Inf Syst E-Bus Manage
DOI 10.1007/s10257-017-0347-x

ORIGINAL ARTICLE

What's your real age? an empirical analysis of identity fraud in online game

Daehwan Ahn[1] · Seongmin Jeon[2] · Byungjoon Yoo[3]

Received: 15 January 2015 / Revised: 15 July 2015 / Accepted: 7 September 2015

Abstract In this paper, we empirically examine the ID fraud problem in online game. We analyzed over 260,000 users' behavior using terabytes of big data. The results of the econometrics analysis showed that the behavior pattern of group around 40 years old was very similar to that of teenagers. Considering that the game used for the analysis is a game for young users, this means that some of the users in the group around 40 years old may be teenagers who have stolen the parent's ID. In addition, we performed discriminant analysis and log traffic analysis to estimate how many young users were using their parent IDs. As a result, about 47% of the users around 40 years old were found to be teenager users. Also, behavior patterns of users who are estimated to be teenagers have been found in other age groups.

Keywords Virtual world · Online game · Identity fraud · Big data · Classification system

✉ Seongmin Jeon
smjeon@gachon.ac.kr

Daehwan Ahn
penris32@snu.ac.kr

Byungjoon Yoo
byoo@snu.ac.kr

[1] College of Business Administration, Seoul National University, Seoul, South Korea

[2] College of Business, Gachon University, Seongnam, South Korea

[3] Graduate School of Business, Seoul National University, Seoul, South Korea

Published online: 17 June 2017

1 Introduction

With the development of information technology, a platform for various virtual worlds has emerged. A number of remote users have become able to interact mutually through avatars in online systems in these virtual worlds (Castronova 2007). According to the study by Bell (2008), a virtual world is defined as "a synchronous, persistent network of people, represented by avatars, facilitated by networked computers." As MMORPGs provide new patterns of collaboration and social interaction, the games have become interesting examples of virtual worlds analyzed as a research topic (Assmann et al. 2010; McKenna et al. 2011a; Roquilly 2011).

MMORPG is categorized as a genre of online role-playing game in which a number of game players interact with one another (MMORPG, n.d.). Game players are expected to choose a character in a virtual world and control many of that character's actions, primarily aiming to grow the chosen character. Most MMORPGs feature a character growth system where players acquire experience points for such actions and use those points to reach higher levels of the character. High-level characters are likely to have more capabilities in the game. Normally, battles with monsters and the completion of missions or quests are the typical ways to earn experience points. The purchase of "items" is another method to acquire experience points in most MMORPGs. Players may also team up with other players in order to level-up rapidly. The players obtain virtual items and currency that have tangible value in the virtual world.

The market for MMORPGs, including the United States, has grown exponentially. According to the Wall Street Journal (2011), revenue of MMORPGs since 2009 has increased by 35% to $2.6 billion in 2011. World of Warcraft (WoW), one of the most widely-known MMORPGs, had more than ten million subscribers as of February 2012. The MMORPG is recognized as the highest generator of cash among game genres (Digi-Capital 2011). WoW players typically pay $12.99–14.99 in monthly fees. More than 20 million users are estimated to be paying MMORPG subscribers around the world.

In order to provide rating guidelines for games, classification systems are used to control user access for age appropriateness. The systems in many cases follow the content ratings provided by organizations such as the Entertainment Software Rating Board (ESRB). Ratings regarding entertainment software tend to be categorized as Everyone, Teen (ages 13 and older), Mature (ages 17 and older), and Adults Only (ages 18 and older). The criteria for this categorization include the level of violence, gambling, sexual content and strong language (ESRB 2014). The classification systems for MMORPG are supposed to identify a user's age and limit her or his playtime and ability to purchase items. Since April 2011, the Chinese government has started to regulate online game operators to implement a "game fatigue system" to encourage users under 18 to play less than 3 h per day (ChinaHearSay 2011). The South Korean government has also taken action to curb online game addiction by making a "shutdown" law, forbidding users under 16 from playing online games from midnight to 6 a.m. Furthermore, the South Korean government has signed into law a "cooling off" system to control the hours when an individual user can play during a 24 h period (Forbes 2012; Device 2012). Online game players in China are required to register under their real name and present their identity number to verify that they are older than 18. However, results of a survey showed that about 15% of players under 18 had registered with a parent's ID number when signing up so as not to be affected by the control system (ChinaHearSay 2011).

The purpose of this study is to test the classification system of an MMORPG. The game industry has seriously debated the issue of real identity in MMORPG and considers the regulations related to this issue as a critical one. In this study, we have performed tests to determine behavioral differences among age groups in an MMORPG by analyzing a micro-transactional data set which was received from one of Korea's leading online game publishers. The research setting can be said to be ideal in that the MMORPG is open to anyone wishing to register, although there are restrictions on the purchase of items for players under 14. Our results show the possibility of identity fraud. In particular, our econometric analysis shows that the group consisting of individuals around 40 years old is classified together with the group of those under 14. According to additional discriminant analysis and log traffic analysis, about 47% of the users around 40 years old were found to be teenager users.

Only a few studies, including those by McKenna et al. (2011b) and Kozinets (2010), have dealt with identity and social movements in MMORPGs. Specifically, McKenna et al. (2011b) presented a multi-dimensional conceptual framework to identify social movements using the example of behaviors of gay and lesbian groups in the virtual world. Contrarily, this study finds discrimination among the behaviors of various age groups through empirical analyses of big data set accumulated by actual transactions.

The remainder of this paper is organized as follows. Section 2 reviews previous studies regarding MMORPGs and identity fraud. Section 3 presents the data collection procedure and descriptive statistics about our data set. Section 4 describes the method and model used to compare the behaviors of the age groups. Sections 5 and 6 illustrate the results and robustness checks individually. Section 7 presents conclusions and their implications.

2 Literature review

Our study is closely related to previous research that discussed virtual worlds, MMORPGs and identity fraud. First, the emergence of virtual worlds enables a number of people to interact with one another in an online world. Virtual worlds provide new forms of social interactions by supplying virtual spaces in which social functions work. With the advancement of virtual world-related technology, more social movements have been organized through virtual worlds which are becoming more and more realistic. Furthermore, the use of virtual worlds through the Internet enables social movements to engage in collective actions with global reach (McKenna et al. 2011a). In this virtual world, each individual is able to take on an alternate persona or personae at the same time (Barfield 2006). Previous papers have attempted to define the virtual world Gensollen (2007) as a tool that "projects an identity into a generated three dimensional reality" or an "interactive computer simulation." Items such as armor, space stations, and condominiums for avatars are able to be transformed to bytes of digital codes and changed into a physical medium (Rheingold 2000). A virtual world is likely to constitute a prosperous and sustainable place where communities of users who are connected online continue interacting with one another. The community may become a strong network when users share a bond in regard to key commonality like personal interest or loyalty (Shankar and Bayus 2003; Lazarus 1993; Federal Trade Commission 2010).

Second, several studies in the information systems (IS) field have tried to examine MMORPGs. According to the research carried out by Alemi (2007) the avatars representing the users in games behave differently from the users themselves in the real world. The study proposed a two-tiered justice system of both the In-Game Justice System and the Real World Justice System in order to provide a means to resolve conflicts which arise between the two worlds. Users can customize their avatars by modifying the elements provided by the game developers. In most MMORPGs, a number of users continue to evolve their character avatars in the virtual world. MMORPG companies build communities diverse enough to attract sufficient user motivation to become part of a virtual world (Roquilly 2011). The mechanism of network externalities is likely to get involved in this context. Network externalities work very effectively when the company is able to build a game diverse enough to meet various requirements (Shy 2001; Katz and Shapiro 1985; Farrell and Saloner 1985). Interactions between the virtual and real worlds can be identified by Real-Money Trading (RMT), an economic activity in which people exchange their virtual property such as currency, items, and even characters, for real currency. So far, two opposing attitudes of online game operators toward RMT have stood out. One view is that RMT is regarded as a natural act of players with the advantages of accelerated personal trades and reduced costs for physical stores. Whereas, the other view is that RMT is the cause of illegal transactions and consequently should be prohibited (Itsuki et al. 2010).

Third, identity fraud has been described as the unlawful change of an individual's identity (Koops and Leenes 2006). Studies in the field of psychology have presented the coping theory to explain identity fraud. Two different views of coping are outstanding: That of the process view which focuses on the process of managing difficult circumstances, and of the style or personality view, which stresses an individual's personal style of managing and defending psychological integrity (Lazarus 1993). Identity fraud may occur due to consumers' conventional behaviors, as well as because of computer-related threats (Federal Trade Commission 2010). That is to say, identity fraud likely happens both offline and online. Identity thieves are able to obtain an individual's identity by making use of conventional methods or advanced technological methods (Lai et al. 2012). Identity fraud in MMORPGs can be categorized as an instance of identity cloning among a couple of classifications where the players pretend to be other players during the progress of the game (Ramaswamy 2006). Regarding the purchase of items online, the possibility that online games place underage users at risk for identity theft in numerous ways exists. Children and teens may use a parent’s credit card information (Empowering Parents 2014).

Beyond the topic of identity fraud, there has been numerous research on measuring a degree of cyber-security (Aissa et al. 2012; Wang et al. 2012) and managing systems to retain security (Parthasarathy et al. 2012), and analyzing the behavioral pattern of fast-flux botnet which is used for cyber-crimes such as phishing, spam, and click fraud (Caglayan et al. 2012).

3 Data description

The data set we used in this analysis is a selected part of the restored database of an MMORPG obtained from one of the most distinguished service providers in Korea. The background of this MMORPG is a fantasy world where players control character avatars of their own, exploring the landscape, fighting various monsters, completing quests and interacting with non-player characters or other players. The game that we analyzed is developed to mainly target child and teen users, so the game provides cute avatars and easy interfaces for the young users.

To classify our raw log data which is massive over terabyte, we coded the in-memory data manipulation algorithm using Java. The data set provides detailed information on the users and their behaviors including: age, gender, play time, battle time, rest time, and the number of party members. Our sample data consisting of 284,194 user data records were recorded during the period of February–August 2010. Table 1 describes the important variables used in this analysis.

3.1 Age distribution

Figure 1 motivated us to raise the issue of the possibility of identity fraud as we found abnormal distribution across age groups. The distribution of user ages illustrates a double hump pattern. The majority of players are expected to be classified into the group representing players of around 10 years in age as we consider the game’s cute avatars and easy interfaces. However, the second largest group of users consists of players around 40 years old. This is an interesting finding which can be regarded as abnormal when we take into account the decreasing pattern in the groups of 20 year olds and 30 year olds, respectively. Specifically, the numbers of users which age from 36 to 45 are exceptionally larger than neighboring age groups.

In the MMORPG, users under 14 have an incentive to falsify their identity. This is due to the fact that, to play this game, users under 14 should gain parental approval. Furthermore, other users would not want to team up with young players based on an assumption that adult users are better at playing games. When a community makes a team with new members, there is no doubt that skilled players with high levels and more items are preferred. In particular, leaders of communities in their late teens or early 20 s have a rationale to avoid including members who could be perceived as too young in their team.

Table 1 Definition and description of the variables

Variable	Definition	Descriptions
Age	Age of game users	Age registered in user's account
Gender	Gender of game users	Gender registered in user's account
Purchase count	The frequency to purchase items in cash	The age groups are likely to have access to different amounts of money with which to purchase game items
Play time	The period during which users play the game	It could be assumed that the users within an age group have similar life styles
Battle time/rest time	The ratio between battle time and rest time	This ratio demonstrates how willing users are to have battles while they are playing the game. If this ratio is low, users are likely to spend more time exploring unknown areas or partake in non-battle activities. This means that the users with low bat/rest ratio are not yet familiar with the game and they need to spend more time than the users who have knowhow. Meanwhile, users with a high ratio of Battle time/Rest time are likely to possess know-how regarding how to develop their character avatars efficiently in that, by getting involved in a battle, the avatar will attain a high level rapidly. Therefore, this measurement will represent how skilled the users are with the MMORPG
Party member	The number of members in the party	The more users the party has, the stronger the party becomes in battle in most cases. This measurement will show the alliance levels of users

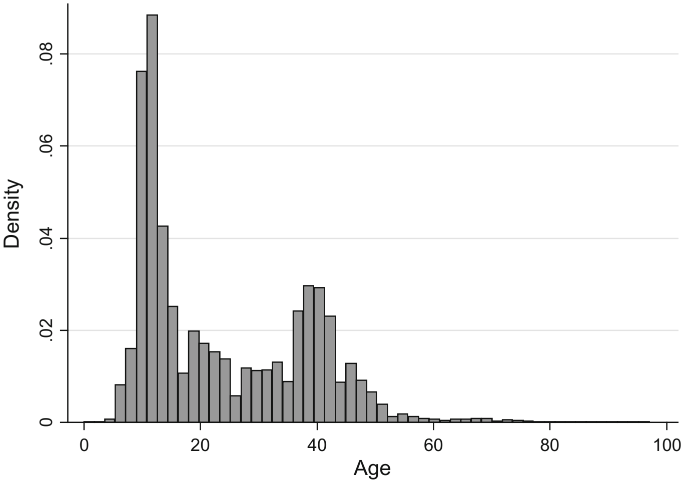

Fig. 1 Histogram for user ages

3.2 Group description

To examine the possibility of identity fraud, behavioral patterns among the age groups are analyzed. We begin our analysis by dividing users into age groups to compare the behaviors of juvenile users with adult users in other age groups.

As we observe the presence of the double humped pattern, we divide the age groups into four groups: 14 and under, 15–35, 36–45, and 46 and above. We will concentrate on the two distinctive groups which are under 14 and 36–45 that shows the odd double humped pattern. We assume that the substantial numbers of members in the 36–45 age group are actually young people using their parent's identity.

The youngest group represents 42% of the total population, while the group between 15 and 35 accounts for 30%. The group between 36 and 45 suspected of having ID frauds represents 22% of the population. The most senior group accounts for 7%.

The descriptive statistics shows that purchase count by group 2 members are higher than that of group 1 which includes young users. It is because adult game users are more able to spend cash to purchase items both to strengthen their character and to save time to spend putting a meaningless effort to the game.

Interestingly, the pattern of group 3 is more similar not to group 2 but to group 1. This seems odd because group 3 and group 2 are also adult users who have similar purchasing power. Even the purchase of group 3 is much lower than that of group 4 which includes elderly users over 46 years old. Generally, it is a common notion that elderly game users (group 4) are not willing to spend cash to play game than young adult game users (group 2 and group 3).

This odd pattern can be shown in other variables such as bat/rest, play time, and party members. In particular, the bat/rest is one of the key clues that demonstrate the possibility of ID fraud. In Table 1, it is already described that bat/rest explains users' knowhow and capability of understanding the game.

Therefore, we suspected that this odd situation comes from ID fraud in that young users use their parent ID. The goal of this study is to prove the pattern and situation shown in our data is abnormal. Additionally, by analyzing traffic data, we found a clue that can prove our suspect that young users use their parents' ID.

4 Method and model

Negative binomial regressions model with dummy variables are set up in order to analyze behavioral differences across age groups. We attempt to identify the differences among user age groups. The dummy variable model will clarify any differences which exist in regard to the frequency of item purchase.

$$\begin{aligned} Y_i = \beta_0 &+ \beta_1 \ln(Play\,time_i) + \beta_2 \ln(Battle\,time/\mathrm{Re}st\,time_i) \\ &+ \beta_3 \ln(Number\,of\,Party\,Members_i) \\ &+ \delta_1(Age\,Group_i) + \delta_2(Gender_i) + \varepsilon \end{aligned} \tag{1}$$

In the model, the frequency of item purchase is used as a dependent variable. Our focus is to compare the differences among age groups. As the independent variable represents frequency, we take the negative binomial regression model on top of a simple linear regression model. Logarithm values of play time, the ratio between

Table 2 Averages of behavioral variables of age groups

Age group (age)	Purchase count	Play time	Battle/rest time	Party member
1 (0–14)	0.2598	2.30E+07	0.1542	75.1147
N = 118,604 (41.73%)	(2.5225)	(380,000,000)	(0.1235)	(436.915)
2 (15–35)	1.7583	4.10E+08	0.1786	442.5093
N = 83,980 (29.55%)	(10.6323)	(3,980,000,000)	(0.1360)	(2186.638)
3 (36–45)	0.4963	9.76E+07	0.1571	130.6858
N = 62,427 (21.97%)	(4.3880)	(1600,000,000)	(0.1150)	(1022.82)
4 (46 above)	1.0949	1.75E+08	0.1607	226.2491
N = 19,183 (6.75%)	(7.1240)	(2300,000,000)	(0.1252)	(1485.753)
Total	0.8109	1.64E+08	0.1625	206.0891
N = 284,194 (100%)	(6.6434)	(2380,000,000)	(0.1261)	(1377.067)

Standard errors are presented in parentheses

battle time and rest time and the number of party members are used to reflect highly skewed distributions of variables as shown at Table 2.

5 Results

A negative binomial regression model provides us with the opportunity to clarify the relationship that purchase frequency is statistically significantly affected by which age groups in which users belong. Table 3 describes both results from the negative binomial regression model and Ordinary Least Square (OLS) model. The results from both models represent that all the explanatory variables such as logged play time, logged battle time and rest time, as well as logged party members, are statistically significant to explain the dependent variable of the number of purchases. The results from the negative binomial regression model with dummy variables show that a user's age group significantly influences the purchase frequency. All the coefficients for dummy variables are positive and statistically

Table 3 Negative binomial regression and OLS results

	(1) NBREG	(2) OLS
ln_playtime	0.625*** (−0.00692)	0.759*** (−0.0148)
ln_battletime/resttime	−0.521*** (−0.0207)	−1.065*** (−0.0536)
ln_partymember	0.00562 (−0.00888)	0.679*** (−0.0213)
Dummy age group 2	0.342*** (−0.0238)	0.927*** (−0.0592)
Dummy age group 3	0.244*** (−0.0271)	0.246*** (−0.0639)
Dummy age group 4	0.703*** (−0.0395)	0.926*** (−0.102)
Dummy gender 2	−0.119*** (−0.0206)	0.149*** (−0.0507)
Constant	−11.68*** (−0.1)	−14.64*** (−0.217)
R-squared		0.122

The dependent variable is the number of purchase, *** $p < 0.01$

significant. That is, groups 2, 3, and 4 are interpreted to have a higher purchase frequency than group 1. The degree of influence of group 3 is found to be the least. We find that age group 3 is most similar to group 1 among all the age groups, as the coefficient for the group 4 is 0.703 greater than those of other groups, while the coefficient of the dummy variable for group 3 is as small as 0.244.

6 Robustness check

6.1 Discriminant analysis

We perform a discriminant analysis to verify robustness of the models which are developed in this study. The results of the analysis are presented in Table 4. Table 4 shows how each true age group (1, 2, 3, 4) is classified as newly-defined groups after the discriminant analysis using four different variables which are play time, purchase count, number of party members, and bat/rest each. After conducting the discriminant analysis, the true age group 1 can be categorized as newly- classified group 1, 2, 3, and 4. For example, the rate of true age group 1 which is classified as newly-defined group 1 is 49.28% and the rate of true age group 2 which is classified a newly-defined group 2 is 53.33%. However, interestingly, the rate of true age group 3 which can be classified as newly-defined group 3 is just 17.92% which is relatively extremely low compared to the case of group 1 and 2. (The reason why the true group is divided into many groups is that discriminant analysis uses a simple linear line to divide the intersection of two groups. Therefore, normally, the discriminant analysis is not used to show precise results but to see the big picture. Also, the sample size of true age group 4 (=8730) is relatively small compared to other groups, it can be neglected.) In particular, the rate of true group 3 classified as newly-defined group 1 is extremely high compared to newly-defined groups 2. This means that true group 3 is more similar to newly-defined group 1 than to newly-defined group 2.

6.2 Log traffic analysis

We performed a log traffic analysis to estimate how many young users were using their parent IDs. To identify the frequency of identity fraud, we uses transaction data

Table 4 Discriminant analysis result

True age group	Classified group1	Classified group2	Classified group3	Classified group4	Total
True group 1	28,117 (49.28%)	13,703 (24.02%)	10,321 (18.09%)	4918 (8.62%)	57,059
True group 2	12,323 (28.63%)	22,956 (53.33%)	5271 (12.24%)	2499 (5.80%)	43.049
True group 3	13,738 (46.44%)	8168 (27.61%)	5302 (17.92%)	2374 (8.03%)	29,582
True group 4	3455 (39.58%)	3302 (37.82%)	1387 (15.89%)	586 (6.71%)	8730
Total	57,633 (41.64%)	48,129 (34.77%)	22,281 (16.10%)	10,376 (7.50%)	138,420

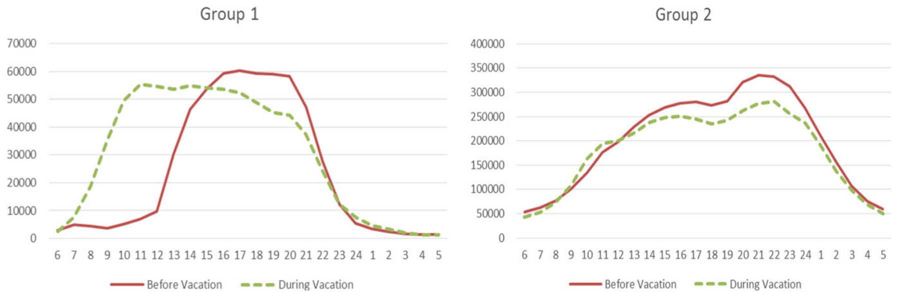

Fig. 2 Log traffic in group 1 and group 2

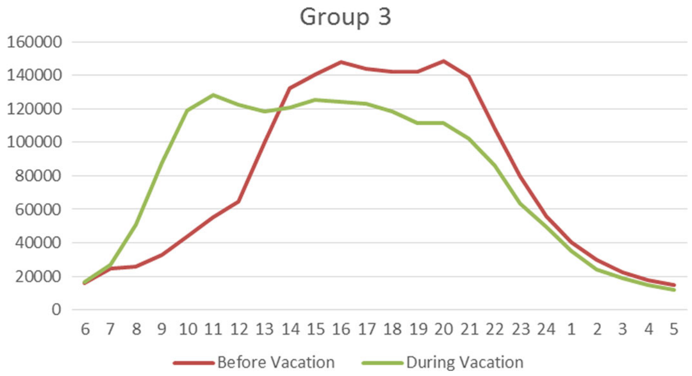

Fig. 3 Log traffic in group 3

that changes rapidly before and during elementary school vacation because the users in group 1 are elementary school students. Transaction data for each week before and during elementary school vacation are investigated Fig. 2.

It is presented that group 2 (users from 15 to 35 years old) shows an unchanging traffic pattern regardless of elementary school vacation. On the other hand, it is shown that there are dynamic traffic changes in group 1 (group of elementary school students) before and during vacation. This is because elementary school students are able to have access to online games in the morning during vacation, while they normally were in school at the time before vacation. We find a definite difference in traffic patterns between child and adult groups.

In this context, if identity frauds occur in group 3, the traffic pattern of group 3 should be somewhat similar to that of group 1.

Figure 3 represents the traffic pattern of group 3. As expected, group 3 has a similar traffic pattern to group 1. This demonstrates that the existence of identity fraud in group 3 at Table 5.

We additionally estimated the actual rate of identity using log traffic data. The specific point of time is 12 pm, as it is the time when elementary students begin having access to online games before vacation. Before vacation, a log traffic increases rapidly after 12 pm. In contrast, during vacation, most of the users in groups 1 and 3 can freely have access to online games from 12 pm. As a result, at

Table 5 Average traffic data before and during vacation

Time	Average traffic data before vacation					Average traffic data during vacation				
	Group 1	Group 2	Group 3	Group 4	Total	Group 1	Group 2	Group 3	Group 4	Total
6	2870	53,532	16,000	16,873	89,274	2607	42,600	16,751	12,558	74,517
7	4939	61,929	24,842	16,135	107,845	7702	52,968	26,849	14,920	102,439
8	4346	76,861	26,143	18,133	125,482	18,800	72,921	50,576	22,956	165,253
9	3711	100,776	33,104	23,965	161,556	35,200	108,836	87,740	34,840	266,616
10	5133	134,072	44,039	32,256	215,500	49,605	162,682	119,097	51,250	382,634
11	7075	176,652	55,281	40,075	279,083	55,328	194,633	128,193	55,838	433,993
12	9776	198,278	64,632	42,457	315,143	54,543	200,382	122,395	55,810	433,131
13	30,210	227,876	99,750	53,487	411,323	53,536	216,495	118,131	60,944	449,107
14	46,382	253,068	131,994	61,834	493,278	55,014	237,929	120,608	67,835	481,386
15	53,652	269,218	140,392	69,218	532,479	54,120	247,658	125,487	65,955	493,220
…	…	…	…	…	…	…	…	…	…	…
Total	567,147	4,840,848	1,868,081	1,134,882	8,410,958	724,941	4,367,246	1,911,323	1,114,543	8,118,053

Table 6 Estimated schoolchild ratio

	Group 1 (under 14)	Group 2 (15–35)	Group 3 (36–45)	Group 4 (above 46)
Traffic gap between during vacation and before vacation (at 12 pm)	44,767	2104	57,763	13,353
Estimated schoolchild ratio (%)	82	1	47	24

12 pm, the gap of the traffic patterns between before vacation and during vacation is the approximate number of elementary school students committing identity fraud Table 6.

Consequently, it is found that around 47% of the users in group 3 have a similar traffic pattern to users in group 1. Most of the users in group 1 are elementary school students. Around 24% of group 4 also has a similar traffic pattern to the users of group 1. All of these results seem to be related to the possibility of identity fraud. In group 2, 99% of users show the consistent traffic pattern regardless of vacation, which suggests that most of them are users who do not commit identity fraud. Considering this, 82% of the users in group 1 indicate the traffic pattern of elementary school students, while the remainders of the users (18%) are suspected to be either pre-school children who use their own identity or adult users who use children's identity, which could also be identity fraud.

7 Discussions and contributions

In this study, we present the possibility of identity fraud, as a number of users in MMORPG may use the identities of individuals in other age groups. The accurate prediction of the identity fraud is far from clear. However, the results of the analyses can be interpreted in several ways.

One interpretation of the negative binomial regressions model shows that there is a behavior difference between some age groups. The frequency of item purchase, play time and battle participation are shown differently depending on age groups. However, The results of the econometrics analysis showed that the behavior pattern (especially for purchasing) of group around 40 years old was very similar to that of teenagers. This is odd because there must be a different purchasing power between child users and adult users. Even, other adult groups except for the age around 40 years old show much higher purchase counts than the group of child users. Additionally, considering that the game used for the analysis is a game for young users, this means that some of the users in the group around 40 years old may be teenagers who have stolen the parent's ID.

We also performed discriminant analysis and log traffic analysis to estimate how many young users were using their parent IDs. As a result, about 47% of the users around 40 years old were found to be teenager users. Also, behavior patterns of users who are estimated to be teenagers have been found in other age groups.

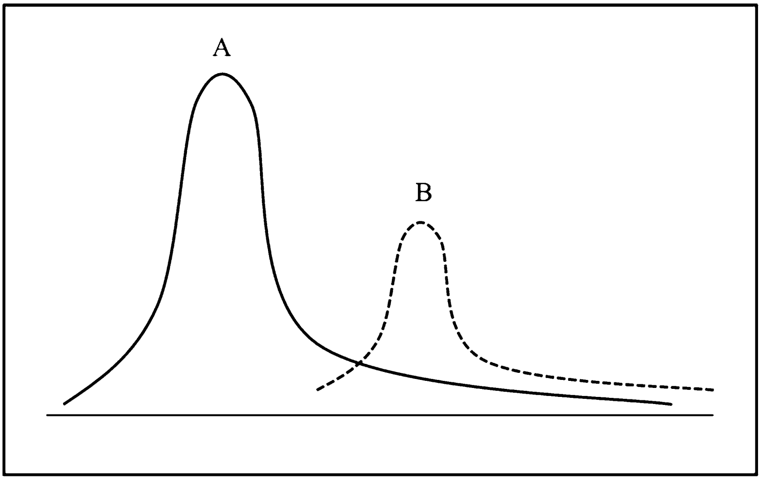

Fig. 4 Intuition for user age distribution

We come to infer that the distribution of the ages can be separated into two groups of real and fake identities as shown in Fig. 4. As long as the distribution of curve A follows normal distribution and fraud users use their parents identities, curve B can be assumed to represent the group of children users who fraud their parents' IDs.

According to the National Crime Victimization Survey (2013) by The Bureau of Justice Statistics (BJS), Americans spent $24.7 billion in 2012 while all other kinds of crimes (losses for household burglary, motor vehicle theft, and property theft) cost just $14 billion. Also, in the report by Ponemon Institute (2013), it is stated that identity fraud brings not only social damages to the society but managerial damages to firms both directly and indirectly. One of the managerial implications of this paper is that firms can detect and measure that there is a group of people who commit identity fraud. Moreover, by doing so, they can prevent identity fraud in advance.

Beyond identity fraud, we clearly demonstrates that group 2 has a higher skill level and means to pay for items. This result can provide MMORPG service providers with the implication that they should segment their market properly. The number of users over the age of 50, as well, is increasing, which should draw the attention of game developers. However, we present the plausible reason that a substantial number of fake senior users can exist. Furthermore, the study provides managerial implications for MMORPG service providers that a marketing campaign for a specific user demographic could be wrongfully targeted because a substantial portion of the targeted age groups may be, in reality, much younger users who use fraudulent identities. Other implications for government regulations is that the policies based on a user's age can be ineffective in controlling the amount of play time per day or in preventing juvenile users from playing games during certain times of the day. To make the policies effective, the systems to ensure that identities are real should be required in advance. Additionally, it is believed that the fraud detecting method presented in this paper can be generalized in other contexts. It is due to the fact that other game companies collect data similar to the user behavior data used in this study.

While the findings of this study provide practical implications for the possibility of identity fraud in online games, it is important to note its limitations. The possibility of behavioral differences among age groups is inferred through analyses of users' behaviors. We do not have a suitable method to verify whether the age information of users is real or not. Identifying whether users are using their real identity is difficult even though MMORPG service providers have been trying to identify fraudulent users in various ways. Some service providers have authentication of identity through a mobile device and ad hoc questions for users, only to find it hard to verify the information at the end of the day. Considering the reasonable amount of doubt related with identity fraud, there are additional research opportunities. A plausible alternative is to have experiments to identify reactions by age group to confirm the results of this study. For instance, a service provider may offer deals on items exclusively targeted for a certain group or during the hours, say, school hours, when a certain age group is more or less likely to be able to access the game.

Acknowledgements The authors appreciate the research support from Center for Information& Communication Business and Research at Seoul National University.

References

Aissa AB, Abercrombie RK, Sheldon FT, Mili A (2012) Defining and computing a value based cyber-security measure. IseB 10(4):433–453

Alemi F (2007) An avatar's day in court: a proposal for obtaining relief and resolving disputes in virtual world games. UCLA J Law Technol 11(2):1–54

Assmann JJ, Drescher MA, Gallenkamp JV, Picot A, Welpe IM, Wigand RT (2010) MMOGs as emerging opportunities for research on virtual organizations and teams. In: Americas conference on information systems (AMCIS), p 335

Barfield W (2006) Intellectual property rights in virtual environments: considering the rights of owners, programmers and virtual avatars. Akron Law Rev 39(3):649–700

Bell MW (2008) Toward a definition of "virtual worlds". J Virtual Worlds Res 1(1)

Bureau of Justice Statistics (2013) National Crime Victimization Survey (NCVS)

Caglayan A, Toothaker M, Drapeau D, Burke D, Eaton G (2012) Behavioral analysis of botnets for threat intelligence. IseB 10(4):491–519

Castronova E (2007) Exodus to the virtual world: how online fun is changing reality. Palgrave Macmillan, New York

ChinaHearSay (2011) China's online game real id system, take two http://www.chinahearsay.com/chinas-online-game-real-id-system-take-two/

Device (2012) timed online gaming restriction possibly coming to South Korea. http://www.devicemag.com/2012/02/17/timed-online-gaming-restriction-possibly-coming-to-south-korea/

Digi-Capital (2011) Global games investment review

Empowering Parents (2014) Kids stealing from parents: what you need to know now. http://www.empoweringparents.com/is-your-child-stealing.php

ESRB (2014) http://www.esrb.org

Farrell J, Saloner G (1985) Standardization, compatibility, and innovation. RAND J Econ 16(1):70–83

Federal Trade Commission (2010) Talking about identity theft: a how-to guide

Forbes (2012) South Korea may limit young online gamers to 2 hours a day to prevent bullying. http://www.forbes.com/sites/carolpinchefsky/2012/02/16/south-korea-may-limit-young-online-gamers-to-2-hours-a-day-to-prevent-bullying/

Gensollen M (2007) L’Economie Réelle des Univers Peristants: Vers une Propriété Virtuelle? In: Beau F (ed) Culture d’univers: jeux en réseau, mondes virtuels, le nouvel âge de la société numérique. FYP éditions, Paris, pp 1–13

Itsuki H, Takeuchi A, Fujita A, Matsubara H (2010) Exploiting MMORPG log data toward efficient RMT player detection. In: Proceedings of the 7th international conference on advances in computer entertainment technology, ACM, pp 118–119

Katz ML, Shapiro C (1985) Network externalities, competition, and compatibility. Am Econ Rev 75:424–440

Koops BJ, Leenes R (2006) Identity theft, identity fraud and/or identity-related crime. Datenschutz und Datensicherheit-DuD 30(9):553–556

Kozinets RV (2010) Netnography. Doing ethnographic research online. Sage Publications Ltd, London

Lai F, Li D, Hsieh CT (2012) Fighting identity theft: the coping perspective. Decis Support Syst 52:353–363

Lazarus RS (1993) Coping theory and research: past present, and future. Psychosom Med 55(3):234–247

McKenna B, Gardner L, Myers M (2011a) Issues in the study of virtual world social movements. PACIS 2011 Proceedings. Paper 129. http://aisel.aisnet.org/pacis2011/129

McKenna B, Gardner L, Myers M (2011b) Social Movements in World of Warcraft. AMCIS 2011 Proceedings–All Submissions. Paper 83. http://aisel.aisnet.org/amcis2011_submissions/83

Parthasarathy R, Shirazi BA, Peterson N, Song WZ, Hurson A (2012) Management and security of remote sensor networks in hazardous environments using over the air programming. IseB 10(4):521–548

Ponemon Institute (2013) 2013 Cost of data breach study: global analysis. Benchmark research sponsored by Symantec Independently Conducted by Ponemon Institute LLC May 2013. https://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

Ramaswamy VM (2006) Identity-theft toolkit. CPA J 76(10):66–70

Rheingold H (2000) The virtual community: homesteading on the electronic frontier. MIT Press, London

Roquilly C (2011) Control over virtual worlds by game companies: issues and recommendations. MIS Q 35(3):653–671

Shankar V, Bayus BL (2003) Network effects and competition: an empirical analysis of the home video game industry. Strateg Manag J 24(4):275–384

Shy O (2001) The economics of network industries. Cambridge University Press, Cambridge

Wall Street Journal. (2011). Gaming’s new frontier after zynga. http://online.wsj.com/article/SB10001424052970204443404577051992472392070.html

Wang JA, Guo M, Wang H, Zhou L (2012) Measuring and ranking attacks based on vulnerability analysis. IseB 10(4):455–490