A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment

Eun Byol Koh, Joohyung Oh, and Chaete Im

Abstract—**The term BYOD(Bring Your Own Device) collectively refers to the related technologies, concepts and policies, where employees do works by accessing corporate's internal IT resources, such as database and applications, using their personal mobile devices like smart phones, laptop computers and tablet PCs. As operational convenience has improved with the advent of a new IT environment, such as BYOD and smart-work, security threats are increasing at the same time. To deal with those threats, there are several security solutions such as NAC(Network Access Control) and MDM(Mobile Device Management) products. However, it is insufficient to resolve risk factors occurring in BYOD environment with them due to their limitations and users' psychological repulsion to the control of personal devices. Thus, it is necessary to establish a flexible security policy considering numerous and diverse types of terminals and various circumstances. In addition, security policy must be aimed at protecting corporate data by isolating users of abnormal behaviors as well as at ensuring utilization of various personal devices and work continuity. This paper studies on security issues possibly occurred in the new IT environments of BYOD and smart-work and describes problems which cannot be solved with the existing technologies and solutions. Finally, this paper proposes an integrated security system to resolve this new security threats. It shows that this system examines the context information conducting a dynamic access control based on it.**

Index Terms— **BYOD(Bring Your Own Device), Context-Awareness based Dynamic Access Control, MDM(Mobile Device Management), NAC(Network Access Control), Security**

I. Introduction

THESE days the distribution and the use of personal smart devices have expanded and smart-work services spread. This phenomenon brings to the advent of BYOD era where individuals use their personal smart phones and tablet PCs in work environment. BYOD (Bring Your Own Device) is the general term of technology, concept and policy for employees to do works with their personal devices such as smart phones, laptop computers and tablet PCs, accessing corporate internal resources like database and applications. With the advent of BYOD, corporate internal infrastructures have shifted from a closed to an open environment. That is, it is now possible to access to corporate servers for work and service from every point of contact through Internet with personal smart devices while it was only possible inside corporate network in the past. In a closed environment, corporate data are processed and stored only by devices owned by the respective company. However, in an open environment, such data processing and storage is also possible by using individuals' personally owned devices. The right to own, manage and control devices and data has also been shifted from an IT department inside a company to individual users. Thus, while security policies of the past focused on user-centered security policies such as user authentication, corporate infrastructures in an open environment triggered by the advent of BYOD require device-centered security policies such as device authentication. Directly speaking, in the past security was required mainly for risk factors at the entry to and the exit from a corporate network. But in the recent times where BYOD is permitted, management of not only a specific point but also all points to access a corporate network has become necessary.

According to a survey conducted by Cisco in 2012 on 600 companies, 95% of them are already permitting the use of personally owned smart devices in their work environments and assets so that productivity of their employees has improved as a result. From users' point of view, BYOD certainly increases convenience and efficiency of work. However, from the companies' point of view, security threats also increase as much as the convenience improved as a result of the advent of a new IT environment, such as BYOD. One of the reasons for the increased security threats is the issue of managing smart devices which have diverse operating systems. At present, numerous manufacturers are producing smart devices containing various operating systems. According to a survey by OpenSignal in 2012, 3997 types of Android OS devices are being used and, for 70% of these devices, the respective manufacturers use the OS with variation. In addition to this issue concerning the device itself, the security is faced with a difficult situation since corporate confidential data can be easily leaked as a result of negligence in device management. And efficient control of personal devices can be difficult due to frequent device change.

All users including individuals, companies and institutions

Manuscript received Dec 03, 2013; revised Dec 17, 2013. This work was supported by the IT R&D program of MSIP/KEIT(Ministry of Science, ICT and Future Planning/Korea Evaluation Institute Of Industrial Technology). [10045109, The Development of Context-Awareness based Dynamic Access Control Technology for BYOD, Smartwork Environment].

Eun Byol Koh is with KISA(KOREA INTERNET & SECURITY AGENCY), Seoul, 138-950, KOREA (phone: +82-2-405-5442; fax: +82-2-405-5129; e-mail: ebkoh@kisa.or.kr).

Joohyung Oh is with KISA(KOREA INTERNET & SECURITY AGENCY), Seoul, 138-950, KOREA (e-mail: jhoh@kisa.or.kr).

Chaete Im is with KISA(KOREA INTERNET & SECURITY AGENCY), Seoul, 138-950, KOREA (e-mail: chtim@kisa.or.kr).

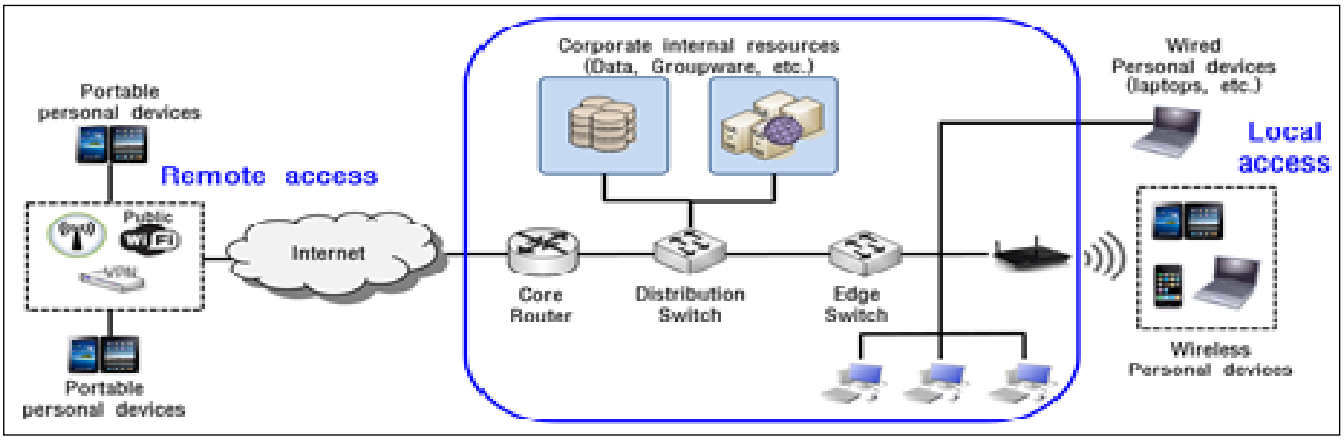

Fig. 1. Diagram of BYOD and Smart-work Environment

share a common notion that it is necessary to invest in information security as much as the convenience they enjoy. According to a questionnaire survey conducted on 1192 corporate IT officers by IT World in 2013, the corporate IT officers emphasized the necessity of security as a major issue concerning the environment shift to BYOD. In other words, the necessity of security technology can be raised as the key issue to introduce the BYOD system. As internal corporate infrastructures permit access by individual devices, it becomes necessary for security technologies to prevent the leak of corporate data. In addition to internal data leaks, security concerning threats from the outside to the corporate internal network must also be taken into consideration. In fact, at an educational institute in the U.S., a personal device infected with a mobile malicious code interrupted normal service of the institute's internal IP address allocation server (DHCP server), and thus caused a network failure in 2013 (Network World, 2013).

The industries are releasing various products in preparation for new security threats in the changed IT environment. The representative examples are NAC (Network Access Control) solutions and MDM (Mobile Device Management) systems. NAC controls users' network access by identifying authenticated users or forces compliance with security policy through such methods as isolation. MDM is a system for remote mobile device management. MDM software provides a means to make a privileged list about who has which devices and what kind of authorities to access corporate internal applications. In BYOD, NAC and MDM are coming into the limelight as the technologies to prevent it from access to corporate internal infrastructures with lost or stolen devices or personal devices hacked/infected with malware. However, it is insufficient to handle security threats which can occur in BYOD and smart-work environment with the existing solutions because of limitations in these solutions and users' psychological repulsion to the control of personal devices.

In BYOD and smart-work environment, it is necessary to consider a flexible security policy due to numerous types of terminals and their use in diverse contexts. In addition, security policy must be aimed at protecting corporate data by isolating users of abnormal behaviors as well as at ensuring utilization of various personal devices and work continuity. For this, it is urgently required to prepare integrated security solutions and to develop a dynamic access control technology based on the context information gathered.

This paper proposes dynamic access control method based on profiles of individuals or groups to deal with the elements of security threats to internal corporate infrastructures, i.e. data leak in BYOD and smart-work environment. This paper in Chapter II-A discusses technology and product trends as well as security issues possible to occur in the special environments such as BYOD and smart-work. In Chapter II-B, it describes security threats and problems that cannot be resolved with the existing technologies. In Chapter II-C, it explains that integrated security solution is necessary to handle diverse security threats and problems, and thus proposes a dynamic access control technology based on context information as a new method.

II. SECURITY ISSUES AND NEW DYNAMIC ACCESS CONTROL SYSTEM AS A SOLUTION

A. Security Issues for BYOD and Smart-work Environment

The formation of BYOD and smart-work environment, a new IT environment, has been accelerated as a result of the following: implementation of the wireless Internet environment, popularization of smart devices including tablet PC and smart phone, increased use of desktop virtualization and cloud services, increased emphasis on real-time communication, and work continuity. Businesses are actively introducing BYOD in order to improve their productivity and work efficiency and also to reduce the cost of purchasing devices. Gartner predicts that about half of all businesses will introduce BYOD environment by 2017. In addition, even if businesses do not introduce BYOD actively, it would be impossible to block the trend of personal device use in jobs with an exception of some government offices.

As such, in the era of BYOD, internal corporate infrastructures are shifting from closed environment to open environment. This means that personal devices' access to corporate infrastructures is permitted anytime, anywhere. Personal devices can access a company's infrastructures using wireless router (AP) and switch within the company and through mobile communication network, open Wi-Fi and VPN from outside the company.

The shift to an open environment brings such benefits as work continuity and convenience. On the other hand, it has resulted in a number of security threats never before experienced in the past. Above all, as personal devices access a company's internal infrastructures, the risk of the corporate

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

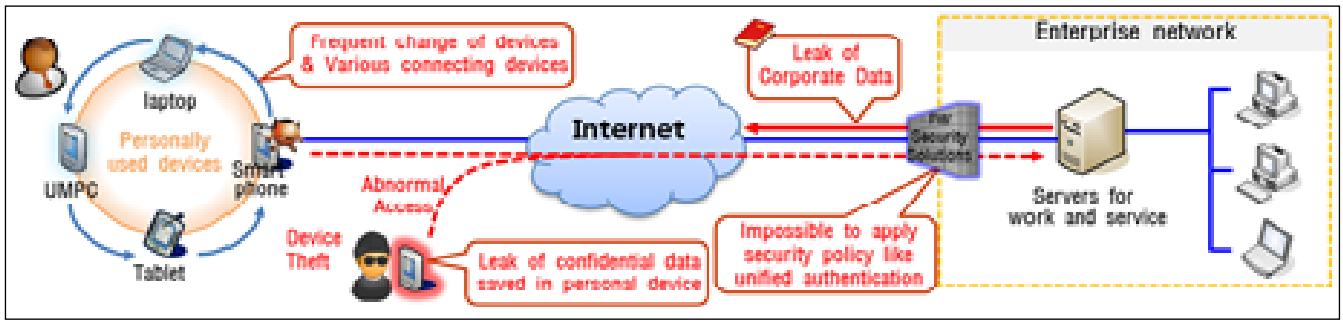

Fig. 2. Security Threat in BYOD and Smart-work Environment

internal data leaks has also increased. It is possible for internal corporate data to be leaked to the outside as a result of personal device loss or theft. In addition, as a personal device infected with malicious codes accesses a company's internal infrastructures through intranet, it may lead to a threat to the company's IT assets. According to the results of Symantec's Honey Stick Project announced in 2012, 70% of personal devices lost were found to have directly accessed personal and corporate services for information viewing. In addition, it was found that 25% of adult office workers in the U.S. had experiences where their personal devices used in BYOD were infected by malicious codes or hacked (ESET, 2012). This verifies that there is a risk for hackers to abnormally access internal corporate infrastructures using normally registered personal devices.

In addition to the risk occurring as a result of corporate data access by personal devices, a factor to increase security risk in BYOD environment is the increased risk of data leaks caused by unskilled security policy implementation by companies introducing BYOD system. According to the Data Protection Trend Report by Acronis Korea in 2013 that contain results of interviews with around 4300 corporate officers from eight countries, 60% of companies are still not establishing security policies in relation to mobile devices. Together with administrators' unskilled operation, the special quality that a company's internal services and data can be accessed anytime, anywhere by personal devices of diverse operating systems and versions adds to the difficulty of security policy setting.

The key security issues and threats in BYOD and smart work environment are categorized as follows: First, it is difficult to identify terminal devices. As each individual may have a number of mobile terminals, such as a laptop PC, a tablet PC and a smart phone, the number of terminals subject to management increases exponentially. Accordingly, fluctuations in management, such as for unregistered terminal devices and devices not accessing corporate data and services for a long period of time, increase. A key security threat that may occur as a result of such fluctuations is ID (account) spoofing. A company's internal services can be accessed abnormally as a malicious user or an external user that is not an employee of the respective company steals a normal user's account with their terminals. Second, it is difficult to identify normal users. Considering the possibility that account information for user authentication can be acquired or spoofed using a lost terminal with automatic login setting, it is difficult to identify whether or not a user is normal or malicious. In addition, the frequent personnel shifts, such as by retirement, employment and long-term business trips, result in changes in the authority and related user information and such changes cause difficulties in management. An example of a security threat caused by this is the illegal acquisition of a normal device. A malicious user or an external user that is not an employee of the respective company can access the company's internal services abnormally using a stolen terminal of a normal user. Third, context information of a terminal device includes access location, access point, status of the device not making any accesses for a long period of time, whether or not the device is stolen, whether or not the name of the device holder has been changed illegally, whether or not the device is subject to jailbreak/rooting, status of the device being infected by malicious codes and illegal private AP installation and connection states. As a company's internal data can be accessed without time and space limitations using personal mobile devices, it is difficult to identify terminal context information as of the above. As a result, internal data leaks can be triggered by a malicious user through abnormal terminal behaviors, such as illegal temporary private wireless AP installation, connection and removal within the company, using a stolen terminal or a spoofed account. Fourth, it is difficult to detect internal data accesses and malicious behaviors as a result of abuse and misuse of the authority. Under the new environment, a malicious external user can access a company's internal service network and infect it with malicious codes by disguising his or her personal mobile device as a normal terminal. In this case, it is difficult to identify the malicious behavior. This, in turn, illustrates that malicious behaviors, such as to access internal system data, and thus to delete or leak the data to the outside or to trigger malicious code infection on them, are possible using authority of a legitimate user (company's employee).

B. Trend and Problems of Existing Technology and Solutions

Security technologies and products that have climbed to the limelight as of late in BYOD and smart work environment, the new IT environment, are NAC and MDM. NAC technology inspects whether or not a user PC (terminal) complied with security policy before it accesses an internal network, and thus controls network access according to the state of the terminal being abnormal. In addition, MDM is a system that provides such functions as remote terminal registration/ management, suspension of lost terminal use and terminal tracking control anytime, anywhere using OTA (over the air) when a mobile device is in 'power on' state.

NAC solution was introduced with a goal to block network

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

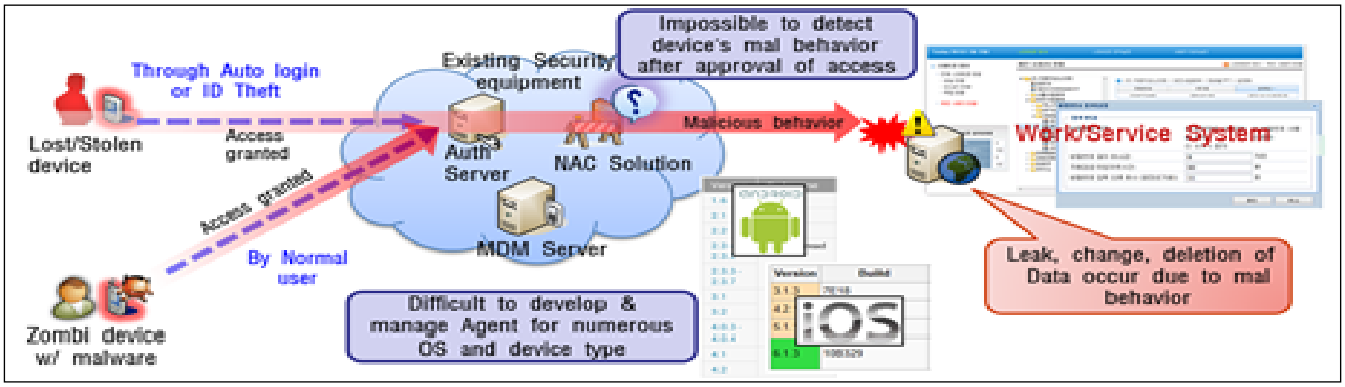

Fig. 3. Limitation of the Existing Solutions for Security Threats in BYOD

access by infected PCs in order to prevent the malicious codes spreading in internal corporate network. The functions of NAC are to control accesses by identifying authenticated users or devices, to define access control policies and to force compliance with the security policies in switches or routers. In other words, the purpose of NAC solution is to prevent terminals without invasion prevention software (such as a vaccine) from accessing network and thus infecting other terminals. As the release began in full scale in 2006, this solution has since been developed further in terms of the functions it offers. At present, NAC solution provides wired and wireless integrated security functions, such as a powerful IP-based control function, a function to authenticate mobile terminals and a function to verify terminal security and integrity. However, although NAC standardization has been attempted, a number of standards are still used in mixture among companies. In addition, NAC solution mainly aims at user authentication and access control. Accordingly, it lacks the function to detect abnormal user or device behaviors, and thus to respond to them following network access. Moreover, as it focuses on authentication based on the registered users, this solution has insufficiency in terms of the function for device authentication. Most of all, NAC solution is intrinsically designed to block network access itself. However, as previously mentioned, BYOD environment has a special security requirement, which is to protect corporate data by isolating users of abnormal behaviors in addition to ensuring the use of diverse personal devices and work continuity. Therefore, NAC solution alone is not sufficient in handling security issues occurring in BYOD environment.

MDM technology is taking the center stage as of late together with NAC. Displaying the fastest growth among corporate mobile software technologies, the global market scale of MDM expanded from $3.5 billion in 2011 to $5 billion in 2012 as a result of the increased necessity of mobile terminal device management. Recently, MDM provides a comprehensively protective function for a variety of channels subject to data leaks, such as operating apps, camera, recorder and Wi-Fi, and, at the same time, a function to administer control on company-wide monitoring and user environment through the central management console.

There are also problems, however, in the access control based on MDM system that provides a function to directly control personal devices in BYOD environment. MDM is an application. Therefore, access control and monitoring of other applications are difficult. In addition, system-level network layer access and behavioral analysis for network data are impossible. Above all, it is difficult to distribute and spread this method because individual users are reluctant about MDM agent installation on their personal devices in demanding their privacy protection. At the same time, as a result of continuous version management on diverse terminals, the related costs increase.

As such, both NAC and MDM have limitations in protecting internal resources of a company in the BYOD and smart work environment. To improve on these weaknesses, an access control method based on a link between NAC and MDM is proposed as of late. This method provides effective network blocking function through limited terminal information collection. However, it still has such limitations as lack of a real-time terminal device status check function and security issues concerning terminals not installed with MDM agent.

C.A Dynamic Access Control System Based on Context Information

While businesses are converting to BYOD and smart-work environment in full scale, security threats in the corporate internal infrastructures such as data leak are pointed out as the biggest obstacle. Some BYOD security issues can be handled with the existing security solutions such as NAC or MDM. However, it is not sufficient. A security solution exclusively designed for BYOD is necessary, especially for the period after the access is granted. That is, it is necessary to be able to detect abnormal behavior of users with personal devices during service use.

For the purpose of having secure BYOD environment, it is required to develop a dynamic access control technology based on context information. In fact, these days the existing security solutions do not have a function to check real-time status of personal devices after users' accessing to internal corporate services. To solve this problem, it is necessary to develop a technology detecting abnormal access and use of terminal devices on a real-time basis. Furthermore, it should solve potential security threat and increase of cost due to the management of terminals without MDM agent. This leads to develop a technology for real-time collection of the context information of devices under agentless mode. Another aspect is that, it is difficult to set a flexible security policy because there are so many types of terminal devices and diverse uses and circumstances in using them. Thus, it is necessary to develop a dynamic access control technology based on the context information gathered.

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

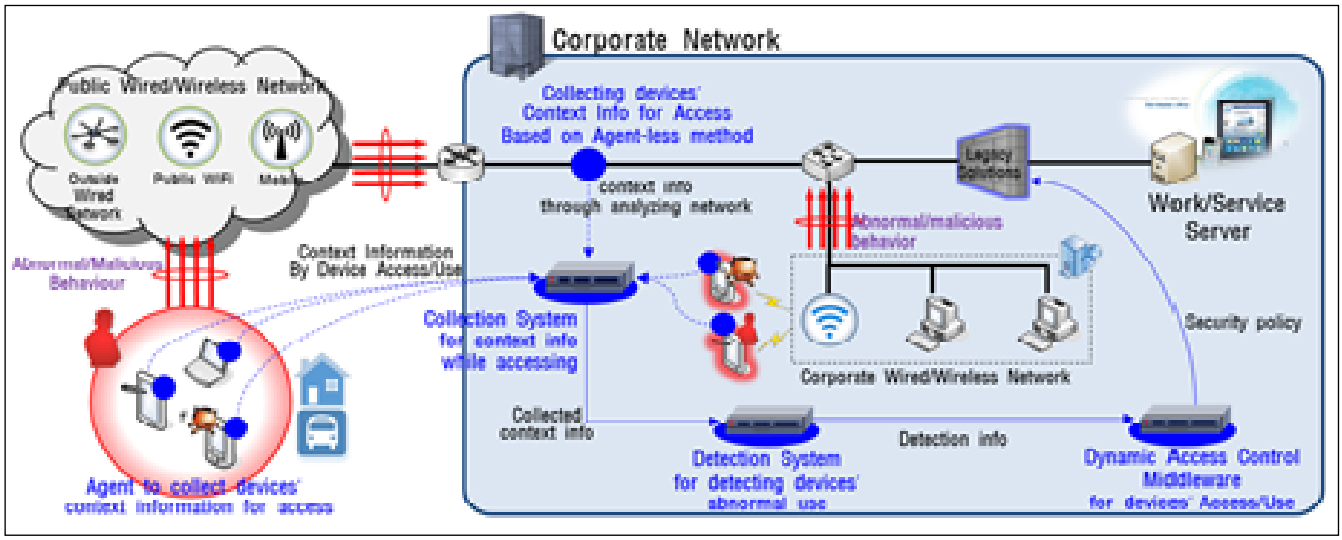

Fig. 4. Context Awareness based Dynamic Access Control System

This paper proposes the dynamic access control system based on context information gathered. This proposed system is comprised of a collection system, a detection system and a control system. This system collects context information of a device under agentless mode. It is to collect context information through network analysis following user authentication when the users' terminal devices try to access a corporate network. The collected context information is analyzed by the detection system, and thus abnormal and malicious behaviors are detected. Detection result is sent to the control system. According to this result, it controls access of devices by legacy security equipment or the new method like dynamic change of access privilege. This process is monitored and controlled until the use of corporate network and service is ended.

In the collection system, the context information is collected basically in the agentless mode and user and device information is extracted through network packet analysis. Under agentless mode, the amount of collectable information is bound to be smaller than that under agent mode. Therefore, user and device information must be collected as much as possible using various methods including DHCP fingerprinting. Agent is installed only if users/devices are detected to do abnormal or malicious behaviors while using networks and thus isolated. These users/devices needs to install agents to retry to access the network since it is necessary to collect information accurately this time. In addition, this policy minimizes agent installation.

In the detection system, users' normal behaviors are saved in the database while each user is profiled doing work. Then, the accumulated data are used in determining users' abnormal and malicious behaviors. For this, profiling of each user is necessary. In this system, the term 'Profile' refers to a set of data with which a specific object can be identified and behaviors of the object can be determined. These are elements that compose real-time context information of each user, such as access time and location, and the user's previous behavior records as well as average and statistics of all users' data within the system. After profiling, abnormal behaviors for access and use of corporate networks/services are detected through comparison with real-time detection data against elements comprising normal behavior patterns.

Lastly, in the control system, access control is carried out according to detection results and policies. This access control includes not only device access control through legacy equipment such as MDM, NAC or firewall, but also access control with new method. For example, like the way that ARP spoofing does, it dynamically controls the access by changing the authority of access.

III. Conclusion

In BYOD and smart-work environment, the new IT environment, the existing technologies alone are not sufficient in handling the new security threats. With the special qualities that BYOD and smart-work environment provide, it has become possible to access internal corporate data using personal devices. The use of personal devices in jobs has become an undeniable trend. Through proper use, this certainly brings benefits to companies in terms of improved work efficiency and cost reduction. However, as much as the benefits enjoyed, it amplified security-related difficulties for IT departments in companies. A number of new security issues have appeared including the control of devices used to access data, in addition to the accessing time and location.

Nevertheless, the legacy solutions have limitations due to the fact that it is the personal devices. Users concern about their personal information leaks and they have psychological repulsion towards installing the agent. Accordingly, a study on the dynamic access control technology based on context information is required. In other words, operation will not be possible with the conventional method of access control administered on the basis of specific conditions. Thus, it will be necessary to first permit the network access and to profile users' behaviors, and then to block accesses that deviate from the range of normal behaviors while monitoring those behaviors.

In the future we will study on technologies to detect abnormal use of corporate services and resources by individuals or devices and on dynamic control technologies for such system.

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

ACKNOWLEDGMENT

This work was supported by the IT R&D program of MSIP/KEIT(Ministry of Science, ICT and Future Planning/Korea Evaluation Institute Of Industrial Technology). [10045109, The Development of Context-Awareness based Dynamic Access Control Technology for BYOD, Smartwork Environment]

REFERENCES

[1] K. W. Miller, "Security and Privacy Considerations," in *IT Professional*, vol. 14, No. 5, 2012, pp. 53–55.
[2] *Guide to BYOD Strategy*, IDG Deep Dive, IDG Korea, 2012.
[3] V. Frias-Martinez, J. Sherrick, S. Stolfo, A. D. Keromytis, "A Network Access Control Mechanism Based on Behavior Profiles," 25th Annual Computer Security Applications Conference, Honolulu, Hawaii, 2009.
[4] V. Frias-Martinez, S. Stolfo, A. D. Keromytis, "Behavior Based Network Access Control: A Proof-Of-Concept," Intrusion Detection Systems Lab, Columbia University, 2010.
[5] PacketFence, (2008-2013). PacketFence Developer's Guide [Online]. http://www.packetfence.org
[6] M. Finneran, "BYOD Requires Mobile Device Management," in informationweek, 2011.
[7] *ForeScout CounterACT: Virtual Firewall*, ForeScout Technologies, Inc., 2012.
[8] *Choosing a Network Access Control (NAC) Solution That is Right for Your Netwrok*, Whitepaper, ForeScout Technologies, Inc., 2011.
[9] UserAgentStrings.com. (2005-2011). List of User Agent Strings. [Online]. Available: http://www.useragentstring.com/pages/useragentstring.php
[10] *Architecture Guide for System Center Mobile Device Manager,* Microsoft Corporation, 2008.
[11] *802.1X: PORT-BASED AUTHENTICATION STANDARD FOR NETWORK ACCESS CONTROL (NAC)*, Juniper Networks, Inc., 2010
[12] J. Wilson, "Network access control has evolved significantly, worth a fresh look," Whitepaper, Infonetics Research, Inc., 2009.
[13] *NAC 2.0*, Geninetworks, 2011.
[14] R. Yampolskiy, "Behavioral Modeling: an Overview," *American Journal of Applied Sciences*, vol. 5, no. 5, pp. 496–503, 2008.
[15] *Cisco TrustSec How-To Guide: ISE Profiling Design Guide*, Cisco, 2012.