Relational Characteristics of Maliciousness and Hacker in a Cyberattack

Jin-keun Hong, Jung-Soo Han

***Abstract**: Cyber security threats are increasing day by day. However, this threat is sophisticated and intelligent. Therefore, artificial intelligence-based learning algorithms are emerging to effectively respond to cybersecurity threats. However, there has yet to be any interest or approach in studying the likelihood of an attack by efficiently analyzing the causes of the attack by individuals, religious groups, and hackers subordinate to state agencies.*

An idea in this study is to analyze hacker tendencies. And the link to how hacker tendencies affect attacks is being sought by the intelligence algorithm, which provides a sample of the predictive model as a preliminary study.

Therefore, this study required a study on what an attacker's individual is influenced by, how a hacker subordinate to a religious group is affected by an attack from a religious group, and how a hacker subordinate to a national institution is affected by an attack from a state institution. In this study, however, we briefly focused on the factors that affect these attacks. In this study, we proposed an intelligent simplified model that predicts threats with the goal of producing results on whether or not an attack by combining the pattern of attack with inputs and weighing factors. Therefore, three groups of attackers were analyzed. From this, a simple intelligent algorithm model was presented The results of this study are expected to help derive the correlation between future hacker attack propensity analysis and intelligent algorithm. Future research will implement a threat analysis system that can more specifically derive attack propensity factors and apply them to intelligent algorithms (weights, f functions) to determine whether an attack is possible or not.

***Keywords** : cyberattack, learning, hacker, analysis, malicious.*

I. INTRODUCTION

As the threat of cyberattacks has become more sophisticated and intelligent in recent years, research is actively conducted to predict security threats based on the AI Deep Learning model.

The U.S. federal government has presented a roadmap for the development of cybersecurity technologies along with the enhancement of cybersecurity in national cybersecurity strategies.

When looking at the materials presented, the operations for cybersecurity are evolving. The question is how to learn constantly and efficiently about threats to cyberattacks based on artificial intelligence. And how to effectively analyze this vast amount of relevant big data. And the key to the threat analysis model is how to optimize the identification of malicious patterns in this Big Data. By the way, research into this threat analysis model can make better use of the information provided primarily in the deep web environment than in the Internet environment. Therefore, we would like to look at the Deep Web and related studies on cybercrime and look for ways to predict the threat of cyberattacks.

Ryan Williams et al. present about hacker forum exploit collection and classification for cyber threat intelligence [1]. Their interest is in how to effectively design about web crawlers, application of deep learning algorithms, and, detection and visualization of the collected exploits in the Deep Web. These studies are typically characterized by considering a deep learning algorithm as a general approach to deep webs.

Mengyun Tang et al. review deep learning techniques in breaking text-based on captchas and designing image-based on captcha [2]. The proposed Captchas is based on deep-learning technology and has been successful in attacking Roman-based texts distributed by 50 international websites and 3 Chinese Captchas. The study suggests an image-based style-space security problem, which suggests that text Captchas is unsafe. Therefore, Mengyun et al. Were interested in developing image-based captchas using deep learning technology.

S Sandhya et al. present about assessment of website security by penetration testing with wireshark [3]. The study is concerned with topics that use the Wireshark tool to identify vulnerabilities. This paper examines the various tools available for penetration testing and provides basic penetration testing practices.

Taro Ishitaki et al. [6] studied the application of deep recurrent neural networks for prediction of user behavior in tor networks. In this paper, they provide an interest in neural network for predicting user behavior in tor environment. DRNN based deep learning neural learning algorithm is applied to predict user behavior.

Gerorge Hurlburt review about shining light on the dark web [5]. This paper reviews relation of deep web content such as private web, contextual web, dynamic content, limited access content, and access control techniques.

Tetsuya Oda et al. present neural network based on user identification for tor network [6]. The characteristics of the Tor network are to provide anonymity to the user. With

Revised Manuscript Received on September 25, 2019

Jin-Keun Hong[*1]**,** Division of ICT, Baekseok University, Cheonan City, South Korea. Email: jkhong@bu.ac.kr

Jung-Soo Han[2]**,** Division of ICT, Baekseok University, Cheonan City, South Korea. Email: jshan@bu.ac.kr

Tor, users can avoid the principle of non-repudiation. There have been many studies to detect malicious users in Tor network. In this study, they also apply the deep learning neural network learning model which is applicable in Tor network. The client uses the Tor network to send data to the Tor server and analyze it through Wireshark.

Taro Ishitaki et al. [7] are presented the application of neural networks and Friedman tests in tor networks. In this paper, we present the Friedman test for the application of neural networks and user identification in the tor network. They are conducting experiments on concealed units considering tor clients and surface web clients.

In addition, Taro Ishitake et al. are proposed a neural network for intrusion detection in tor network [8]. This study also applies neural network for intrusion detection in Tor network. They use a neural network that is propagated to Bac and configure Tor server and Deep Web client. Back is derived from neural circuit model and it is used for intrusion detection.

Poonam Patel et al. [8] are studied a theoretical review of social media usage by cyber criminals. In this paper, they are approaching forensic and forensic investigation methods with the relation of hacker and SNS. This study starts with the question of legal liability and the interest in tracking crucial evidence, such as when and where.

Andrew J. Park et al. present about hackers hedging bets [10]. The online hacking forum is a community where information exchange and related tools can be purchased to prevent various crimes such as hacking, credit card fraud and money laundering. The topic of research on the hacking forum is the topic of interest.

Ivan Del Pozo et al. are presented social engineering in psychology to information security [11]. In this study, they are interested in the relation between hacking forums and victims of cybercrime. In fact, there has been a lack of access to or interest in research. In this respect, this study is an interesting study.

Ericsson Marin et al. studies mining key hackers on dark web forums [12]. In this paper, they are investigating a method to verify core hackers based on reputation. In order to identify key hackers, related contents have been used or SNS and sequence based on analysis methods have been performed. In order to identify the key hackers, an optimized method is proposed in comparison with machine learning.

Under this background, this study looked at the nature of individual hackers, individual hackers affected by religious groups, and individual hackers is dependent on national institutions, and presented a model for cyber threat detection of intelligent learning models based on these attributes.

Also the research of these related researchers on Deep Web or Dark Web has attracted interesting interest in our research. Therefore, this study will examine the characteristics of Deep Web and Dark Web.

We also analyze the tendencies of attackers. We look at what kind of tendency the state-led attackers have in hacking. Also, what kind of proprietors are the attacker individual? Where does the attack start? What are the psychological variables that cause attacks? This study was conducted with interest in this topic.

II. CHARACTERISTICS OF HACKER IN CYBERATTACK

Where does the psychological motive for hacker's attack propensity start? First, we examine the major psychological factors that cause cyberattacks.

A. Individuals who are dependent on the country or government agency

Government agencies and individuals who are subordinate to the state are used as an accessory to government-led offenses. This is the type of attackers that are like industrial espionage or bank hairy. In the case of China, joining a Christian or Islamic group is seen as a threat to national security or public safety. If so, individuals belonging to these organizations may be potential targets that are attacked by hackers employed by the state or government agencies.

NGOs and religious leaders of border states can also be targets of attacks. Therefore, an individual employed by a state or a government agency is only an agent for attack beyond the level of individual values and personality.

In India, religious identity is emphasized as politics which is centered around Hindu nationalists. For them, Muslim minorities are subject to oppression. In that case, hackers hired by the government are tools to attack them. Hackers, therefore, can be sponsored by the government and attack local governments, foreign terrorists, anti-government personnel and major corporations against the government. Those who are attacked by hackers are exposed to sensitive information, including credit card information, medical record information, and identity information, and are seriously affected by actual financial or reputation.

If a state agency attacks an individual or company, the factors vary. In this case, the main factor is the use of this method when the domestic situation of the national institution deteriorates and the internal issue or problem is to be transformed to the outside. It is also used as a solution to the problem of security and conflicts in the country. When the actual state agency is in this situation, factors considered for cyber security activities are required to establish tactics, methods and procedures to carry out cyberattacks. In addition, details for specific operational performance are defined.

An attacker who is ordered by a government agency performs an operation for attack first. The attacker decides to what range to attack. The attacker also decides which attack tool to use. In addition, the attacker analyzes the level of access to the exploit. The attacker decides how much manpower is needed for this attack, how much resources and time will be needed. The tool used for the attack will decide whether it is a collectible tool or a known tool.

However, in order to increase the actual attack effect, there is a possibility that the attacker may apply the tool that has been used before. From the perspective of the analyst, look at the various factors to find the trail of the attacker. These factors include what language the malware is in, how long it takes to attack, and how the binary build path is. From this we look for similarities with previous attacks.

The most important of these factors is motivation to attack. It is most important to identify the immediate cause of the attacks performed by hired attackers. If so, what information should analysts use to identify attacks based on their motives? The information needed for analysis includes spear phishing messages, attached contents, and website information used in attacks. According to the cyber security research analysis, the Chinese government recently seizes sensitive information from the military security and economic aspects through the spear phishing attacks targeting the national institutions, government organizations and private organizations in Asia.

Hackers sponsored or hired by the Chinese government have cyber-attacked Russian defense companies and energy companies. They cyber-attacked the government of Mongolia and cyber-attacked Korean IT companies, Japanese government, Taiwanese media and government agencies, Vietnamese government and individuals against the Chinese government in Hong Kong.

B. Individuals subordinate to religious organizations and Individual tendency

Individuals belonging to religious groups seek to discover their presence within the group. These religious groups may transcend national boundaries and transcend gender or political tendencies. The shared values pursued in the religion to which the individual belongs solidify the membership of the group.

The stronger the uniqueness of a religious group to which an individual belongs, the stronger the conflict or competition among other factions within the same religion. Conflicts and conflicts within religious groups can start from the superiority of their group. Differences between these groups also cause conflicts and social conflicts. It is difficult for an individual's values attached within a religious group to deviate from the ideals and perceptions that the group pursues.

Therefore, one individual in the group is influenced by the religious values and interests of the group and can sometimes seek aggressive and sometimes unreasonable choices. Cyber terrorism caused by a religious group is a kind of hostile attack that is mostly caused by a religious group's biased value system. These attackers are based on the ideology of religion and aim to bring fear and anxiety to the target.

Therefore, one person who is subordinate to a religious group can be forced by the others from the group or participate in cyber terrorism voluntarily. A voluntary attacker will engage in hostile attacks and participate directly in malicious activities of online. The aggressiveness of attackers who are subordinate to religious groups is strongly influenced by the religion of the group and the customs based on them. Motives to induce malicious behavior by these people may include financial interests, political interests, and competitive or vengeful as well as divine religious beliefs.

An individual who is subordinate to a religious group can be controlled and encouraged on the one hand by the norms or customary actions that the group is aiming even in cyberattacks. The value system of a religious group affects the perception of how an individual in a group understands cyberattacks, how to beautify cyberattacks and free them from moral judgments. Therefore, their negative perception of other religious groups can induce a strong sense of belonging within the group and affect group members in behaving maliciously.

III. ATTACK ANALYSIS MODEL OF MALICIOUSNESS OF HACKER AND CYBER ATTACK

This journal uses double-blind review process, which means that both the reviewer (s) and author (s) identities concealed from the reviewers, and vice versa, throughout the review process. All submitted manuscripts are reviewed by three reviewer one from India and rest two from overseas. There should be proper comments of the reviewers for the purpose of acceptance/ rejection. There should be minimum 01 to 02 week time window for it.

The original intent includes not only the need for any action, but also the decision as to whether or not an action will occur. However, the evil intentions caused by the attacker occur when the actor tries to harm or thinks that his actions will lead to negative or adverse consequences. In fact, malicious intent is related to the intention of crime as a criminal consciousness. Therefore, malicious programs purposely used to compromise or destroy an IT system are inherently evil, regardless of the motivation to initiate the attack.

Therefore, it is related to human evil intent that malicious code is intentionally distributed by an attacker. This act may be carried out by individuals employed by the state or governmental authority or by persons dependent on religious groups.

However, this behavior may be relatively malicious or good depending on the degree of social, cultural, political, religious value system or acceptance that the society accepts. However, the malicious intent to deal with someone like this can be confirmed if the motive for the attack is known, although it is subjective.

If so, what is directly influenced by the evil deeds of an individual who is subordinated by a religious group, state, or government agency? The evil intentions of cyberattacks originate from personality traits or mental instability. This evil intention is influenced by the individual's feelings and self-awareness. It is also influenced by the attitudes and behaviors of individuals responding to specific events and is influenced by behaviors and borderline propensity in interpersonal relationships. It is also influenced by individual values, social norms, and social perceptions of cyberattacks.

Also what are some of the symptoms of maliciousness

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

caused by this malicious intent? These types of symptoms include symptoms that are caused by individuals, symptoms that are caused by the group, and symptoms that are caused by the state or government agencies.

The attacker looks for hacking tools and malicious source code. They also find helpful notes to share and share stolen data. The hacker learns the techniques from the hacking messages acquired through Internet relay chat, receiving the attack technology through the black market.

The system of the attacked industry is as follows: Entertainment industrial systems, chemical industry systems, food and agricultural industrial systems, metal and mining industry systems, telecommunication industry systems, aerospace and defense industry systems, construction industry systems, energy industry systems, education industry systems, Systems, high technology, communication and transportation industry systems, and so on.

APT core attack groups are as follows: APT1 (China), 3 (China), 5, 10 (China), 12 (China), 16 China, 17 China, 18 China, 19 China), 30 (China), 32 (Vietnam), 33 (Iran), 34 (Iran), 37 (North Korea).

Major attack types are as follows: Backdoor installation, Zero-day exploit attack, Phishing mail, macro attack, Non-patched vulnerability attack, Spear phishing attack, Web mail attack, SNS storage server attack, C & C attack, Attack on Adobe Flash Vulnerability, Korean word processor vulnerability attack in Republic of Korea.

The following types of malware are used by APT37, which is supported by North Korea: KARAE, Soundwave, Zumkong, Ricecurry, Coraldeck, Pooraim, Slowdrift, Milkdrop, Gelcapsule, Dogcall, Happywork, Ruhappy, Shutterspeed, Winerack and so on.

In this study, we investigate the tendency of attacker and cyberattack. For this purpose, the related diagram can be expressed as follows in figure 1. It is necessary to understand the impact of attacker's personality on cyberattack.

A. Simplified Analysis Model due to Individuals who are dependent on the country or government agency

The following diagram illustrates attack analysis model of government's tendency for cyberattack in Figure 1. The influence of cyberattacks on the culture of the nation can be changed depending on whether it is hostile or friendly to the cyberattack. The impact of the government on cyberattacks can vary depending on whether the physical countermeasures against over activity are reasonable. The impact of cyberattacks on the organization can be affected by the high or low frustration of the members of the government. The impact of a cyberattack can be different when the country is too strong in its own sense of bond compared to other countries. The influence of government social politics on cyberattacks can vary depending on whether they are friendly or hostile in relations with other countries.

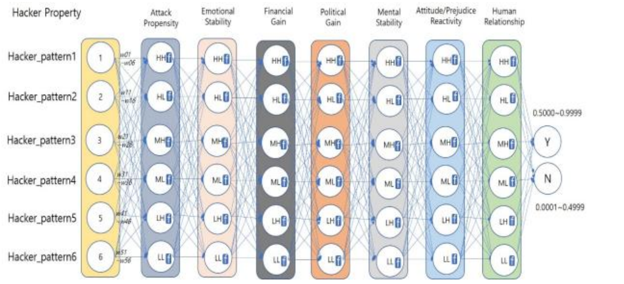

Fig. 1. Learning model of hacker who are dependent on the country for attack analysis

Where w1~w56 is weight factor for relational coefficient between input and first hidden layer and f can be used rectified linear unit (ReLU) function. Also learning weighting stage of evaluation of attack propensity is 1st hidden layer, stage of evaluation emotional stability is 2nd hidden layer. 3rd hidden layer is dependency by financial gain, and 4rd hidden layer is evaluation of political gain. 5th hidden layer is stage of evaluation of mental stability. 6th hidden layer is stage of evaluation of attitude and prejudice reactivity. 7th hidden layer is stage of evaluation of human relationship.

B. Simplified Analysis Model due to Individuals subordinate to religious organizations and Individual

The following diagram illustrates case of attack analysis model for an attacker's tendency. Based on the six patterns of hackers, it is shown that hackers have a tendency to attack propensity, emotional stability, mental stability, attitude and prejudice Attitude / prejudice reactivity, and interpersonal relationship (human relationship).

Where learning weighting stage of evaluation of individual attack property is 1st hidden layer, stage of evaluation of emotional stability is 2nd hidden layer. 3rd hidden layer is dependency by evaluation of mental stability, and 4rd hidden layer is attitude and prejudice reactivity. 5th hidden layer is stage of human relationship.

Attackers may have different impacts on the cyberattack depending on the tendency of the attack to be sensitive to certain events. In addition, attackers may have different effects on cyberattacks depending on the degree of unstable emotions. Also attackers may have different impacts on cyberattacks depending on the degree of emotional stability. Attackers may have different impacts on cyberattacks depending on their attitudes and prejudices about specific incidents. Attackers may have different impacts on cyberattacks depending on their interpersonal abilities in Figure 2.

Therefor for individuals, if personality is open, weights can be set by considering the possibility of attack relatively low. Whether an individual's conscience is moral or not can also be weighted by considering the possibility of attack. The weight can be set when determining the possibility of attack considering the stress level of the individual. If there is a narcissistic psychic force, the probability of attack is high, and the weight can be set considering this.

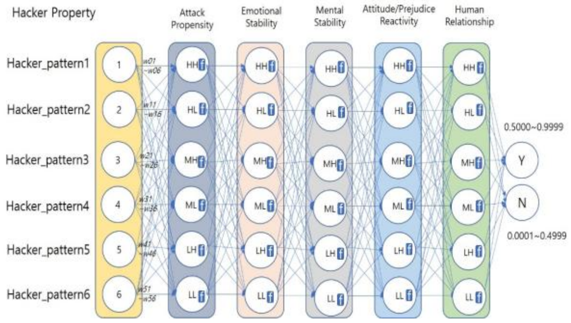

Fig. 2. Learning model of hacker subordinate to religious organization for attack analysis

In Figure 3, attackers may have different effects on the cyberattacks according to the tendency of the religious belief among the social cognitive characteristics according to the specific events. Attackers may also have different impacts on cyberattacks, depending on whether religious beliefs are ethical in understanding the attack. Attackers can have different effects on cyberattacks depending on their religious beliefs. Attackers can have different effects on cyberattacks, depending on whether religious groups support terrorism directly or indirectly. Attackers can have different effects on cyberattacks, depending on whether family members respond positively to terrorism.

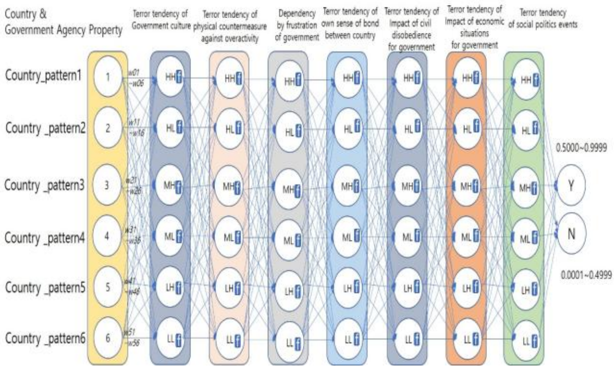
Country & Government Agency Property
Terror tendency of Government culture
Terror tendency of physical countermeasure against overactivity
Dependency by frustration of government
Terror tendency of own sense of bond between country
Terror tendency of Impact of civil disobedience for government
Terror tendency of Impact of economic situations for government
Terror tendency of social politics events
Country_pattern1
Country _pattern2
Country _pattern3
Country _pattern4
Country _pattern5
Country _pattern6
1
2
3
4
5
6
w01~w06
w11~w16
w21~w26
w31~w36
w41~w46
w51~w56
HH f
HL f
MH f
ML f
LH f
LL f
0.5000~0.9999
Y
N
0.0001~0.4999

Fig. 3. Learning Diagram of hacker property subordinate to religious organization for attack analysis

Also learning weighting stage of evaluation of terror tendency of government culture is 1st hidden layer, stage of evaluation of terror tendency of physical countermeasure against overactivity is 2nd hidden layer. 3rd hidden layer is dependency by evaluation of dependency by frustration of government, and 4rd hidden layer is evaluation of own sense of bond between country. 5th hidden layer is stage of evaluation of impact of civil disobedience for government. 6th hidden layer is stage of evaluation of impact of economic situations for government. 7th hidden layer is stage of evaluation of social politics events.

IV. CONCLUSION

In this paper, it is to analyze hacker tendencies. And the link to how hacker tendencies affect attacks is being sought by the intelligence algorithm, which provides a sample of the predictive model as a preliminary study. Therefore, this study required a study on what an attacker's individual is influenced by, how a hacker subordinate to a religious group is affected by an attack from a religious group, and how a hacker subordinate to a national institution is affected by an attack from a state institution.

In this paper, we proposed an intelligent simplified model that predicts threats with the goal of producing results on whether or not an attack by combining the pattern of attack with inputs and weighing factors. The results of this study are expected to help derive the correlation between future hacker attack propensity analysis and intelligent algorithm. Future research will implement a threat analysis system that can more specifically derive attack propensity factors and apply them to intelligent algorithms (weights, f functions) to determine whether an attack is possible or not.

ACKNOWLEDGMENT

This paper is sponsored of project funding of Industrial Academia Cooperation in Baekseok University.

REFERENCES

1. Ryan Williams, Sagar Samtani, Mark Patton, Hsinchun Chen, “Incremental Hacker Forum collection and classification for proactive cyber threat intelligence,” in ISI2018. https://doi.org/ 10.1109/ISI. 2018.8587336
2. Mengyun Tang, Haichang Gao, Yang Zhang, Yi Liu, Ping Zhang, Ping Wang, “Research on Deep Learning Techniques in Breaking Text Based Captchas and Designing Image based Captcha,” IEEE Transactions on Information Forensics and Security, 13(10), pp. 2522-2537, 2018. https://doi.org/ 10.1109/TIFS.2018.2821096
3. S Sandhya, Sohini Purkayastha, Emil Joshua, Akash Deep, “Assessment of website security by penetration testing using wireshark,” in ICACCS2017, https://doi.org/10.1109/ICACCS. 2017.8014711
4. Taro Ishitake, Ryoichiro Obukata, Tetsuya Oda, Leonard Barilli. “Application of deep recurrent neural networks for prediction of user behavior in tor networks,” in WAINA2017, https://doi.org/10.1109/ WAINA.2017.63
5. George Hurlburt, “Shining light on the dark web,” IEEE Journal & Magazines, pp. 100-105, 2017, https://doi.org/10.1109/MC.2017.110
6. Tetsuya Oda, Ryoichiro Obukata, Masafumi Yamada, Taro Ishitake, Masahiro Hiyama, Leonard Barolli, “A neural network based user identification for tor network,” in CISIS2016, https://doi. org.10.1109/CISIS.2016.89
7. Taro Ishitaki, Tetsuya Oda, Leonard Barolli, “Application of neural networks and friedman test for user identification in tor networks,” in BWCCA2015, https://doi.org/10.1109/BWCCA.2015.88
8. Taro Ishitake, Donald Elmazi, Yi Liu, Tetsuya Oda, Leonard Barolli, Kazunori Uchida, “Application of Neural Networks for Intrusion Detection in Tor Networks,” in IEEE 29th ICAINAW2015, https://doi.org/10.1109/WAINA.2015.136
9. Poonam Patel, Krishnan Kannoorpatti, Bharanidharan Shanmugam, Sami Azam, Kheng Cher Yeo, “A theoretical review of social media usage by cyber criminals,” in ICCCI2017, https://doi.org/10.1109/ICCCI.2017.8117694
10. Andrew J. Park, Richard Frank, Alexander Mikhaylov, Myf Thomson, “Hackers hedging bets – a cross community analysis of three online hacking forums,” in ASONAM2018, https://doi.org/10.1109/ ASONAM.2018.8508613
11. Ivan Del Pozo, Mauricio Iturralde, Felipe Restrepo, “Social engineering – application of psychology to information security,” in FiCloudW2018, https://doi.org/10.1109/ASONAM.2018.8508613
12. Ericsson Marin, Jana Shakarian, Paulo Shakarian, “Mining key hackers on darkweb forums,” in ICDIS2018, https://doi.org/ 10.1109/ICDIS.2018.00018

AUTHORS PROFILE

Jin-Keun Hong who serves professor in division of ICT in Baekseok University of South Korea. He was registered an excellent researcher at Marquis Who's Who in the world, IBC, and ABI human dictionary according to research results of ICT & Security. His research topic is convergence information security technology. Especially, he is focusing on C-ITS and future security technology prediction.

Jung-Soo Han received a BS, an MS, and a PhD in Computer Engineering from Kyung Hee University, Republic of Korea. Since 2001, he has been a Professor in the Division of Information & Communication Technology, Baekseok University, Cheonan City, Chungnam, Republic of Korea. In 2014, he researched Convergence IT and Creative Education Methodology at California State University Fullerton as an Exchange Professor. His research topics include Data Mining, Contents Planning, 3D Modeling and CBD, Telemedicine, Knowledge-based Decision Support Systems, Intelligent Systems, Convergence, HCI, and Recommendation Systems. He has edited books on computer science and convergence technology. He serves as Executive Editing Director of the International Conference on Convergence Content (ICCC), as General Co-Chair of the International Conference on Digital Policy & Management (ICPDM), as General Co-Chair for steering committees of the International Conference on Convergence Technology (ICCT), as Workshop Chair of the International Conference on Information Science and Application 2013, as Workshop Chair of the 2nd International Conference on IT Convergence and Security 2012, as Vice President of the Korea Contents Association, as Vice President and a member of the Editorial Committee of the Society of Digital Policy & Management, and as Vice President of the Editorial Committee of the Korea Contents Association.