해 알 수 있듯이 해커는 주로 VPN 장비의 취약점을 이용하거나, 외부 단말기에 대한 제어권을 탈취하여 내부망에 침입하는 공격 기법을 사용한다.



<그림 6> 접속 단말 감염을 통한 보안 위협[2]

외부 단말기의 감염위협이 될 수 있는 상황은 다음과 같다.

가. 해킹메일

해킹메일은 해커가 직장동료나 정부 기관등을 사칭하여, 악성코드가 포함된 첨부파일이나 크로스 사이트 스크립팅 등 악의적인 웹사이트 링크를 전송하여 디바이스 제어권을 탈취하기 위한 기법이다. 주로 악성코드를 심어 외부 단말기의 제어권을 탈취하거나, VPN 서비스의 접속 인증 정보를 탈취하기 위한 목적으로 사용된다.

나. 신뢰할 수 없는 네트워크 및 개방형 Wi-Fi

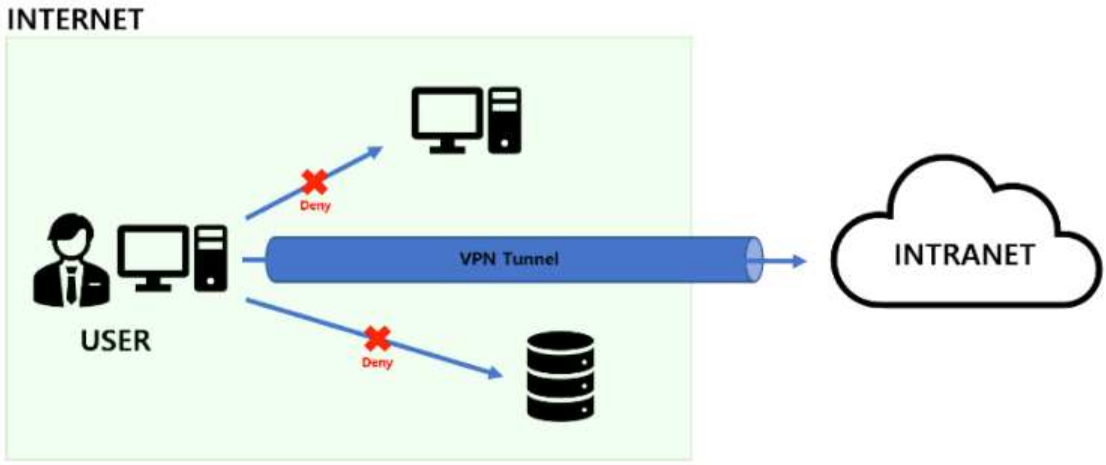
공공 와이파이에서는 중간자 공격, 패킷 스니퍼, 와이파이 스푸핑 등을 통해 디바이스를 공격할 수 있어, 보안에 매우 취약하다.[17] 이에 KISA '비대면 업무환경 도입·운영을 위한 보안가이드' [1]에서는 개방형 Wi-Fi를 사용한 사내망에 접속을 점검할 것을 권고하고, 금융보안원 '금융회사 재택근무 안내서' [4]에서는 NFC, 핫스팟 등의 네트워크 접속 기능을 차단할 것을 권고한다.

다. 악성프로그램

정보통신망 이용촉진 및 정보보호 등에 관한 법률에서는 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램을 악성 프로그램이라고 정의한다.[18] 주로 해킹메일을 통해 감염되거나 인터넷상에서 신뢰할 수 없는 프로그램을 다운로드하는 경우 감염된다. 악성 프로그램은 특성에 따라 스파이웨어, 백도어, 키로그 등 다양하게 분류되며, 디바이스의 정보를 빼거나, 원격으로 접근하여 화면이나, 키보드 입력 값 등을 탈취할 수 있고, 디바이스를 직접적으로 제어할 수도 있다. 이에 백신 프로그램 등을 통해 악성 프로그램을 조기에 탐지하고, 승인된 프로그램만 설치할 수 있도록 통제하고 있다.

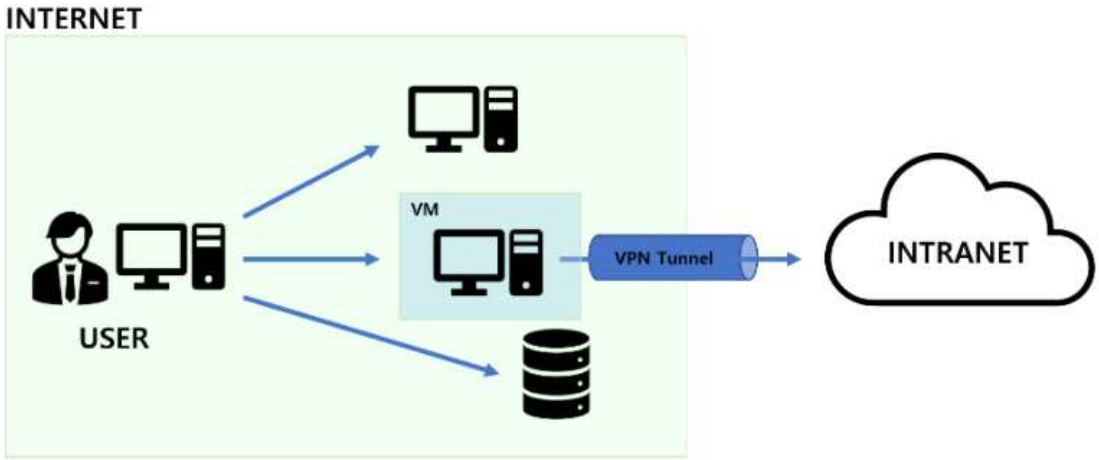
라. 가상머신을 통한 VPN 접속

VPN으로 사내망에 접속된 상태에서 인터넷 연결을 차단하지 않는다면, 사내망과 인터넷망의 접점이 발생하게 된다. 이는 해커가 실시간으로 사내망에 접속할 수 있는 접점을 제공할 수 있으므로, 금융보안원 '금융회사 재택근무 안내서' [4]에서는 내부망 접속 시 인터넷 연결 차단을 의무사항으로 규정하고 있다. 이에 기업은 <그림 7>와 같이 외부와의 통신을 항시 VPN Gateway를 통하도록 하고, VPN 통신에 사용되는 LAN 카드를 제외한 모든 LAN 카드를 통제하는 방식 등을 사용하고 있다.



<그림 7> 인터넷을 통제한 접속 방식

그러나 사용자가 편의를 위해 <그림 8>과 같이 가상머신(VM ware, Hyper V등)을 이용하여 가상머신 내부에서 VPN 통신을 한다면 가상머신의 LAN 카드를 통제하기 때문에, 호스트 PC에서는 인터넷을 사용할 수 있으며, 이 경우 사내망과 인터넷망은 다시 접점이 생겨 해커가 실시간으로 접속할 수 있게 한다.



<그림 8> 가상머신을 이용한 사내망 접속

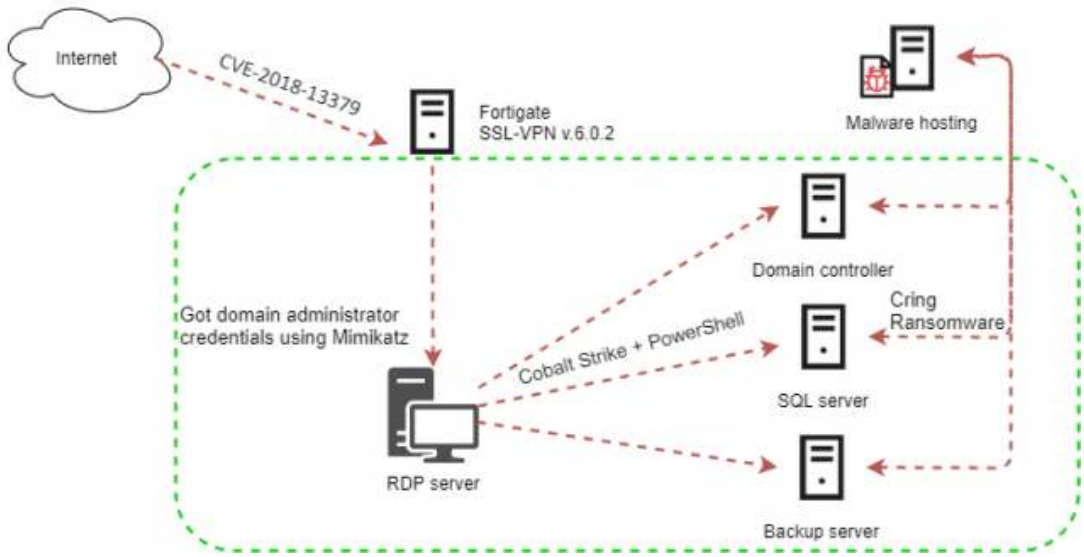
4) 내부망 접속 후 활동

가. 무선 도청

공격자가 내부망에 성공적으로 접속 시 내부망에 존재하는 개인 정보 데이터를 무선 도청할 확률이 높다. 이러한 행위는 보안성뿐만 아니라, 데이터 유출과 같은 심각한 사고로 이어질 수 있다.

나. 랜섬웨어 유포

유럽에서 VPN 취약점을 이용해 배포된 랜섬웨어 크링(Cring)은 공격자가 내부망에 침투 성공 후, 통신이 이루어지는 데이터를 도청하는 중간자 공격 기법을 사용하였고, 도청한 데이터에 랜섬웨어를 심어 유포하는 공격을 가했다.[19] 이에 VPN 망 접속 단계에서의 보안 강화를 넘어, VPN 접속 이후의 보안대책 강화도 필수적이다.



<그림 9> 랜섬웨어 '크링' 공격 워크 플로우[19]

2. 모델 제안

(1) 망 접속 과정에서 취약점을 극복하기 위한 모델 제시

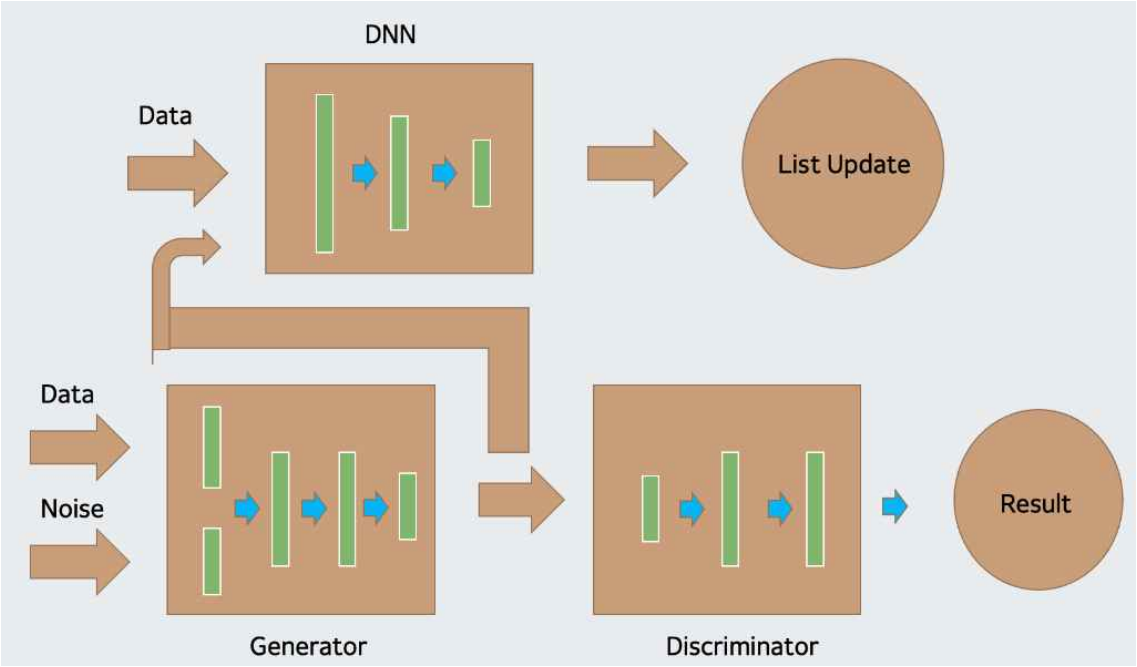
1) AI 기반 프로세스 탐지 모델

본 논문에서는 망 접속 보안 절차를 강화하기 위한 방안으로 생성적 적대 신경망을 이용한 프로세스 통제 모델을 제시한다. 이는 프로세스의 접근 요청을 분석하여

자동으로 블랙리스트로 추가하는 방식으로 모델의 구성도는 <그림 10>과 같다.

보안 사고 사례 중 비인가 프로세스의 접근 요청 로그를 분석한 후 원-핫 인코딩(One-Hot encoding)을 사용하여 데이터 전처리 작업을 수행한다. 이에 정리된 데이터를 DNN을 통해 학습 후 분류 작업을 수행하며, 정상 혹은 비정상으로 이진 분류 결과가 도출되기에 활성화 함수로 ReLU와 Sigmoid를 사용하였다.

보안 사고 사례 데이터는 모수가 희소해 딥러닝 학습 중 과적합의 위험성이 존재한다. 본 논문에서는 이 점을 해결하기 위해 GAN을 통해 다양한 사례의 데이터를 추가 생성하였다. 그 후 생성된 데이터를 DNN 모델에 재학습(Retraining)하여 모델의 안정성과 정확도를 높였다.



<그림 10> AI 기반 프로세스 탐지 모델 구성도

2) 가상머신 탐지 절차가 추가된 인증 모델

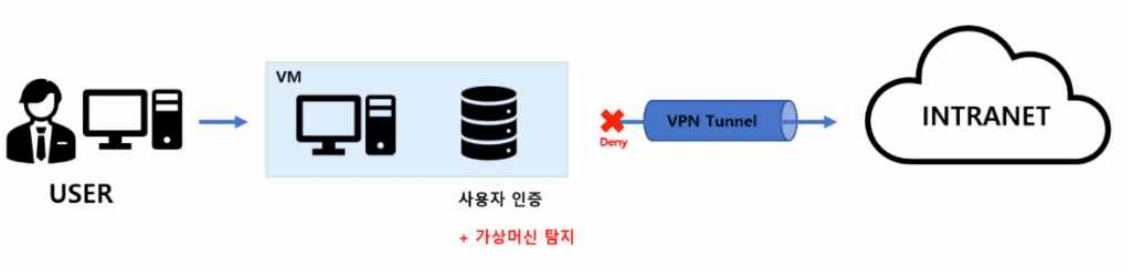
연구기관이나 보안회사는 수없이 등장하는 새로운 악성코드를 모두 직접 분석하기에는 한계가 있어, 자동분석시스템을 개발하여 활용하고 있다. 하지만 자동분석 시스템은 대부분 공개된 가상머신 기반으로 제작되고 있고, 악성코드는 이러한 가상머신을 우회하기 위한 다양한 기법들을 활용하고 있다. 이에 따라 악성코드가 가상

머신을 우회하기 위해 가상머신 환경을 검증하는 행위를 원격(재택)근무 접속 과정에 적용한다면, 가상머신으로 인터넷 차단 기능을 우회하려는 시도를 극복할 수 있다. 악성코드가 가상머신을 탐지하는 방법에는 <표 2>와 같은 방법들이 있다.

가상머신 우회 방법	구체적인 행위
레지스트리 키 확인	RegOpenKeyExA()를 이용하여 레지스트리에서 가상머신과 관련된 키가 있는지 확인
프로세스 확인	_stricmp를 이용하여 가상머신과 관련된 프로세스가 있는지 확인
파일 확인	FindFirstFileA를 이용하여 가상 머신과 관련된 파일있는지 확인

<표 2> 악성코드의 가상머신(자동분석시스템)우회 방법[20]

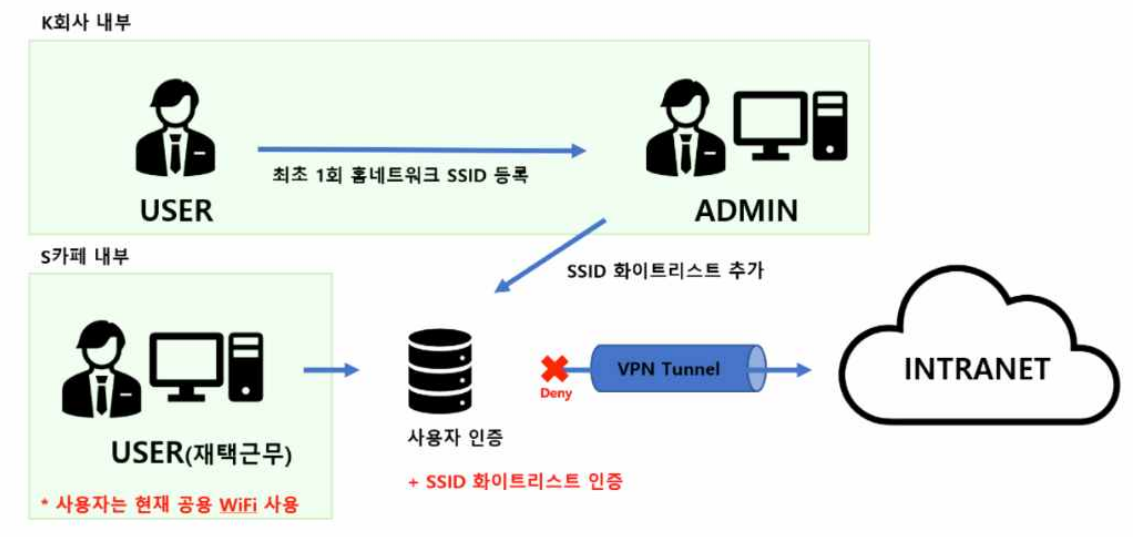
본 논문에서는 가상머신 탐지 절차가 추가된 망 접속 인증 모델을 제안한다. 사용자 외부 단말기에서 원격(재택)근무를 위해 VPN에 접속 시 <그림 11>과 같이 검증 과정을 거친다. 가상머신 내부에서 접속하는 상황이 감지되면 VPN 접속을 차단하여, 인터넷과 사내망의 접점 발생으로 사내망에 접속하는 상황을 방지한다.



<그림 11> 가상머신 탐지 절차가 추가된 인증 모델

3) 무선 네트워크 사용 시 SSID 화이트리스트가 추가된 인증 모델

본 논문에서는 사용자 인증과 연계하여 SSID 화이트리스트를 적용한 네트워크 인증 보안 모델을 제안한다. <그림 12>과 같은 인증 절차를 거쳐 홈 네트워크가 아닌 공공장소에서의 무선 네트워크를 통한 접속을 방지한다.

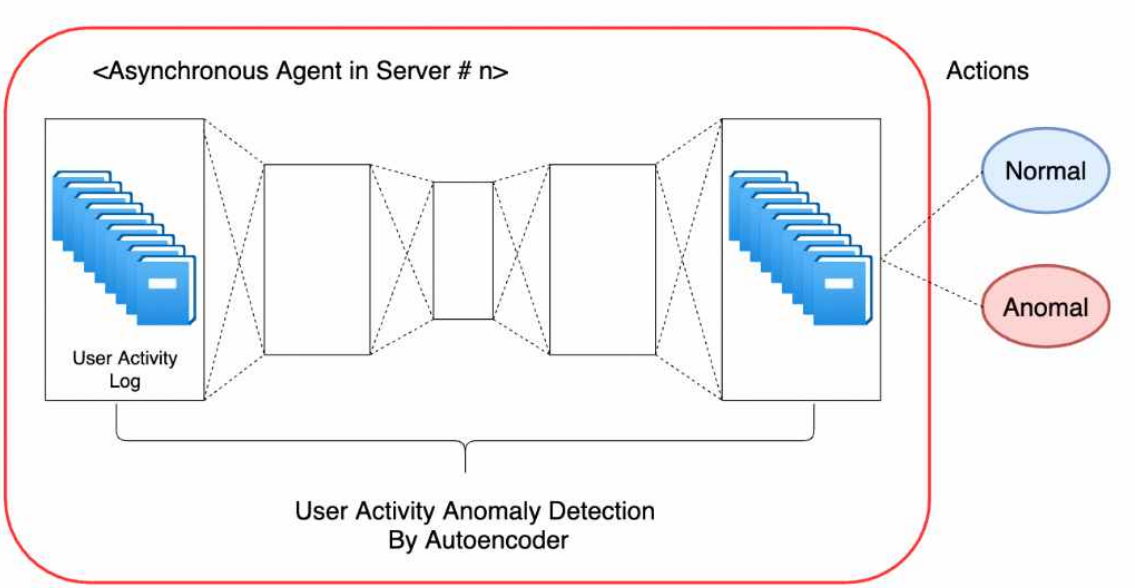


<그림 12> 무선 네트워크 사용 시 SSID 화이트리스트 인증 절차가 추가된 인증모델

(2) 내부망 내 보안절차를 강화한 모델

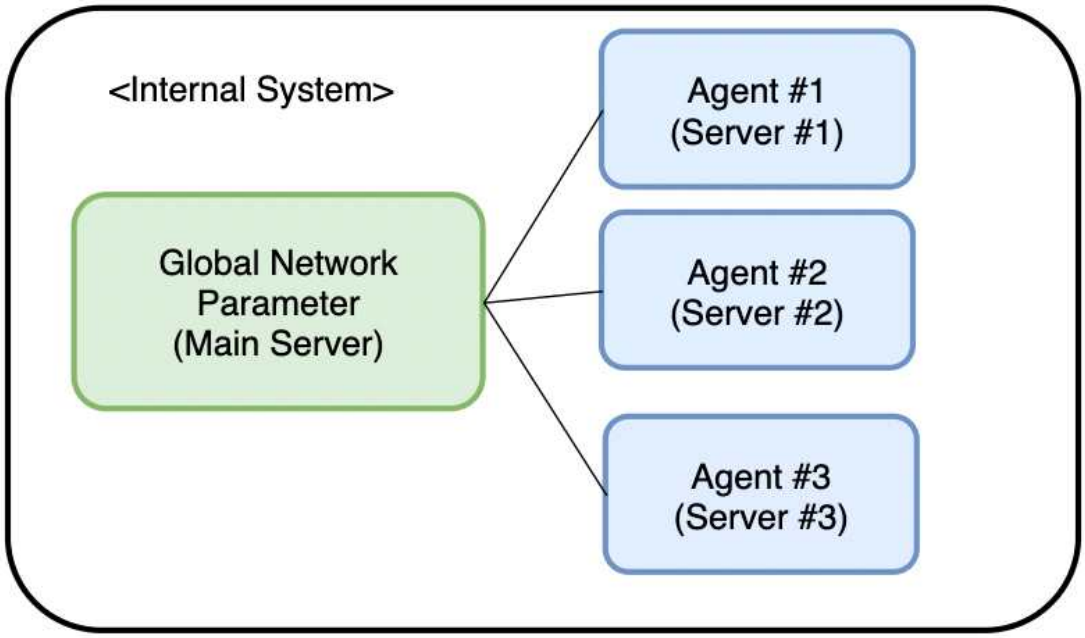
1) 심층 강화학습을 이용한 이상징후 감지

VPN을 통해 원격(재택)근무 시스템에 접속 후, 사용자가 부서 및 업무 성격에 벗어난 시스템에 접근을 시도하거나, 비정상 트래픽 발생 시 로그 분석을 통해 감지한다. 딥러닝 기반 이상탐지 모델은 뛰어난 성능을 토대로 효과적인 이상징후를 탐지하지만, 새로운 데이터 추가로 모델 업데이트 시 갱신된 데이터를 포함한 빅데이터를 재학습해야 하는 한계를 가진다. 이러한 딥러닝 연산의 특성은 학습 과정에서 발생하는 취약점을 즉시 보완하기 어렵기 때문에 적대적 공격과 같은 기법에 취약하다는 한계점이 존재한다. 본 모델은 이러한 한계점을 극복하기 위해 새로운 상황에 적응하고, 모델을 스스로 강화해 나가는 심층 강화학습을 적용하였다. 강화학습을 위한 Optimal Policy를 학습하기 위한 모델 구조는 <그림 13>와 같다.



<그림 13> 로그 분석을 통한 이상징후 탐지 모델

각 서버에 저장되어 있는 사용자 활동에 대한 로그를 수집 후 파싱 및 시퀀스 벡터로 분해하여 특징을 추출한다. 이후 추출한 특징을 Autoencoder에 입력하여 일반 사용자 활동 패턴과 상이한 이상 징후를 포착한다. 이를 통해 정상/비정상 여부를 판단하고, 판단 활동에 대한 샘플을 중앙 서버로 전송한다. 중앙 서버에서는 심층 강화학습 모델인 A3C를 사용하였으며, 각 서버 내 에이전트들의 행위를 반영하여 정책을 업데이트하고, 이상징후 탐지모델로서의 성능을 개선해 나간다.



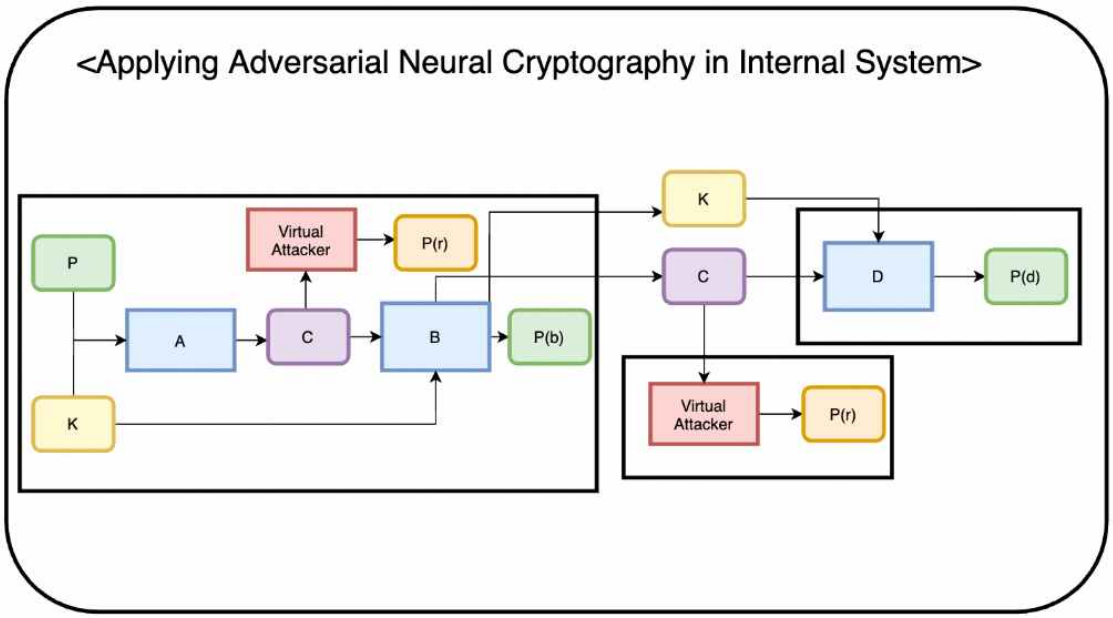
<그림 14> A3C 기반 내부망 이상활동 모니터링 모델

이상징후 탐지모델에 의해 사용자의 활동이 이상 행위로 판단된 경우, 해당 계정의 활동상태를 잠금으로 변경 후, 추가 인증 절차를 통해 접속 인가 여부를 판단한다. 이를 통해 실시간으로 이상 활동을 탐지하고, 사내망에 접속한 공격자의 활동을 조기 차단함으로써, 보안성을 강화한다.

2) 적대적 신경 암호화를 이용한 보안 통신 모델

금융권은 마이데이터 사업 및 클라우드 도입으로, 개인 정보를 안전하게 보호할 수 있는 방안이 필수적이다. 현재 블록체인, 동형암호와 같은 다양한 암호화 기법들이 제시되고 있으며, 가까운 미래에 여러 빅데이터 솔루션의 기반이 될 것으로 전망된다. 이외에도 사내망에서 발생하는 데이터 송수신에도 이러한 암호화 기법이 적용된다. 블록체인 시스템은 파일의 변조가 불가하기 때문에 데이터의 무결성을 보장하면서 보안성을 확보할 수는 있지만, 데이터의 수정이 발생하는 내부망 통신에 블록체인 시스템을 적용하기에는 분명한 한계점이 존재하다. 추가적인 대안으로 제시되는 동형 암호화는 데이

터 암호화에 있어 데이터의 크기를 큰 폭으로 증가시키기 때문에, AI 기반 모니터링 시스템을 구축하기에는 대용량의 리소스가 요구되는 단점을 가지고 있다. 이에 본 논문에서는 구글에서 발표한 암호화 기술인 적대적 신경 암호화 기법을 이용하여 내부망 통신의 보안성을 강화하고, 정보 유출 방지에 활용할 수 있는 방안을 제시한다.[21]



<그림 15> 적대적 신경 암호화를 이용한 내부망 보안 통신 모델

적대적 신경 암호화 기법은 생성적 적대 신경망인 GAN을 이용해서 데이터를 암호화하고, 데이터의 기밀성을 보장하는 것을 목표로 한다. 암호화 통신 시나리오는 서버 내부 통신, 서버 간 통신으로 설정한다.

가. 서버 내부 통신 시나리오

서버 내부 통신 시나리오는 전송자 A, 수신자 B, 가상의 공격자로 구성한

다. A는 B에게 데이터 P를 안전하게 통신하는 것을 목표로 하고, 가상의 공격자는 통신을 도청하는 것을 목표로 한다. A와 B는 비밀키인 K를 공유하며, A는 P를 암호화한 C를 B에게 전송한다. B와 가상의 공격자는 각각 암호화된 데이터를 받아 처리하고, P를 복구하려 시도한다.

나. 서버 간 통신 시나리오

서버 간 통신 시나리오는 전송자 B, 수신자 D, 가상의 공격자로 구성한다. B는 A로부터 수신받아 복구한 P를 다시 암호화해서 다른 서버 D에게 전송하고, 가상의 공격자는 통신을 도청하는 것을 목표로 한다. B와 D는 비밀키를 공유하며, D와 가상의 공격자는 암호화된 데이터를 받아 복구하려 시도한다.

GAN 기술을 이용하여 송신자와 수신자는 공격자를 물리치는 방법을 배우면서 성공적으로 통신할 수 있도록 학습한다. 송신자와 수신자는 사용할 암호화 알고리즘을 미리 정의하지 않고, 어떠한 형태의 공격자의 시도에도 효과적으로 도청을 방어할 수 있다는 장점이 존재한다. 이러한 장점을 이용하여, GAN 암호화는 높은 수준의 개인 정보를 유지하지 않고도 회사와 신경망 간 정보를 교환하는 데 사용될 수 있다. 즉, 모델이 정보를 선택적으로 보호하는 방법을 학습할 수 있다. 이에 본 논문에서는 내부망에서의 보안 통신을 위한 효율적인 암호화 기법으로 적대적 신경 암호화 기법을 제안한다.

3. 실험을 통한 모델 검증

(1) 테스트 데이터셋

테스트를 위한 샘플 데이터셋은, LogPAI가 이상 징후 분석 연구를 위해 제공한 시스템 로그 데이터셋을 사용하였다. 데이터셋은 200개 이상의 Amazon EC2 노드에서 빅데이터 처리를 프레임워크인 HDFS(Hadoop Distributed File System)을 실행하는 동한 확보된 HDFS 로그로 구성되어 있으며, 11,175,629

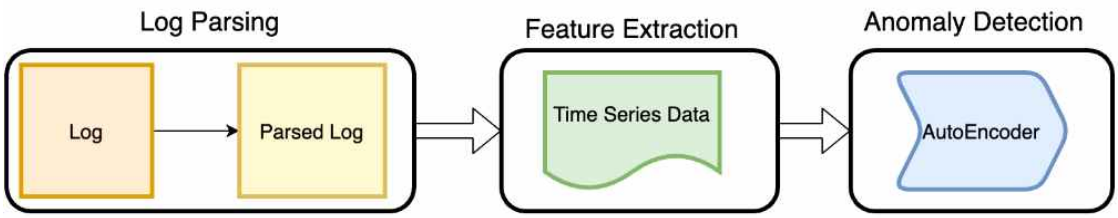
개의 데이터와 575,062개의 세션으로 구성되어 있다. 로그의 이상 여부는 세션 수준에서 레이블링하였다.

081110 011237 13 INFO dfs.DataBlockScanner: Verification succeeded for blk_6996194389878584395
081110 014023 5733 INFO dfs.DataNode$PacketResponder: PacketResponder 0 for block blk_4741107979793372752 terminating
081110 103333 9016 INFO dfs.DataNode$PacketResponder: Received block blk_4263664068073345850 of size 67108864 from /10.251.214.67
081109 214009 2594 INFO dfs.DataNode$DataXceiver: 10.250.5.237:50010 Served block blk_3166960787499091856 to /10.251.43.147

<표 3> HDFS 테스트 데이터셋의 로그 메시지

(2) 내부망 보안 실험

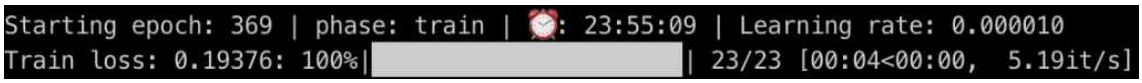
실험의 과정은 <그림 16>과 같다.



<그림 16> 실험 절차

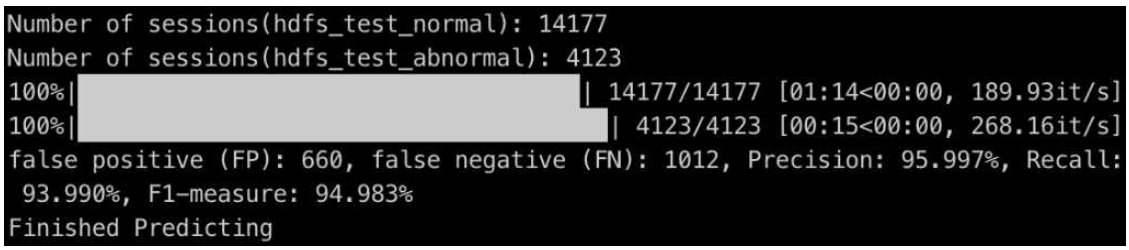
HDFS로 정제한 로그는 수신 블록, src(송신자 IP), dest(수신자 IP)로 이루어져 있다. 이렇게 연속적으로 쌓인 로그를 파싱을 통해 시간에 따른 시계열 데이터로 변환한 뒤, 시계열 데이터의 전처리 기법인 샘플링을 이용하여 이런 시계열 데이터를 벡터 단위로 분해하여 특징을 추출한다. 특징이 추출됨

으로서 전처리가 완료된 이 시계열 데이터를 오토인코더 모델의 입력으로 넣은 뒤, 이상징후를 탐지하도록 학습을 수행하였다. 전체 강화학습 모델은 A3C 모델을 사용하였으며, 성능 검증을 위해서는 이상징후 탐지 모델의 분류성능평가지표로 많이 사용되는 정밀도(Precision), 재현율(Recall), F1 score를 산출하였다. 총 369 epoch를 진행 한 뒤, Train Loss는 0.19376까지 떨어진 것을 확인하였다.



<그림 17> 모델 학습 결과 Train Loss

심층 강화학습 결과 이상분류 탐지모델의 성능 평가지표로 0.9599의 정밀도, 0.9399의 재현율, 0.94983의 F1 지수를 얻을 수 있었다. 이를 통해 심층 강화학습 기반 이상 로그 트래픽 탐지 모델이 효과적으로 이상 활동을 탐지하는 것을 확인할 수 있었다.



<그림 18> 모델 성능 검증 결과

Ⅳ. 결론

1. 기대효과

본 논문에서는 현재 재택근무 보안 시스템이 가지는 취약점을 보안 사고 동향에 맞춰 분석한 뒤, 보안사고를 사전에 탐지·대응할 수 있는 모델을 제안하였다. 가상머신 사용 여부 탐지, 공용 Wi-Fi 사용 여부를 사전에 탐지하여 디바이스 감염위협을 조기에 차단할 수 있다. 또한 이미 사용자의 재택근무 장비가 감염이 되고 난 후 상황을 가정하여, 내부망 접속 시 보안 모델과 내부망 접속 후 이상활동을 제한 할 수 있는 다양한 딥러닝·심층 강화학습 기반 보안 모델을 사용했다. 4차 산업혁명 시대가 도래함에 있어, 보안 기법과 함께 공격 기법 또한 고도화되고 있다. 이에 수많은 개인정보와 중요한 데이터를 다루는 금융업계의 보안 절차를 고도화하여 향후 발생 가능한 수많은 보안 위협으로부터 회사의 자산을 안전하게 지킬 수 있을 것으로 기대된다.

2. 연구의 한계점 및 향후 연구

본 논문에서 진행한 연구의 한계점은 다음과 같다.

(1) 기업마다 다양한 형태의 재택근무 시스템을 사용하고 있기에, 본 논문에서 제안한 모델이 모든 기업의 시스템에 완벽하게 적용할 수 없다는 한계점이 존재한다.

(2) 기업마다 다루는 데이터의 종류가 다르고, 운영하는 서버의 종류가 다르기 때문에, 서버에 축적되는 로그 또한 다양하다. 내부망의 로그 같은 경우는 대외비로 간주되기 때문에, 실제 데이터를 사용한 실험은 진행할 수가 없

었다.

(3) 실제 공격자의 입장에서 내부망에 접속하여, 보안 모델이 동작하는지를 검증하기 위한 공격 시나리오를 작성은 하였으나, 실제 시스템에는 적용을 해 볼 수 없었다.

향후 연구사항은 다음과 같다.

(1) 그래프 딥러닝 알고리즘을 이용한 추가적인 모델의 구현을 통해 이상징후 탐지 모델을 고도화한다.

(2) 모의 재택근무 보안 서버를 구축한 뒤, 시뮬레이션을 진행함으로서 실제 기업에서도 사용이 가능하도록 보안 모델을 강화하는 것을 목표로 한다.

[참고문헌]

[1] Ahmed A. Jaha, Fathi Ben Shatwan, Majdi Ashibani, “Proper Virtual Private Network (VPN) Solution“, 2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies, pp. 309-314, Sept 2008.

[2] 한국인터넷진흥원(KISA), 과학기술정보통신부, 비대면 업무환경(원격근무, 영상회의) 도입・운영을 위한 보안 가이드, 2020.

[3] Murugiah Souppaya, Karen Scarfone, User's Guide to Telework and Bring Your Own Device (BYOD) Security, SP 800-114, 2007

[4] 금융보안원, 금융회사 재택근무 보안 안내서, AGR-Ⅶ-2020-②-203, 2020.

[5] David Silver, Aja Huang, Chris J.Maddison, et. al. “Mastering the game of Go with deep neural networks and tree search“, Nature, 529, pp. 484-489, Jan. 2016

[6] P. Marbach, J.N. Tsitsiklis, “Simulation-based optimization of Markov reward processes“, PhD thesis, MIT, 1998

[7] Vijay R. Konda, John N. Tsitsiklils, “Actor-Critic Algorithms“, Neural Information Processing Systems Conference, p. 1008-1014, Jan 2000

[8] V Mnih, A P Badia, M Mizra, “Asynchronous Methods for Deep Reinforcement Learning“, International Conference on Machine Learning, 2016

[9] Pierre Baldi, ““utoencoders, Unsupervised Learning, and Deep ArchitecturesA,

JMLR: Workshop and Conference Proceedings 27:37-50, 2012

[10] Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mira, et.al, “Generative Adversarial Nets“, Neural Information Processing Systems Conference, 2014

[11] Google Developers, Overview of GAN Structure [Internet], Available: https://developers.google.com/machine-learning/gan/gan_structure

[12] 김정근, 방산업체 해킹 어떻게 이뤄졌나…VPN 등 민간 ’취약점’ 집중 공격 [Internet], Availiable: https://www.news1.kr/articles/?4358998, 2021.08.26.

[13] データの世紀, テレワーク `VPN暗証番号流出　国内38社に不正接続 [Internet]. Avaliable: https://www.nikkei.com/article/DGXMZO62994110U0A820C2MM8000/, 2021.08.26.

[14] 오다인, 美 “이란 해킹조직, VPN 취약점 악용해 정보 유출“ [Internet], Avaliable: https://m.etnews.com/20200922000229, 2021.08.27.

[15] 전유진, 중국 해커 집단 ’VPN 취약점’ 이용, 미국 정부 기관 해킹 [Internet]. Avaliable: https://www.cctvnews.co.kr/news/articleView.html?idxno=226594. 2021.08.26.

[16] 이글루시큐리티, 비대면 근무체계로 인한 보인이슈 및 대응방안 [Internet]. Avaliable: http://www.igloosec.co.kr/BLOG_%EB%B9%84%EB%8C%80%EB%A9%B4%20%EA%B7%BC%EB%AC%B4%EC%B2%B4%EA%B3%84%EB%A1%9C%20%EC%9D%B8%ED%95%9C%20%EB%B3%B4%EC%95%88%EC%9D%B4%EC%8A%88%20%EB%B0%8F%20%EB%8C%80%EC%9D%91%EB%B0%A9%EC%95%88?searchItem=&searchWord=&bbsCateId=47&gotoPage=4, 2021.08.27

[17] Hilah Mazyar, Why You REALLY Need to Stop Using Public WiFi [Internet], Available:https://www.vpnmentor.com/blog/10-reasons-really-need-stop-using-public-wifi/, 2021.08.27.

[18] 법률 제17358호, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 국가법령정보센터.

[19] 지디넷코리아, VPN, 많이 쓰니 해커가 집중 공략했다 [Internet], Available: https://zdnet.co.kr/view/?no=20210409093837, 2021.04.09.

[20] 조성준, “VM 동작과 드라이브 검사를 통한 VM 우회공격 탐지 기법”, 석사, 전남대학교, 광주광역시, 2016.

[21] Martin Abadi, David G. Anderson, ““earning to Protect Communications with

Adversarial Neural CryptographyL, International Conference on Learning Representations(ICLR) 2017 conference, 2016