Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 8, No. 2, 2023

Promotion Mechanism to Information Protection through Virtual-Real Fusion Network

Xirong Gao, Xia Zou

School of Economics and Management, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: To address the increasingly serious information leakage problem, the quantitative mechanism of implementing information protection was explored using information fragmentation tools and the general mechanism of enhancing information protection strength was examined in the virtual-real fusion network. Information fragmentation protection is fragmenting the information content sufficiently and decentralizing the store address sufficiently to prevent others from illegally accessing the information content. The validation analysis using arithmetic examples proved the effectiveness and feasibility of the constructed model for improving information protection. Compared with the virtual network, the virtual-real fusion network can increase the information fragmentation protection strength strength to the infinite status.

Keywords: Virtual-real fusion network, Information protection, Information fragmentation.

1. Introduction

With the continuous development of information economy, network economy and even digital economy, the Internet platform is becoming more and more important in social and economic activities, and more and more market transaction activities are moving from offline to online. It can be expected that future socio-economic activities will be further online in terms of depth and breadth.

However, online transactions are prone to information leakage, and once it happens, it is difficult to be prosecuted through judicial channels. This makes the information leakage become a major problem of the Internet economy. Information protection relies on the system and technology. In view of the opportunistic countermeasures and moral risks that are difficult to eradicate at the institutional level, information protection ultimately relies on technical means. Based on the technical potential of the virtual-real convergence network, this paper explores the full fragmentation of information and the full complexity of keys by relying on the virtual-real convergence network technology to achieve high-strength protection of online information, thereby eliminating the hidden danger of information leakage for the rapid development of the future digital economy.

2. Literature Review

Kim, Wonpo (2020) argues that the large-scale leakage of privacy information occurs, develops and spreads rapidly under the support of emerging technologies such as Internet, big data, artificial intelligence, cloud computing and Internet of Things in the context of 4G/5G[1]. Liu Xianquan et al. (2018) argue that artificial intelligence collects user data with the help of algorithms, and the openness, transparency and legality of the collection process are difficult to guarantee, and pose an unprecedented threat to the security of personal information and privacy[2]. Zhou Linxing et al. (2021) argue that personal information is exposed in full view in the big data environment[3]. Chen Luyong et al. (2018) argued that technological advances have made it particularly easy to obtain consumers' private information, and in addition, the fast and wide spread of online information and the anonymity of the Internet have made some information leaks beyond the jurisdiction and control of the law[4]. Hong Yuan (2017) argues that user information in the Internet era is growing geometrically and rapidly, but the development of information encryption technology is far behind the development of storage media technology of information, and it is also difficult to solve the problem of information leakage in the process of transmission[5].

mark et al. (2021) analyzed the theoretical base of the information leakage notification system from four aspects: deterrence, mitigation, information coercion and personal autonomy[6]. Chen Wanzhu et al. (2022) discussed the way to crack information leakage in health care mainly from the perspective of system design, and argued that the system of personal health care information leakage notification system and the construction of a multi-subject notification system for personal health care information leakage should be improved[7]. Tang, Lin et al. (2022) considered that the reasonable restriction of "discretionary space" is the core of the personal information leakage notification system, and proposed that in improving the personal information leakage notification system, the focus should be on the normalization of the restriction of discretionary space, the weakening of external regulatory indicators and the effectiveness of the content of personal information leakage notification[8]. Liu Yan (2022) argued that a scenario-based dynamic governance approach should be adopted for the security issue of reader information leakage, raising awareness of personal information security maintenance, and fulfilling personal information security protection obligations such as security assessment and leakage notification throughout the data life cycle[9].

The existing literature on information leakage mainly focuses on the design of information leakage prevention systems and models for intervening in privacy dissemination under traditional networks, while there is no research on information protection enhancement mechanisms under virtual-real convergence networks.

3. Information Fragmentation Protection Path

3.1. Sufficiently small information fragmentation discovery probability

(1) Variable setting. Let the total number of cloud servers storing information be N. The maximum number of fragments of a piece of information that can be fragmented in theory is $n \ll N$, and the number of fragments that are actually fragmented is $m \leq n$. Now, *m* fragments of information are stored in several cloud servers.

(2) Scenario 1: The maximum number of information fragments stored in a single server is 1. Under scenario 1, *m* information fragments will occupy *m* servers, forming a "one-to-one" storage model. In this case, there are (C_N^m) combinations of "one-to-one" storage servers for *m* fragments.

Considering that *m* is a variable parameter, i.e., *m* can be any integer in the interval of $[1, n]$, which is $m \in [1, n]$. As a result, the "one-to-one" storage status of *m* information fragments in *m* servers can vary in *n* ways depending on the actual value of *m*. In this case, there are ($\sum_{m=1}^{n} C_N^m$) combinations of "one-to-one" storage servers for *m* fragments of information.

In fact, among the ($\sum_{m=1}^{n} C_N^m$) combinations of "one-to-one" storage servers for *m* pieces of information, there is only one correct combination. Accordingly, under scenario 1, the probability of finding *m* information fragments from *N* cloud servers, i.e., the information fragment discovery probability, is denoted as $F^{(1)}$, which is calculated as in equation (1).

$$F^{(1)} = \frac{1}{\sum_{m=1}^{n} C_N^m} \tag{1}$$

(3) Scenario II: There is no upper limit on the number of information fragments stored by a single server. Under scenario 2, the number of servers occupied by *m* information fragments can be any integer in the interval $[1, m]$, forming a "many-to-one" storage model. In this case, there are ($\sum_{j=1}^{m} C_N^j$) combinations of "many-to-one" storage servers for *m* fragments of information.

Similarly, considering that *m* is a variable parameter, i.e., *m* can take any integer in the interval $[1, n]$ ($m \in [1, n]$). Therefore, the "many-to-one" storage status of *m* information fragments in the server can vary in *n* ways depending on the actual value of m. In this case, the "many-to-one" storage status of *m* information fragments can be changed. In this case, there are $\{\sum_{j=1}^{n}[(n-j+1)C_N^j]\}$ combinations of "many-to-one" storage servers for *m* information fragments.

Similarly, among the $\{\sum_{j=1}^{n}[(n-j+1)C_N^j]\}$ combinations of "many-to-one" storage servers with *m* pieces of information, there is only one correct combination. Accordingly, under scenario 2, the probability of finding *m* information fragment locations from *N* cloud servers, i.e., the information fragment discovery probability, is denoted as $F^{(2)}$, which is calculated as in equation (2).

$$F^{(2)} = 1/\{\sum_{j=1}^{n}[(n-j+1)C_N^j]\} \tag{2}$$

In summary, as long as the number of information fragments is large enough, either $F^{(1)}$ or $F^{(2)}$ will be a sufficiently small value, i.e., the information fragment discovery probability is sufficiently small. Of course, relatively speaking, $F^{(2)}$ is smaller than $F^{(1)}$, which indicates that the information fragment discovery in Scenario 2 is a bit more difficult.

3.2. Sufficiently small sorting probability of information fragments

To sort the *m* actual information fragments from the theoretical *n* information fragments, there will be (A_n^m) sorting choices. Among them, there is only one correct sorting. Therefore, the probability of getting the correct sort can be given by equation (3).

$$G^{(1)} = 1/A_n^m = (n-m)!/n! \tag{3}$$

Considering that *m* can take any value in the interval $[1, n]$, then *m* actual information fragments are taken from the *n* theoretical information fragments for sorting, and there will be ($\sum_{m=1}^{n} A_n^m$) overall sorting choices. Accordingly, the final overall probability of correct sorting will be given by equation (4).

$$G^{(2)} = 1/\left(\sum_{m=1}^{n} A_n^m\right) \tag{4}$$

From equation (4), the correct information fragment sorting probability will be a sufficiently small value as long as the number of information fragments is sufficiently large. In short, the information fragment sorting probability is sufficiently small.

3.3. Sufficiently small information reduction probability

(1) Information reduction probability definition. The "information reduction probability" is defined as the product of the "information fragment discovery probability" and the "information fragment ordering probability", as shown in equation (5).

$$\Omega = F \cdot G \tag{5}$$

(2) Scenario 1: The maximum number of information fragments stored in a single server is 1. Scenario 1 is a "one-to-one" storage mode, and the information fragment discovery probability is $F^{(1)}$ expressed by equation (1). By substituting Eq. (1) and Eq. (4) into Eq. (5), the information restoration probability of Scenario 1 can be obtained as Eq. (6).

$$\Omega^{(1)} = \frac{1}{(\sum_{m=1}^{n} C_N^m) \cdot (\sum_{m=1}^{n} A_n^m)} \tag{6}$$

(3) Scenario 2: There is no upper limit on the number of information fragments stored in a single server. Scenario 2 is a "many-to-one" storage mode, and the information fragment discovery probability is $F^{(2)}$ expressed by equation (2). By substituting Eq. (2) and Eq. (4) into Eq. (5), the information restoration probability in Scenario 2 can be obtained as Eq. (7).

$$\Omega^{(2)} = \frac{1}{\{\sum_{j=1}^{n}[(n-j+1)C_N^j]\} \cdot (\sum_{m=1}^{n} A_n^m)} \tag{7}$$

In summary, as long as the number of information fragments is large enough, both $\Omega^{(1)}$ and $\Omega^{(2)}$ will be a sufficiently small value, that is, the information restoration probability is sufficiently small. Of course, relatively speaking, $\Omega^{(2)}$ is smaller than $\Omega^{(1)}$, which indicates that information restoration is a bit more difficult in Scenario 2.

4. Information Fragmentation Protection Strength and Ranking

4.1. Quantitative expression of information fragmentation degree

The higher the information fragmentation degree is, the smaller the information restoration probability is, and vice versa. Therefore, the information fragmentation degree can be expressed as the inverse of the information restoration probability, i.e., as shown in equation (8).

$$\varphi = \frac{1}{\Omega} = \frac{1}{F \cdot G} \tag{8}$$

The specific value of information restoration probability Ω is calculated by equation (6) in "one-to-one" storage mode, and by equation (7) in "many-to-one" storage mode.

4.2. Information fragmentation protection strength definition

Let the maximum number of times the computer tries to restore information content per unit time be ν, then the value of ν represents the information restoration arithmetic of the computer. At this point, the information fragmentation protection strength can be defined according to equation (9).

$$K = \frac{\varphi}{\nu} = \frac{1}{\Omega \cdot \nu} = \frac{1}{F \cdot G \cdot \nu} \tag{9}$$

5. Conclusion

Aiming at the topic of information protection in the network era, the concept of information fragmentation was defined, the quantitative mechanism of implementing information protection using the information fragmentation tool was explored, and the general mechanism of enhancing information protection strength in the virtual-real convergence network was examined. Specific findings of the study are as follows:

(1) Information protection mechanism refers to the use of network security technology to achieve sufficient concealment of Internet information through certain technical embedded system design, so as to avoid others' snooping and stealing of information content. Commonly used information protection mechanism mainly includes information fragmentation protection mechanism protection mechanism.

(2) Information fragmentation protection mechanism, mainly through the full fragmentation of information content and the full decentralization of storage addresses, fully reduce the probability of information fragmentation discovery, information fragmentation sorting probability and information restoration probability, and then effectively prevent others from illegal access to information content. There are three ways to enhance the intensity of information fragmentation protection: first, to increase the total number of information cloud storage servers; second, to increase the upper limit of the number of information fragments; and third, to reduce the computer information restoration arithmetic.

(3) The way to improve the protection strength of information fragmentation by virtual-real convergence network: significantly increase the total number of cloud storage servers and the maximum number of information fragments, and effectively limit the computer information reduction arithmetic, so as to achieve a significant increase in the protection strength of information fragmentation. Compared with the virtual network, the virtual-real convergence network can increase the information fragmentation protection strength to infinity.

References

[1] Kim, Wonpo. On the leakage and protection of personal privacy data in the era of big data [J]. Journal of Tongji University (Social Science Edition), 2020, 31(03): 18-29.

[2] Liu Xianquan, Lin Yujia. The criminal law response to technological risks in the era of artificial intelligence [J]. Journal of East China University of Political Science and Law, 2018, 21(05): 46-54.

[3] Zhou LX, Han YJ. Research on personal information governance in the big data environment[J]. Intelligence Science, 2021, 39(03): 11-18.

[4] Chen Luyong, Lu Zhipeng. Network monopoly of Internet platform enterprises and citizens' privacy protection--A discussion on the new development and dilemma of citizens' privacy rights in the Internet era[J]. Academic, 2018(07): 38-51.

[5] Hong Yuan. How the Internet information is leaked[J]. People's Forum, 2017(20): 19.

[6] Mark V, Tal Z. Optimizing Breach Notification[J].University of Illinois Law Review,2021,(3):803-864.

[7] Chen Eun-Joo, Sang L-L. A comparative study of Chinese and foreign personal health care information breach notification systems[J]. Modern Intelligence,2022,42(10):123-131+142.

[8] Tang L., Yang L. Personal information leakage notification system in China - a perspective of discretionary regulation (in English) [J]. Science and Technology and Law (in English), 2022(04):115-122. doi:10.19685/j.cnki.cn11-2922/n.2022.04.013

[9] Liu Yan. Risk of personal information leakage of library patrons and its scenario-based management[J]. Library Studies,2022(06):18-26+63.DOI:10.15941/j.cnki.issn1001-0424.2022.06.003.