Peer-to-Peer Netw. Appl. (2016) 9:508–519
DOI 10.1007/s12083-015-0371-x

# A privacy data leakage prevention method in P2P networks

**Cheol-Joo Chae**[1] · **YongJu Shin**[1] · **Kiseok Choi**[1] · **Ki-Bong Kim**[2] · **Kwang-Nam Choi**[1]

Received: 15 March 2015 / Accepted: 15 May 2015 / Published online: 30 May 2015


**Abstract** Registered peers to a P2P service can share and exchange information with other peers without servers using P2P network. In such P2P networks, there are frequent leaks of the internal privacy data of an organization through P2P file sharing. Today, DLP which is a privacy data leakage prevention technology is applied P2P network blocking and file encryption methods. However restricting all the services and normal users is difficult due to the number of ports used by P2P including the port 80. Thus, we propose a privacy data leakage prevention method by releasing a P2P sharing file that does not include privacy data using a privacy data removing technology with a privacy data leaking risk factor. The proposed method provides higher security and performance compared with a DLP method as privacy data is removed from a P2P sharing file.

✉ Kwang-Nam Choi
knchoi@kisti.re.kr

Cheol-Joo Chae
cjchae@kisti.re.kr

YongJu Shin
yjshin@kisti.re.kr

Kiseok Choi
choi@kisti.re.kr

Ki-Bong Kim
kbkim@hit.ac.kr

[1] Korea Institute of Science and Technology Information, 245 Daehangno, Yuseong-gu, Daejeon, Korea

[2] Department of Computer Information, Daejeon Health Science College, 21 Chungjeong-ro, Dong-Gu, Daejeon, Korea

**Keywords** P2P file sharing · Privacy detection · Privacy leakage prevention · Privacy level · P2P

## 1 Introduction

Although recently P2P networking, which is a popular network service on the Internet, has been applied to various areas, a number of security threats are rising due to the inherent weak point of a P2P network. Since a P2P network is an overlay network based on the Internet, it has security issues similar to the existing Internet environment. However the major security issue of the P2P file sharing system today is the privacy data leakage. Privacy data leakage is not only a personal matter, but also can impact on the entire organization as the leaked information also can contain the critical information of the organization in many cases. Therefore organizations use a number of privacy data leakage prevention technologies to prevent personal information leakage by P2P file sharing. The most popular privacy data leakage prevention technology is a DLP(Data Loss Prevention) technology. DLP restricts transferring all files with potential internal privacy data to the outside of an organization. However DLP technologies have some disadvantages. For example, it may restrict transferring a normal file to the outside of an organization due to the high detection-error rate, and it also can invade the privacy of the internal staffs for the data filtering. Thus we propose a technology that can overcome the disadvantages of existing privacy data leakage prevention technologies, and particularly prevent privacy data leakage of an organization through P2P file sharing. The proposed method provides higher security and performance. Since it removes the privacy data on the file shared on a P2P network, it prevents the internal

privacy data leakage, and improves 16 % of the processing performance compared with an existing encryption method for a file with personal information. The structure of this paper is firstly in the Section 2, the issues around a P2P file sharing method are analysed; secondly in Section 3, a privacy data leakage prevention technology is proposed to prevent privacy data leakage in an organization by identifying the privacy data and a privacy data leaking risk factor; and thirdly in the Section 4, the performance of a proposed method is evaluated, and lastly the conclusion in the Section 5.

## 2 Related work

### 2.1 Peer-to-peer network

On a P2P (Peer-to-Peer) network, all computers are connected each other and shares resources, and all participants are servers and clients simultaneously which are different concept from a conventional client–server network. Registered peers to a P2P service configure a P2P overlay network, which is a virtual network separated from a physical network configuration [1–4]. Peers on an overlay network can share and exchange information with the other peers without the aid of a server. This P2P concept means the direct connection between computers, and also provides faster and safer network-resource sharing and data processing. P2P networks can be classified into a centralized P2P network and a distributed P2P network by overlay network configuration. A distributed P2P network is classified as a structured P2P network and an unstructured P2P network by an operation mode and a structure [5]. Table 1 shows P2P classification scheme by network configuration.

Recently the most popular file sharing method of a P2P network is direct transferring between computers without a server. This approach does not upload a sharing file to the server on a P2P network. It stores the file on the designated file on a user's computer, and connects the folder to the Internet using the P2P software. Users using the P2P software can download the stored file from the folder of the other peers through the Internet. Using the approach a P2P network can share a file without a client–server configuration. Additionally the number of participants to share the file on the P2P network increases, it allows a more efficient downloading process. The most popular P2P softwares are BitTorrent, eDonkey, emule, KaZaA, and WinMX.

Figure 1 shows the method to share a file using a P2P network. Peer C downloads a sharing file from peer A, peer B and peer D. The P2P network shares the file based on the piece which is a group of a small fraction of a file. Thus peer C downloads the file consists of 5 pieces from peer A (piece 1 and piece 3), peer B (piece 2 and piece 4) and peer D (piece 5). Using this method, the file from all participants. More than 86 % of companies use a P2P sharing application, and the usage rate increases by 14 % from 61 % in 2012 to 75 % in 2013. The most popular P2P file sharing application is BitTorrent with a share of 63 % followed by Soulseek (25 %), eDonkey (14 %), Xunlei (13 %), and Box Cloud (10 %) [6].

### 2.2 Privacy data leakage on the P2P file sharing

Due to the convenience and efficiency, the usage rate of a P2P file sharing system by the staffs of an organization using their network has increased rapidly. In accordance with the increasing trend, the privacy data leakage of the customers and the staffs through the P2P file sharing has increased too.

Although misuse and abuse of a P2P file sharing method is one of the reasons for the privacy data leakage through a P2P file sharing, the major factor is a malicious virus or malicious code that causes the privacy data leakage by sharing all the

**Table 1** P2P networks by network configuration

| Classification | | Content | Disadvantage |
|---|---|---|---|
| Centralized P2P | | A central sever manage all peers and transfers messages that provides continuous service to support the efficient information searching and storing of each peer. | The increasing number of peers can increase the server load that causes the extensibility issue, and an issue of the central server can affect the entire network. |
| Distributed P2P | Structured P2P | A distributed structure that provides the distributed indexing for mapping contents and peers in a single address space. (e.g., Kademlia and eDonkey) | It consists of a structural self-network. it requires a complex routing algorithm, and a high cost of the network maintenance to handle the participation and withdrawal of the peers. |
| | Unstructured P2P | A structure that provides a messaging service and maintaining the P2P network by the voluntary participation of peers without a central server (e.g., Gnutella, KaZaA, and BitTorrent) | It generates higher network traffic compared with the other P2P networks due to the inefficient use and search of the distributed network resource. |

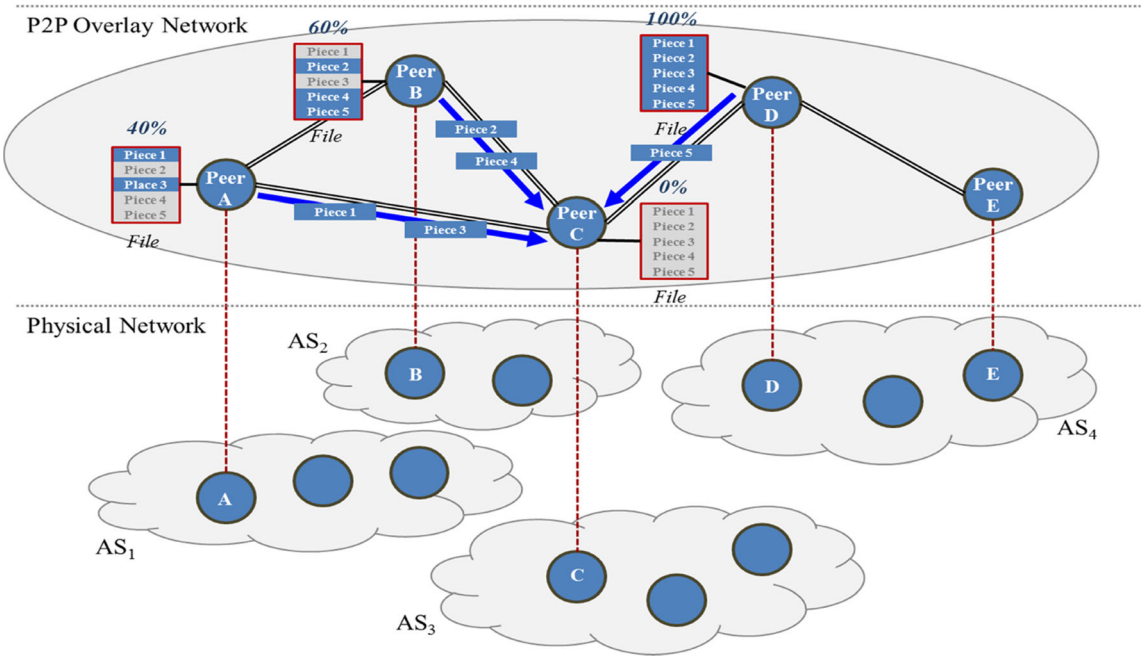


**Fig. 1** File sharing of a P2P network

files of a user. When a user of an organization downloads the code which includes hidden malicious code on a P2P network, the malicious code will infect all internal user's PC, and collect and send all document files to the attacker [7, 8].

For example, a computer worm called Antinny was spreaded through P2P in Japan. Antinny indicated a fault error message, changed the Windows settings to run itself, and duplicated itself. The duplicated Antinny was shared automatically on the Winny network to increase the number of the infection subjects. Antinny was modified to the other forms such as Antinny.B, Antinny.G, Antinny.K, and Antinny.L after the expansion. Antinny and the other modified worms which expanded infected PCs leak various data including business data and secret data on the infected PC to the outside [9]. FTC (US Federal Trade Commission) prosecuted two companies that leaked 95,000 of customer's privacy data including medical codes, driving license numbers, social security codes, names, addresses, and date of birth of 3800 hospitals using P2P malicious code in US in June 2013.

### 2.3 Privacy data leakage prevention technologies

Many technologies are applied to prevent the internal privacy data leakage of an organization through P2P file sharing. The most popular privacy data leakage prevention for an organization is a DLP technology. DLP is developed as an internal security technology to prevent leakage of an important information of an organization. However as the privacy data has been rising as a social issue, the internal information leakage prevention technology is considered as a privacy data leakage prevention technology. DLP is a technology that checks the data on a user's computer or a transferring data on a network, and if the data pattern is identical or similar, detects and blocks the data. For the data leakage prevention, DLP performs media control, packet control, program execution prevention and PC control. The information leakage prevention system like DLP is based on the content searching. There are two DLPs such as network-based DLP and end-point DLP based on the data searching point. Network DLP detects outgoing traffic on the central server. End point DLP monitors the data activity of a user using an installed agent on a client device such as a laptop or a PC, and controls the data leakage. Figure 2 shows the method to prevent information leakage using DLP approach. Analyse outgoing traffic to an external network, categorize and extract the information using a semantic analysis, and encrypt a file or block information leakage. A current DLP system uses a PIE(Parametric Information Extraction) method that performs syntax analysis for information using the parameters, extracts and stores in a database automatically [10, 11].

However, the information leakage prevention system using DLP has some disadvantages.

Firstly, DLP needs traffic and content controls for privacy data leakage prevention. The traffic control restricts uses of protocols and services. It can restrict the

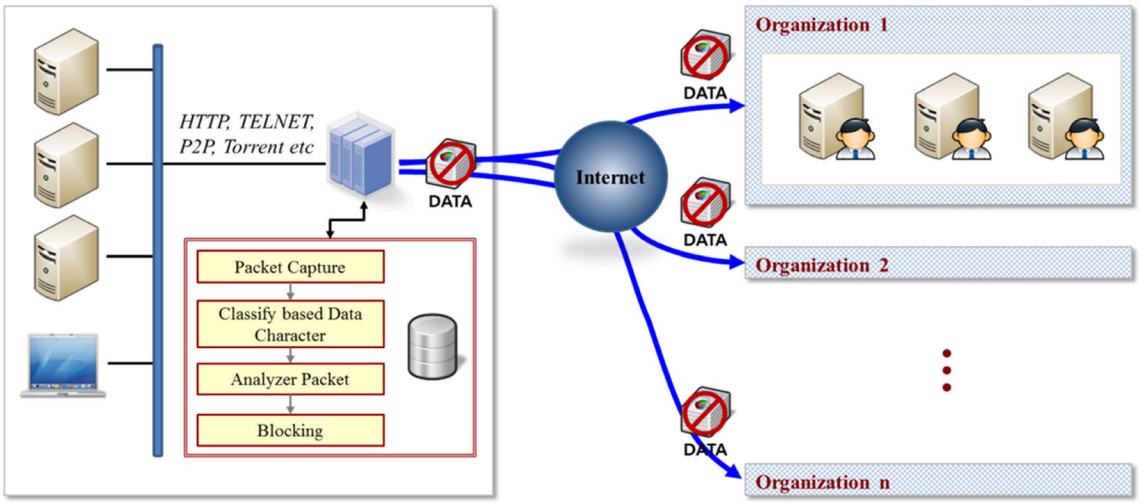


**Fig. 2** Privacy data leakage prevention using a DLP technology

use of services such as P2P, FTP and messengers with potential information leakage. However it is difficult to restrict all the services and normal users from service, since P2P uses a number of different ports including the port 80. Additionally the content control detects outgoing information with various routes, and judges whether or not to transfer. However for the content control technology of DLP, identifying the internal privacy data and defining the risk factor is difficult due to the different importance-criteria of contents by organizational characteristics.

Secondly, DLP cannot protect the privacy data of internal staffs. Since originally DLP is developed to prevent business secretes trading, it uses a content searching technology. However the private information of an internal staff along with customer's information can be included when identifying all packet contents during the content searching process. From the perspectives of privacy protection, protecting the privacy data of an internal staff is also important to the same level of protecting the privacy data of customers. The main reason that there has been continuous criticism of a DLP system from US and Europe is the invasion of privacy of staffs.

Therefore in this paper a privacy data leakage prevention method is proposed to prevent the privacy data leakage of customers and internal staffs by identifying the privacy data and a privacy data leaking risk factor.

## 3 Design of the privacy data leakage prevention system for P2P file sharing

The privacy data leakage prevention system for P2P proposed on this paper identifies the internal privacy data, defines the level, and decides the privacy data leakage prevention policy suitable for each organization by measuring the leakage risk using the each combination of the privacy data level.

Below is the privacy data leakage process from the proposed system. When an internal staff uses a P2P file sharing program, the entire organization is considered as one peer to connect with the external users. The external peers request an internal peer for a file. When the internal peer sends the file, the proposed system detects if the sharing file contains any personal information by detecting the P2P sharing file using a firewall. If the privacy data is included, the proposed method analyzes it using a keyword analysis depends on the level of privacy data leakage risk, and the privacy data is removed from the file using a regular expression. Thus privacy data leakage can be prevented since the new sharing file on a P2P network does not contain any privacy data. Then the file without a privacy data is transferred to the external peer. Figure 3 shows the process of the proposed system.

### 3.1 Privacy data identification and privacy data leaking risk factor

The internal privacy data that must be handled and protected should be identified, and privacy data leaking risk factor should be defined to prevent privacy data leakage [12, 13]. The proposed system categorized to private identity information, $Privacy_{ID} \ni$ {social security number, driving license number, and passport number}, financial information, $Privacy_{Finance} \ni$ {credit card number, and account number}, personal identity number information, $Privacy_{Personal\ Info} \ni$ {telephone number, E-mail, and address}, and social privacy information, $Privacy_{Social\ Info} \ni$ {job, title, religion, and club activity}. The level of privacy data leaking risk factor is classified into six levels from the top P1 to the bottom

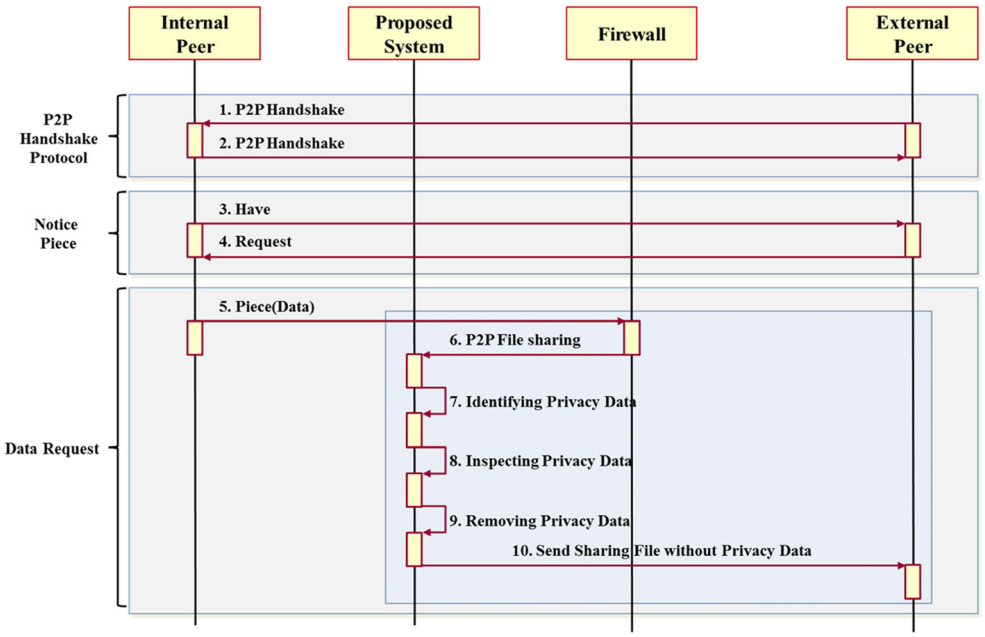


**Fig. 3** Process of the proposed system for privacy data leakage prevention

P6 (P1=Privacy$_{ID}$, P2=Privacy$_{Finance}$, P3=Privacy$_{Personal\ Info}$, P4=Privacy$_{Social\ Info}$) in accordance with the combination of privacy data.

The possibility of the privacy data leakage ($0<P<1$) is defined using logistics regression to define the privacy data leakage prevention policy based on the level of the privacy data leakage risk factor. The privacy data leakage prevention policy can be decided by an organization based on the probability of the privacy data leakage risk. The equation for probability of the privacy data leakage risk ($P$) is Eq. (1). Table 2 shows defining the level of privacy data leaking risk factor.

$$
\begin{aligned}
&\mathrm{P}\left(\mathrm{Y}=1 \middle| x_1,\ x_2,\ \cdots,\ x_p\right) \\
&\quad = \frac{\exp\left(\beta_0+\beta_1 x_1+\beta_2 x_2 \cdots \beta_p x_p\right)}{1+\exp\left(\beta_0+\beta_1 x_1+\beta_2 x_2 \cdots \beta_p x_p\right)} \\
&\quad = \frac{e^A}{1+e^A} \times 100 \qquad (1) \\
&\mathrm{A} = \beta_0 + (\beta_1 \times Privacy_{Level\ 1}) + (\beta_2 \times Privacy_{Level\ 2}) \\
&\qquad + (\beta_3 \times Privacy_{Level\ 3}) + (\beta_4 \times Privacy_{Level\ 4}) \\
&\qquad + (\beta_5 \times Privacy_{Level\ 5}) + (\beta_6 \times Privacy_{Level\ 6})
\end{aligned}
$$

**Table 2** Defining the level of privacy data leaking risk factor

| level | The combination of the privacy data | The description of the combination | The description of the risk |
|---|---|---|---|
| Level 1 | P1+P2 | The combination of the private identity information and the financial information | The private identity exposure and the potential financial damage are expected. |
| Level 2 | P1+P3 | The combination of the private identity information and the personal identity number information | The private identity can be exposed |
| | P1+P4 | The combination of the private identity information and the social privacy information | |
| Level 3 | P2+P3 | The combination of the financial information and the private identity information | The private identity exposure and the potential financial damage are expected. |
| Level 4 | P2+P4 | The combination of the financial information and the social privacy information | The potential financial damage are expected. |
| Level 5 | P3+P4 | The combination of the personal identity number information and the social privacy information | It is possible to estimate the identity and personal details |
| Level 6 | P4 | Social privacy information | Barely possible to obtain the personal details, however it is possible to impersonate. |

The proposed system can prevent privacy data leakage by identifying the internal privacy data, defining the level of the privacy data leakage risk factor, and using the probability of the risk factor. The algorithm for identifying the internal privacy data and the probability of the privacy data leakage risk is below.

Algorithm: Identifying the internal privacy data of an organization and the probability of the privacy data leakage risk

Let $Privacy_{ID}$ = {social security number, driving license number, passport number}

Let $Privacy_{Finance}$ = {credit card number, account number}

Let $Privacy_{Personal\ Info}$ = {telephone number, E-mail, address}

Let $Privacy_{Social\ Info}$ = {job, title, religion, club activity}

```
Function Privacy Grade ()
{
    Switch(Privacy)
    {
        Case 1: If (Privacy = Privacy_ID ) then Grade = "P1";
                Break;
        Case 2: If (Privacy = Privacy_Finance ) then Grade ="P2";
                Break;
        Case 3: If (Privacy = Privacy_Personal Info) then Grade = "P3";
                Break;
        Case 4: If (Privacy = Privacy_Social Info) then Grade = "P4";
                Break;
    }
    Return Grade;
}
```

Function Probability ()

{

$$A = \beta_0 + (\beta_1 \times Privacy_{Level\ 1}) + (\beta_2 \times Privacy_{Level\ 2}) + (\beta_3 \times Privacy_{Level\ 3}) + (\beta_4 \times Privacy_{Level\ 4}) + (\beta_5 \times Privacy_{Level\ 5}) + (\beta_6 \times Privacy_{Level\ 6})$$

$P$ = 1+ exponential A / exponential A x 100;

Return $p$;

}

### 3.2 Privacy data leakage prevention for P2P file sharing

The proposed system consists of a privacy data identifying module, a privacy data leaking risk factor measuring module, and a privacy data leakage prevention module. The privacy data leakage prevention module consists of a privacy data detecting-area defining part, privacy data detecting part, privacy data verifying part, and a privacy data removing part from a sharing file. The privacy data detecting-area defining part of a sharing file reads a file from the first line to the last line. If the read file has an identical privacy data pattern on the privacy data detecting-pattern database, the text information and the location of the local file is stored in a privacy data detecting log. The privacy data detecting log is verified by comparing with the privacy data generating rule in the

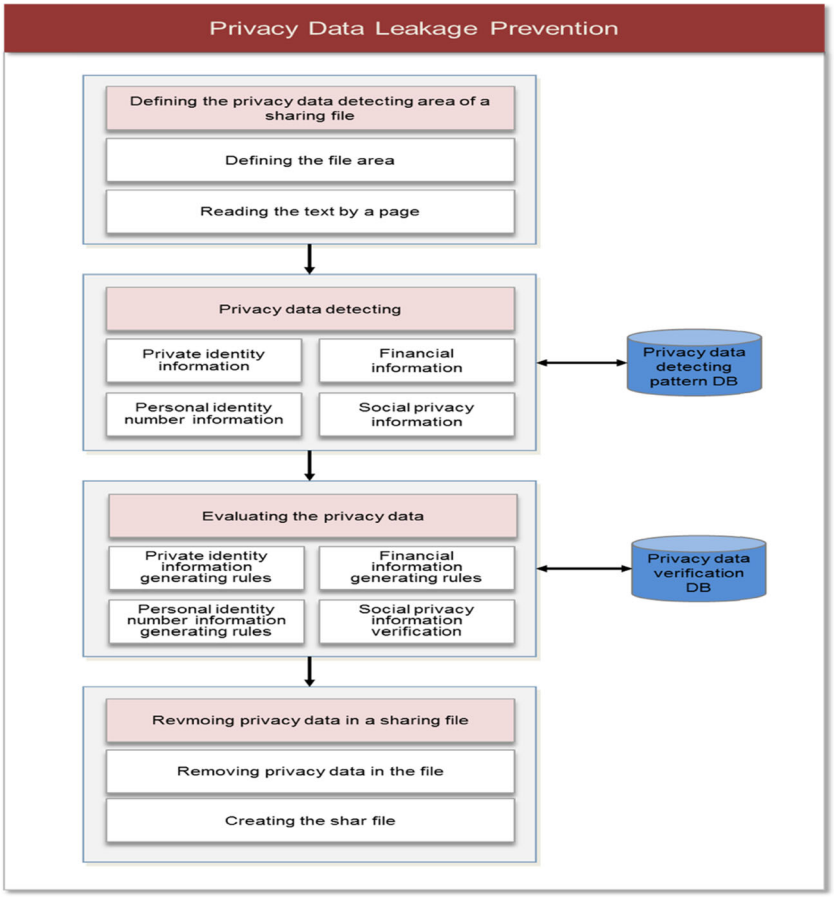


**Fig. 4** Privacy data leakage prevention module

verification database. Finally, the privacy data verified is removed from the sharing file, and create a new file with the privacy data. Figure 4 shows the design of the privacy data leakage prevention module.

The privacy data filter that can filter the privacy data using a regular expression is designed to detect the privacy data from the sharing file. A regular expression is a pattern description made of a meta language to describe a particular type of strings that describe meta characters of a particular string patterns. Table 3 shows the privacy data detection filter of the proposed system. The privacy data detecting filter is stored and managed in the database.

Each privacy data item of the detected privacy data detecting log is verified using the privacy data detecting filter. Since

**Table 3** Defining the privacy data detecting filter

| Privacy data detecting items | Regular expression filter |
|---|---|
| Resident registration number | \\b\\d{2}(((0[1,3,5,7,8]\|10\|12)((0[1–9])\|([1,2][0–9])\|30\|31))\|((0[4,6,9]\|11)((0[1–9])\|([1,2][0–9])\|30))\|(02((0[1–9])\|([1,2][0–9])))\\s*-\\s*[1,2,3,4]\\d{6} |
| E-mail address | \\b[\\w]+@[\\w]+(\\.\\w+)+ |
| Telephone number | \\b0[1–9]\\d{0,2}\\s*-\\s*[1–9][0–9]{2,3}\\s*-\\s*[0–9]{4} |
| | \\b0[1–9]\\d{0,2}\\s[1–9][0–9]{2,3}\\s[0–9]{4} |
| Address | \\b(\\S+[Dobooknam]\\s*)?\\S+Gun\\s*\\S+[Eup,Myeon]\\s*((\\S+[Dong\|Lee]\\s*\\d+)\|(\\S+Ro\\s*\\d+Gil?)\|(\\d+Gil))\\s*\\S* |
| | \\b(\\S+[Dobooknam]\\s*)?\\S+Si\\s*(\\S+Gu\\s*)?((\\S+Dong\\s*\\d+)\|(\\S+Ro\\s*\\d+Gil?)\|(\\d+Gil))\\s*\\S* |
| Financial information | \\b(((1\|2\|6\|9)\\d{3}\\s*-\\s*\\d{4}\\s*-\\s*\\d{4}\\s*-\\s*\\d{4})\|(3\\d{3}\\s*-\\s*\\d{4}\\s*-\\s*\\d{4}\\s*-\\s*(\\d{3}\|\\d{2}))\|((4\|5)\\d{3}\\s*-\\s*\\d{4}\\s*-\\s*\\d{4}\\s*-\\s*\\d{3})) |

a regular expression is a pattern technology based on a meta language, the detected privacy data should be verified whether it is privacy data or not. The verification of each privacy data item uses the generating rule to verify if the detected privacy data detecting logs match with the privacy data generating rule. For detected credit card numbers, the proposed system stores a value set A which is a sum of all numbers multiplied by 2 exclude every second values from the left. (if the multiplied value exceeds 9, the sum of two digits are used. For example, if the value is 10, then perform 1+0). Then every second values are stored in a value set B. If the both value sets A and B can be divided by 10, the algorithm defines the value as a credit card number. The privacy data detecting log is verified using the methodology. When the privacy data verifying process is finished, a new file without the privacy data is generated from the sharing file and transferred to a P2P network. The privacy data leakage prevention algorithm of the proposed system is below.

```
Algorithm : Preventing the privacy data leakage on the P2P sharing file.
Let Privacy Pattern ← Regular Expression
Let Privacy verification ← Privacy Generating Rule
Function Privacy Prevention (P2P share File)
{
        var Privacy detection [];
        For (Page = 1; Page <= Last Page; Page ++)
        {
                If (Read Text = Privacy Pattern) then save Privacy detection[text, location]
                Return privacy detection;
        }
        IF (Privacy detection = Privacy verification) then delete text with location
        Construct P2P share File;
        Return P2P share file;
 }
```

## 4 Evaluating the performance of the proposed system

The proposed system is developed using Java on Windows. The system is installed upstream of the security system of an organization to evaluate the performance. The P2P traffic-identity information is obtained using the security system. If the outgoing traffic is P2P, the file inspection is performed. Figure 5 shows the configuration of the privacy data leakage prevention system proposed for P2P.

The proposed system shared files in the shared folder of the P2P file sharing system user group of the some computer in the organization for 3 days. As a result, 6915 files were shared with the external peers, and the proposed system removed all the privacy data for the external sharing. However, DLP system blocked 5815 files. The privacy which it is unable to block in DLP system was 502 addresses, 202 job, 195 title. In DLP system, because the contents about the privacy was unable to be determined, the address, job and title were unable to be distinguished. In addition, because of blocking the privacy which the privacy detection filter in DLP system coincides with the set regular expression pattern, the privacy false detection was generated. For example, in the case of 2013-0001-0012-0121 patterns like the serial number, it false detection due to the verification functional unpreparedness about the privacy item with the credit card number and it blocked. In the proposed system, the verification for each privacy item was performed and the false-positive rate could be reduced. In addition, there is the defect that there is still the possibility of the leakage of privacy because 5815 share files

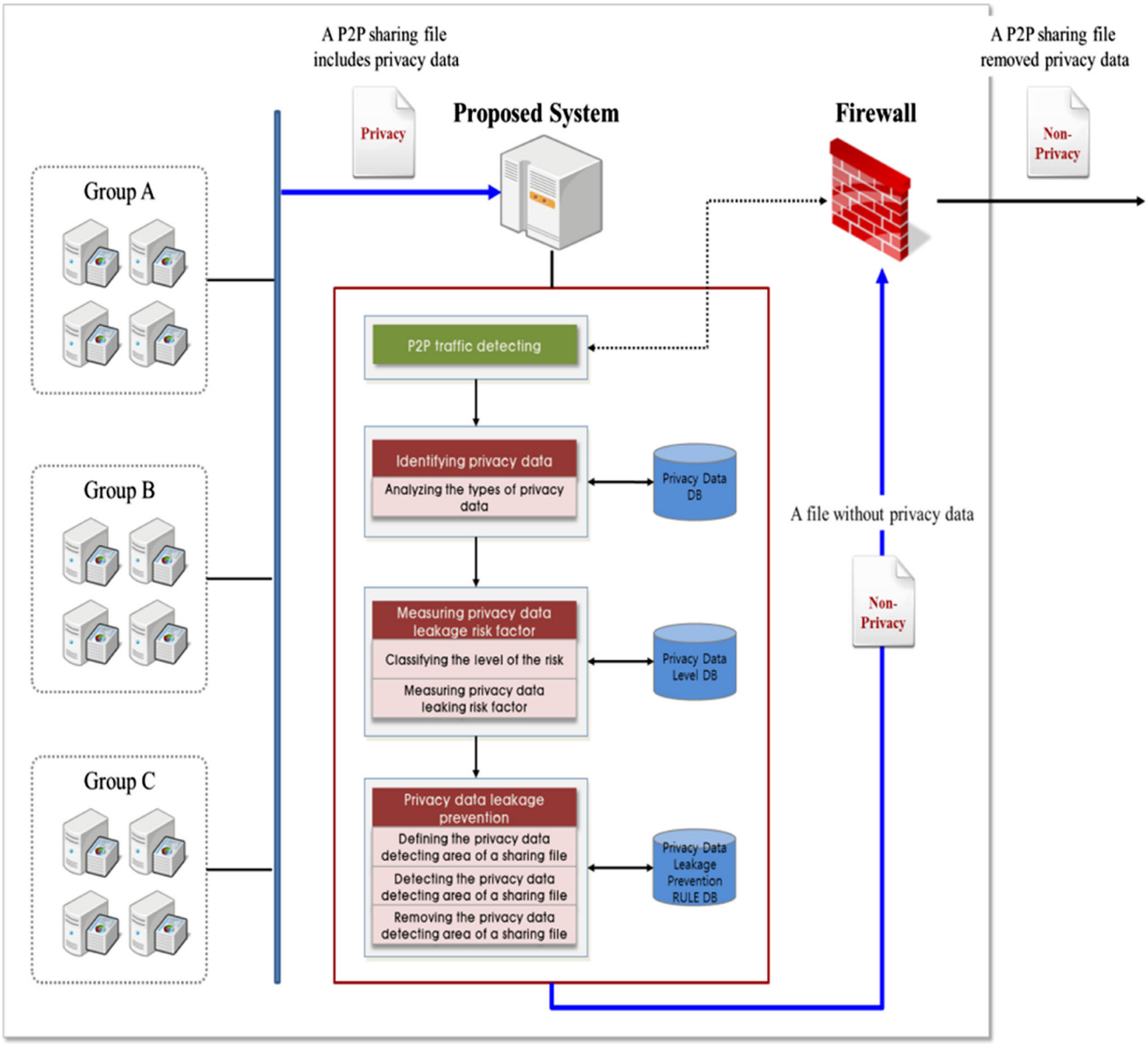


**Fig. 5** Proposed system for privacy data leakage prevention in P2P file sharing

blocked in DLP system are still stored to the shared folder including the privacy.

In the proposed system, in case of implementing the prevention of leakage individual information (the probability of the privacy data leakage risk $P$=100) about all leakage of privacy risk levels the privacy about 6915 files was distinguished and it removed.

From total 6915 P2P sharing files, the algorithm detected 3274 privacy data including 344 resident registration number (10.51 %), 164 financial information (5.01 %), 2369 personal identity number information (72.36 %) and 397 social privacy information (12.13 %). According the analysis, the majority of the leakage was the personal identity number information of customers, and more than 10 % of the private identity information, which is the most sensitive leaked. The proposed system prevents privacy data leakage by removing the detected privacy data. Figure 6 shows the details of the privacy data classification.

Using document coordinate (*, Font, X, Y, Page), the privacy was substituted with * character using. Figure 7 shows the result of removing of the privacy data by the proposed system.

The performance of the P2P sharing file text reading part, the personal information detecting and verifying parts, and the privacy data removing part were evaluated separately for evaluating the performance of the proposed system. With the 100 P2P sharing file the text reading part required average 0.41 s, the privacy data detecting and verifying module required average 3.88 s, and the privacy data removing part required

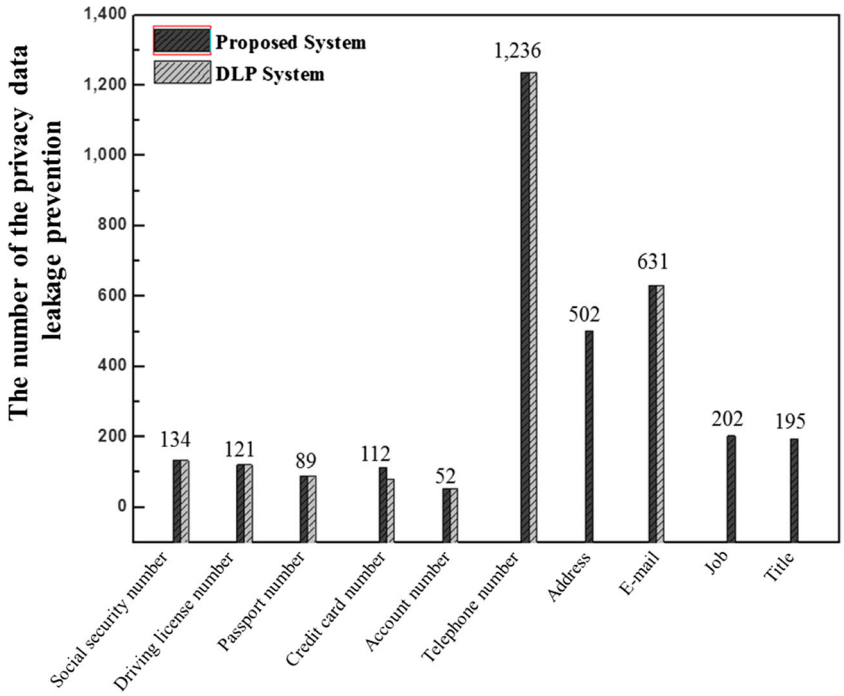


**Fig. 6** Detecting of the privacy data included in the internal P2P sharing file using the proposed system and DLP System

average 7.39 s for processing. Figure 8 shows the result of the process.

Compared with the AES encryption algorithm applied to DLP technologies, the proposed system provides about 16.2 % of performance improvement. Additionally even though DLP technologies encrypt the sharing files, the privacy data was still included in the file. However the proposed method have an advantage of preventing privacy data leakage fundamentally since it removed the information from the sharing file. Figure 9 compares the processing performance by the size of a sharing file between the proposed method and an AES encryption.

## 5 Conclusions

Registered peers to a P2P service can share and exchange information with other peers without servers using P2P

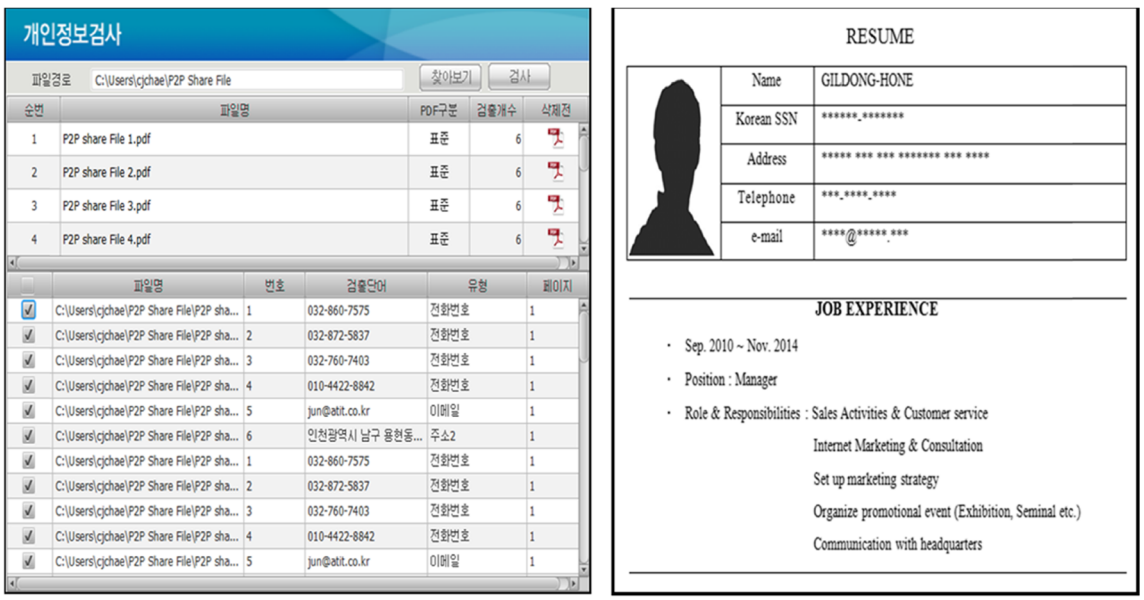


**Fig. 7** The result of removing of the privacy data included in the internal P2P sharing file using the proposed system

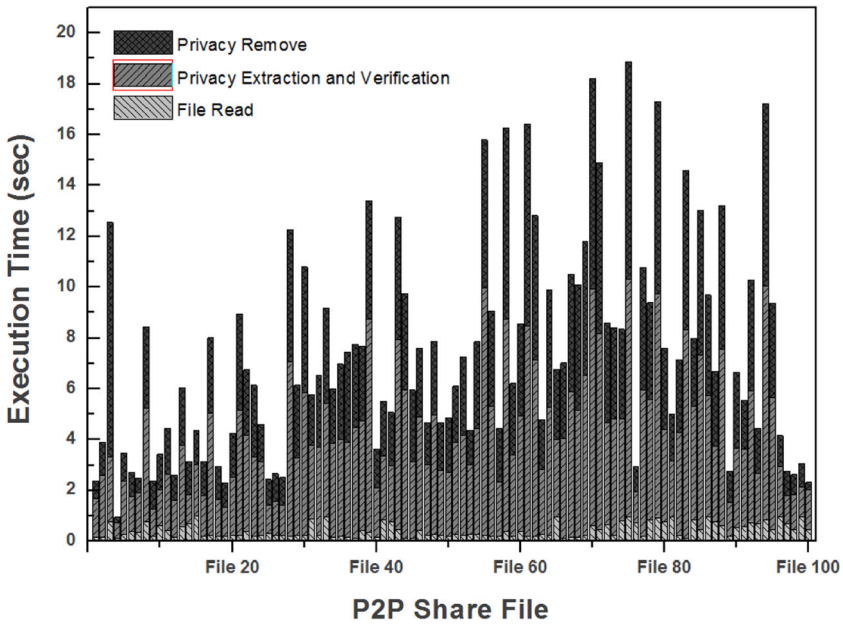


**Fig. 8** Detecting and removing time from the privacy data included in the internal. P2P sharing files using the proposed system

network. This P2P concept means the direct connection between computers, also provides faster and safer network resource sharing and data processing. Due to the advantage the usage rate of a P2P file sharing system increases it has a disadvantage that the privacy data of internal staffs and customers can leak through the P2P file sharing. Thus, we proposed the system that can prevent internal privacy data leakage of the staffs and the customers of an organization through a P2P network. The proposed system identified the privacy data, and removed the information by the privacy data leaking risk factor from the sharing file. This process solved the issues of DLP systems, such as the high detecting-error of the privacy data and invasion of privacy issues. The assessment confirmed that various privacy data could leak when file shared on a P2P network. In this paper, the proposed system prevented the privacy data leakage of a P2P sharing file. However for the future research the privacy data leakage prevention technology for all outgoing files to an external network will be studied.

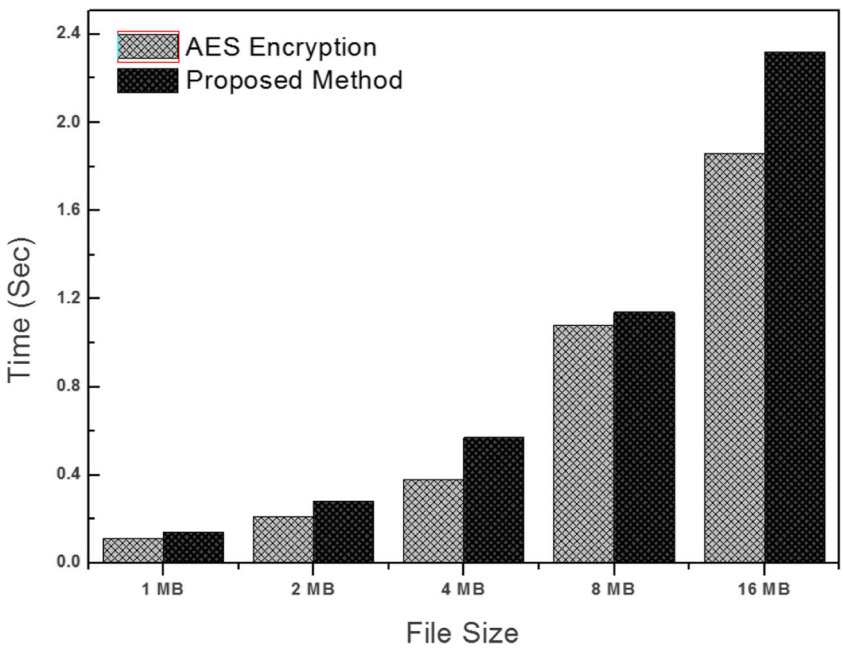


**Fig. 9** Performance comparison between the proposed method and an AES encryption

**Acknowledgments** This research was supported by Maximize the Value of National Science and Technology by Strengthen Sharing/ Collaboration of National R&D information funded by the Korea Institute of Science and Technology Information (KISTI).

## References

1. El-Ansary S, Haridi S (2005) An overview of structured overlay networks. Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless and Peer-to-Peer Networks. CRC, Boca Raton
2. Lua K, Crowcroft J, Pias M, Sharma R, Lim S (2005) A survey and comparison of peer-to-peer overlay network schemes, vol. 7(2). Communications Surveys and Tutorials, Washington, DC
3. Jia D, Yee WG, Nguyen LT, Frieder O (2008) Distributed, automatic file descriptor tuning in P2P file-sharing systems. Peer-to-Peer Netw Appl 1(2):148–161
4. Sasabe M, Wakamiya N, Murata M (2010) User selfishness vs. file availability in P2P file-sharing systems: Evolutionary game theoretic approach. Peer-to-Peer Netw Appl 3(1):17–26
5. Vishnumurthy V, Francis P (2007) A comparison of structured and unstructured P2P approaches to heterogeneous random peer selection. 2007 USENIX Annual Technical Conference, Santa Clara, CA, USA, 17–22 June 2007, pp. 309–322
6. Check Point Security Report (2014) Check point security report homepage. http://www.checkpoint.com/
7. Gheorghe G, Cigno RL, Montresor A (2011) Security and privacy issues in P2P streaming systems: A survey. Peer-to-Peer Netw Appl 4(2):75–91
8. Idota H (2001) The issues for information security of peer-to-peer. Osaka Economic Papers, vol. 51(3)
9. Kim W-S, Kim S (2009) A study on the information effluence state and measure by peer -to-peer programs in Korea and Japan. J Inst Internet Broadcast Commun 9(1):67–74
10. Choi J-U, Lee Y-J, Park J-M (2012) E-DRM-based privacy protection technology for overcoming technical limitations of DLP-based solutions. J Korea Inst Inf Secur Cryptol 22(5):1103–1113
11. Lee D, Kim J, Kim KJ (2010) Data loss prevention research and technology trends. J Korea Inst Inf Secur Cryptol 20(1):56–65
12. Kim J, Park C, Hwang J, Kim H-J (2013) Privacy level indicating data leakage prevention system. KSII Trans Internet Inf Syst 7(3): 558–574
13. Cho S-K, Jun M-S (2012) Privacy leakage monitoring system design for privacy protection. J Korea Inst Inf Secur Cryptol 22(1): 99–106