

## Digital Continuity Guarantee Approach of Electronic Record Based on Data Quality Theory

Yongjun Ren<sup>1,2</sup>, Jian Qi<sup>1</sup>, Yaping Cheng<sup>2</sup>, Jin Wang<sup>3,\*</sup> and Osama Alfarraj<sup>4</sup>

**Abstract:** Since the British National Archive put forward the concept of the digital continuity in 2007, several developed countries have worked out their digital continuity action plan. However, the technologies of the digital continuity guarantee are still lacked. At first, this paper analyzes the requirements of digital continuity guarantee for electronic record based on data quality theory, then points out the necessity of data quality guarantee for electronic record. Moreover, we convert the digital continuity guarantee of electronic record to ensure the consistency, completeness and timeliness of electronic record, and construct the first technology framework of the digital continuity guarantee for electronic record. Finally, the temporal functional dependencies technology is utilized to build the first integration method to insure the consistency, completeness and timeliness of electronic record.

**Keywords:** Electronic record, digital continuity, data quality.

### 1 Introduction

Electronic record is generated in digital devices and digital environment, which is in a digital form to store in tape, magnetic disk, optical disc, etc. This electronic record can be read and processed rely on digital devices, such as computers, and it is transmitted on the Internet [Xie, Wang and Ma (2017); Jiang, Zeadally, Ma et al. (2017); Wang, Gu, Liu et al. (2019)]. With the rapid development of e-commerce, e-government and information system, more and more public information is generated and stored in digital form, and the formats and types of the information are diverse. But the massive and diverse digital public information can't be managed effectively. Moreover, the traditional file storage

---

<sup>1</sup> School of Computer and Software, Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science & Technology, Nanjing, 210044, China.

<sup>2</sup> Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, Nanjing University of Information Science & Technology, Nanjing, 210044, China.

<sup>3</sup> School of Computer & Communication Engineering, Changsha University of Science & Technology, Changsha, 410114, China.

<sup>4</sup> Computer Science Department, Community College, King Saud University, Riyadh, 11437, Saudi Arabia.

\* Corresponding Author: Jin Wang. Email: jinwang@csust.edu.cn.

Received: 27 March 2019; Accepted: 29 September 2019.

strategy is no longer suitable for the storage of the digital record. As result, the digital records are faced with the dilemma of data losing and unavailability.

Some investigations show that about 10% of the electronic record of the government departments in Canadian is unreadable [Xie, Wang and Ma (2017); Qian (2014); Chen, Wang, Xia et al. (2019)]. In 2008, the National Archives and National Library of New Zealand conducted a survey about the electronic record stored by the public sector, in which it showed that [Shen, Zhou, Chen et al. (2017); Wei, Zhang and Ma (2018); Cao, Zhang, Dong et al. (2018)]: about 67% of the electronic record preserved by the public institutions is inaccessible. And about 31% of the controlling index of the record is not available; 20% of the electronic record, which required some special computer software or hardware, is not available; 15% of the electronic record is stored in the medium, which has been obsolete.

Moreover, the regeneration cost will be enormous if these data information lose. The reconnaissance data on Mars in 1957, which is stored on two disks by the National Aeronautics and Space Agency, can't be decoded because of the change of technology. And the National Aviation and Space Agency had to spend a lot of manpower and financial resources to recover the electronic record [Li, Niu, Kumari et al. (2018); Gu, Yang and Yin (2018); Yin, Shi and Wang (2019)]. According to the research of the US National Science Foundation committee, the regeneration of only 20 MB digital information will cost about \$ 64,000 [Ren, Shen, Wang et al. (2015); He, Kumar, Wang et al. (2017); Ge, Liu, Xia et al. (2019)]. More seriously, some digital information can no longer regain once lose.

To solve the problems, in 2007 the UK National Archive firstly proposed the concept of "digital continuity" and launched the "Digital Continuity Project". The aim is to construct the ability of using the digital information according to the required form and the time [Ren, Shen, Liu et al. (2016); Shin, Koo, Hur et al. (2017); Rostami, Sangaiah, Wang et al. (2019)]. In 2009, the National Archive of New Zealand released the Digital Continuity Action Plan to prevent the loss of government information assets and ensure them to be used in the future. The object of the plan is to satisfy the requirement of all the New Zealand public departments for management digital information's identifying, preserving, storage, access, using and so on. The National Archive of Australia presented the 'digital continuity 2020 policy' for government digital information and combined with the digital transformation program and e-government construction to promote the continuity control of public digital information in 2015. Although each country has its own focus, it is aware of the importance of digital continuity of public digital information.

The rest of the paper is organized as follows. Section 2 introduces the related works. Section 3 analyzes the requirements of the digital continuity for electronic record and form the insurance theoretical framework of the digital continuity based on data quality theory. And in Section 4 we define the system model and present the first digital continuity guarantee scheme based on functional dependency theory. Finally, Section 5 concludes this paper.

## **2 Related work**

### ***2.1 Digital continuity***

At present, all countries faced with the serious consequences of bad digital information management, such as digital information is missing, unreadable and difficult to find.

Thus, digital continuity was proposed as a new concept of information management and service. Moreover, it has been widely recognized in the world [An (2016); Upward, Reed, Olive et al. (2013); Li, Liu, Wang et al. (2019)].

Theoretically, digital continuity can be traced back to the record continuum theory. The continuum theory is a basic theory of electronic record operation, which was proposed after the record life cycle theory. In 1996 Frank Upward presented record continuum theory and constructed a record continuum model based on the space-time. The theory reveals the continuity of life movement of electronic record in multiple dimensions. It focuses on the change of record, fond and fond set, and reflects the relation between record preserving form, the business activities and business environment [Wang, Cao, Li et al. (2015); Zeng, Dai, Wang et al. (2019); Wang, Gao, Yin et al. (2018)]. It reveals the method of the consistence management in the whole process management from the formation of records to the preserved archives.

Digital continuity emphasizes the long-term preservation of digital resources, and deals with missing or unreadable of electronic record, which are caused by IT technological change. Some scholars regard it as a theory of long-term preservation of digital information [Huang (2014); Yuan and Wang (2016); Gong, Bo, Tao et al. (2018)]. Though, the view points out the core issue of digital continuity and represents the core target of digital continuity, it doesn't point out that the nature of digital continuity is a continuous process, rather than the simply result of long-term preservation.

## ***2.2 Digital continuity project***

UK National Archive pioneered the concept of the digital continuity and launched the research of the Digital Continuity Project in 2007. Digital continuity is the ability to use your information in the way that you need, for as long as you need. Managing digital continuity is essential if you are to protect the digital information you depend on to do business. Losing your digital continuity could have serious consequences [ISO (2010); ISO (2008); Yan, Zhang, Wan et al. (2019)]. This concept is based on the idea of the risk management of some "changes", i.e., any one or more changes of the information management, technology and business are likely to bring the loss of digital information and digital continuity.

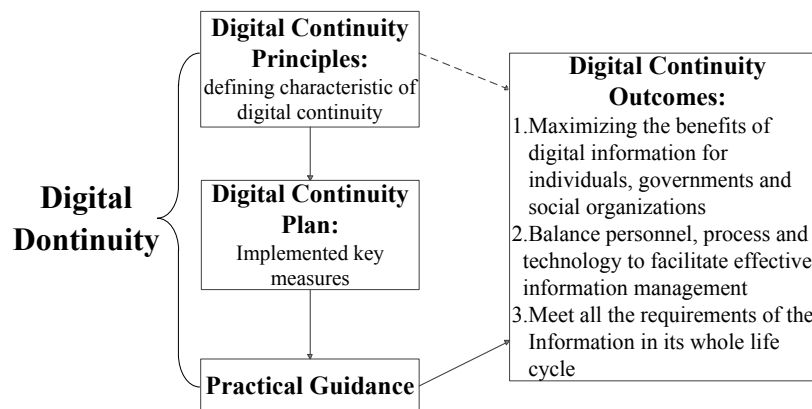
Since 2009, the National Archives of New Zealand National released the Digital Continuity Action Plan to prevent the loss of government information assets and to ensure the long time available for the future [Archives New Zealand (2016); Jia (2016)]. The plan faced all the New Zealand public departments for management digital information's identifying, storage, access, re-use and etc., and it emphasized on making the management of the government digital information be effective and economic. The public departments contain government departments, Royal research institutions, the Royal enterprises, state enterprises, local health committees, higher education institutions and so on. The key issues of the plan include long-term preservation of information, conservation and use of government information, authenticity and reliability of government information, openness and transparent of government information, trust access to government information (sensitive and private information's protection), the economy, efficiency and sustainability of government information management. The

digital continuity of New Zealand is comprehensive analyzed from the environmental level, the legal, business and international environment, and the necessity, feasibility and objective of digital continuity are shown in Tab. 1.

**Table 1:** Action plan of digital continuity plan of the New Zealand

Objective	Action
<b>Responsibility:</b> the head of digital continuity in public department effectively communicates and form the consensus.	Enhance the understanding of digital continuity issues for public department in the strategic sector. Form practice zone cross industry and inter department. Coordinate the existing legal definition and compile the glossary.
<b>Usability:</b> Citizens and the public sector can use public information in the present and future, and the information will be able to prevent access and use without authorization.	Reuse of information and data of the government department. Make sure that certain types of information are limited to access, and the limited strategy is updated according to the data attributes. Understand and consider the views and interests of the group.

In 2015, the National Archive of Australia launched the “digital continuity 2020 policy” for government digital information, which combined with the digital transformation plan and e-government construction, in order to promote the continuity control of public digital information [NAA (2015); Xiao and Wu (2015)]. Digital continuity strategy consists of principle of digital continuity, digital continuity plans, guidelines and practical results, and other digital continuity of the constitution, as shown in Fig. 1.



**Figure 1:** Digital continuity plan of the Australian national archive

Digital continuity is a basic strategy, which ensured that preserved digital information can be used as needed; and then the principle of digital continuity is summarized based on the measures. A series of key measures implemented under the principle of digital continuity is called the digital continuity plan; and the goal of the policy is to achieve

digital continuity [Qian, Shao, Zhu et al. (2018); Wang, Cao, Ji et al. (2017); He, Yu, Zhang et al. (2017)].

### **3 Problem statement**

Generally, digital information is more vulnerable than paper for several reasons, including:

- (1) There is more of it and it is created in a diverse range of formats; opening and using it depends on hardware and software that can become unsupported.
- (2) It can be stored in a variety of places, making it harder to find.
- (3) It is easy to lose essential metadata and context required to understand the information when it is moved between organizations and systems.
- (4) Multiple versions of the same information can exist, making it difficult to determine which version is most accurate or up to date.
- (5) Essential audit data that tells us what has happened to the information, who accessed or changed it and when, can be lost-making it difficult to trust the information.

Digital continuity is a useful method of protecting the long-term use of the information. Specifically, it refers to the maintenance and management of digital information to ensure that it is can be used now and future when needed [Kaur and Kaur (2017); Zhu, Gao, Shen et al. (2017); Wu, Li and Jiang (2017); Wang, Xu and Pei (2017)]. Thus, the information is complete, accessible, and available under the guidance of digital continuity.

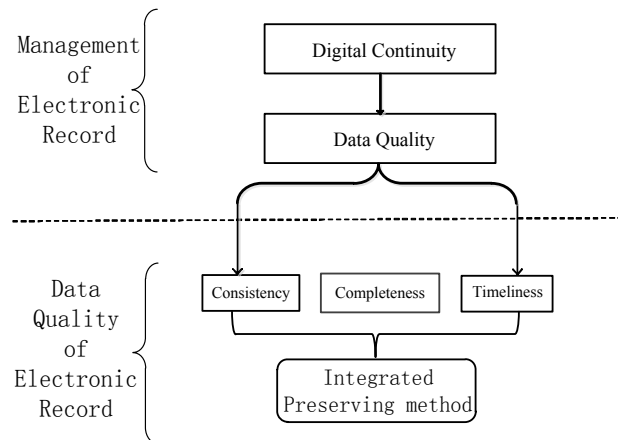
Digital continuity focuses on the risk management and control of some changes. The changes mainly contain that the information and information management (including ownership, staff, policies and procedures, etc.), technology (including hardware, software, format migration, etc.), business (including information can be found and read, operable, understandable and credible demand). The changes of one or more of these three factors may cause the loss of the digital continuity of the digital information [Wang, Zhao and Hou (2012); Liu, Feng and Li (2014); Fu, Wen, Ma et al. (2018)].

### **4 Digital continuity of electronic record based on data quality theory**

According to the theory of data usability, the digital continuity of electronic record can be embodied as data consistency, data completeness and data timeliness. The conceptual framework is shown in Fig. 2.

Data consistency need to ensure that each information in the data set does not include semantic errors or conflicting data. Data completeness requires that there are enough data in the data set to answer various queries and supports for a variety of computing, ensures that electronic documents are complete and unaltered. The completeness contains two aspects. One is the completeness of the single record; the other is the completeness of the fonds. The completeness of the single record refers to the completeness of the single copies of electronic record content, and the context and structure information have no missing or be damaged; the completeness of fonds means that the electronic record and related records are complete, which recorded the activity of document in its life cycle. And the organic connection between records can be revealed and maintained. On one hand, no change means the documents cannot be arbitrarily altered since they have been

generated. On the other hand, they must have a clear basis and detailed record when they need to be changed in special circumstances. That record management policies and procedures should be made clear: which can be added or annotated to the electronic record, under which conditions can be authorized to add or comment after the record is formed. Timeliness of data is to ensure that each record of the information set can be advance with the times. For example, a user in the database address is correct in 2015, but in 2016 may not be correct, that is, data is outdated.



**Figure 2:** The architecture of digital continuity guarantee based on data quality theory

To ensure digital continuity, it is necessary to have an accurate examination of the information management status of each institution. Thus, the digital continuity plan recommends that the digital information and processing are recorded, which are created, captured and used during the business management process. Moreover, the plan requires a clear responsibility, obligations, conditions, costs, benefits and risks of digital information management. The consistency, completeness, timeliness and accuracy of data are not only the basic properties of the digital continuity, but also the essential requirement of the realization of the digital continuity [Zhang, Wang, Liu et al. (2015); Zeng, Mu, He et al. (2018); Zhang, Jin, Sun et al. (2018)].

The digital continuity preserving of electronic record is dependent on the unification of its consistency, completeness, and currency. Hence, constructing a digital continuity preserving scheme based on the unification of data consistency, data completeness, and data currency is a challenge.

## 5 Digital continuity guarantee based on functional dependency

In classical relational data systems, functional dependency theory defines the semantics relationship between attributes. The theory is the abstract reflection of the built-in link of data in the real-world, and plays an important role in designing data normalization, integrating schema, optimizing query, updating data etc. In recent years, researchers have begun to use it to clean data, analyze the semantic relationship between data, detecting the inconsistent and incomplete of damaging functional dependency. Moreover, it can improve

the quality of the data by repairing data based on functional dependency technology [Juels and Kaliski (2007); Wang, Zuo, Shen et al. (2015); Cao, Zeng, Ji et al. (2018)].

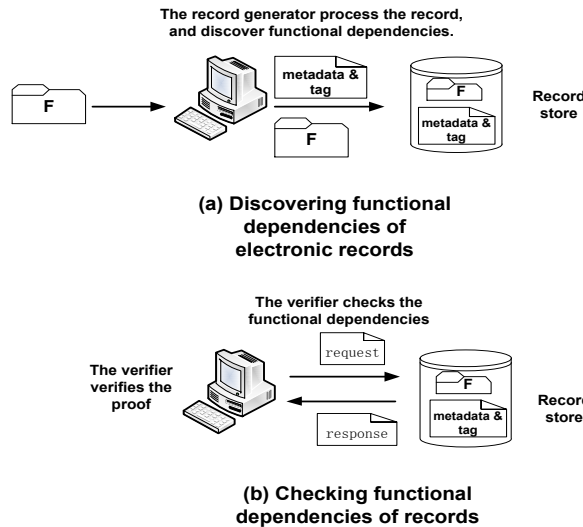
Temporal functional dependency (TFD) is a time-related functional dependency. In addition to providing data consistency and data completeness like the traditional functional dependencies, it can provide data timeliness. So, for the first time, the paper proposes the integrated guarantee method of digital continuity for electronic record based on temporal functional dependency technology.

**5.1 System model**

A representative architecture of the digital continuity guarantees for electronic record based on temporal functional dependencies is illustrated in Fig. 3.

Two processes are presented as follows:

- (1) Record Processing: the generators of electronic record process electronic record and produce the corresponding meta-data, store them in the database; And then the discovery algorithms of functional dependency are run to find the function dependencies in the electronic record and its metadata.
- (2) According to the found functional dependencies, the verifiers of the electronic record run functional dependency checking algorithms to verify whether the current stored electronic record still meets these functional dependencies.



**Figure. 3:** Digital continuity guarantee method of electronic record

**5.2 Integration method of digital continuity guarantee**

In recent years, people have made broad researches about the discovery algorithms of functional dependency [Qian, Shao, Zhu et al. (2018)]. Thus, we will describe whether a temporal relationship  $r \in R$  in electronic record meets a corresponding temporal functional dependency  $[E - Exp(R), t - Group(i)]X \rightarrow Y$ . We do it by following inquiry and verifying whether the result is null:  $\sigma_{cnd}(E - Exp(R)) \diamond_{X=\hat{X}, \rho_{W \rightarrow \bar{W}}} E -$

$Exp(R)$ ), where  $W$  is  $E - Exp(R)$ , and  $cnd$  represents  $\bigvee_{A \in Y} (A \neq \hat{A}) \wedge SameTGroup$ . According to  $T - Group$ ,  $SameTGroup$  will verify that every given valid time in the same group. Thus, if  $E - Exp(R)$  is defined on  $\subseteq UU' \cup \{VT, VT'\}$ , we have  $SameTGroup \equiv VT \in T - nGroup(i) \wedge VT' \in T - Group(i) \wedge V\hat{T} \in T - Group(i) \wedge V\hat{T}' \in T - Group(i)$ . If  $E - Exp(R)$  is defined on  $U \cup \{VT\}$ , we will have  $SameTGroup \equiv VT \in T - Group(i) \wedge V\hat{T} \in T - Group(i)$ . So, according to the difference of the definitions of the temporal group,  $SameTGroup$  generates two different forms: finite set at different intervals or intersecting finite set. First, we consider the condition when  $E - Exp(R)$  is defined on  $U \cup \{VT\}$ . We tested TFD among limited database instances. And the temporal grouping will return a finite set of given granularities, in which each element consists of a number of time segments and these periods are intersecting.

We first consider the issue of the time interval. The time interval can be simulated by the relationship  $Gran$  in the  $(G - id, I, G_s, G_e)$ , where  $G - id$  is the time interval mark,  $G_s, G_e$  represents the start and end time of the event respectively.  $I$  is the granularity mark and can be omitted.  $T - Group(i)$  is used to represent the time granularity of the  $I$ -th time interval. Testing whether the temporal relation  $r \in R$  meets a temporal functional dependency  $[E - Exp(R), t - Group(i)]X \rightarrow Y$  equals to test whether the result of the following query is null:  $\sigma_{cnd}(E - Exp(R) \diamond_{X=\hat{X}, \rho_{W \rightarrow \hat{W}}} E - Exp(R) \diamond \sigma_{G-id=G} Gran)$ , where  $cnd$  represents  $\bigvee_{A \in Y} (A \neq \hat{A}) \wedge G_s \leq VT \wedge VT \leq G_e \wedge G_s \leq V\hat{T} \wedge V\hat{T} \leq G_e$ .

Now, let us consider the case of a limited set of intersecting. Without loss of generality, it assumes that the time of intersection in a finite set can be expressed by the relation  $tGroup$  among the attributes  $(I, T_1, T_2)$ , where  $I$  is the group index,  $(T_1, T_2)$  belong to the same order pair of the time point in the temporal groups, and the temporal groups can be identified by the value of group index. It is known that verifying whether a temporal relation  $r \in R$  meets a temporal functional dependency  $[E - Exp(R), t - Group(i)]X \rightarrow Y$  equals to test whether the result of the following query is null:  $\sigma_{cnd}(E - Exp(R) \diamond_{X=\hat{X}, \rho_{W \rightarrow \hat{W}}} E - Exp(R) \diamond tGroup)$ , where  $cnd$  represents  $\bigvee_{A \in Y} (A \neq \hat{A}) \wedge VT = T_1 \wedge V\hat{T} = T_2$ . In practical situations, we can avoid the connection with  $tGroup$  through including the temporal groups to  $cnd$ .

We take an example and illustrate how to verify the relationship of temporal functional dependencies by querying to each time function dependence. When a patient in the hospital for treatment, the hospital needs to collect a variety of information, such as the doctor's treatment and possible surgery status, this kind of information is time-sensitive. For example, cancer patients often require several courses of chemotherapy treatment. Each chemotherapy cycle is required medication according to a predetermined chemotherapy. A relational schema can be used to represent the treatment during this period. Each patient needs to record and store the treatment regimen, the number of therapeutic drugs, drugs used time and etc. in electronic record. And these information can be represented by the attribute set  $Chemo, PatId, BG, Phys, Drug, Qty, VT$ . The following is the corresponding requirements for the electronic record system that stores the information.



- (1) Patients must take given drug at a certain time every day. Because chemotherapy may produce some side effects, patients must take some cancer drugs to counteract its effects. Thus, some possible data insertion errors can be prevented by testing the temporal functional dependency of electronic record.
- (2) In the course of chemotherapy, according to the determined treatment, patients must take predetermined a number of drugs every day; and if the treatment plan is not changed, the daily medication will not change.
- (3) For specific treatment programs, no matter whether the managers are changed, the daily medication will not change.
- (4) For the patients undergoing the same treatment regimen, if the same number of drugs is taken that day, the number of drugs is the same taken in the next day.
- (5) For the same physician to the same cancer patient, the quantity of the second day's prescribed drug depends on the number of the first day's quantity.

**Pure temporally grouping TFDs.** Among the temporal function dependencies,  $E - Exp(R)$  returns the temporal relation  $r$ . This will enable the functional dependency  $X \rightarrow Y(X, Y \subseteq U)$  to be checked on every maximal subset of  $r$  consisting of tuples, whose  $VT$  values belong to the same temporal group  $t - Group(i)$ . In this example, whether the patient entity meeting the following query will be verify:

$$\sigma_{Qty \neq \bar{Q}ty} \wedge (V\bar{T} - VT)(Patient \diamond_{Chemo=Chemo' \wedge PatId=PatId' \wedge Drug=Drug'} \rho_{W \rightarrow \bar{W}} Patient) \quad (1)$$

**Pure temporally evolving TFDs.** Among the temporal function dependencies,  $E - Exp(R)$  returns a relationship of the property  $U\bar{U} \cup \{VT, V\bar{T}\}$ , which is completed by means of joining operations on some subset of  $U$ .  $Top(i)$  means all the top  $i$  time points which are collected during the monotonically non-empty interval. Then the requirement (2) can be captured by the following temporal functional dependency:

$$[\chi_{PatId, Chemo, Drug}(Patient), Top(i)] Drug, Qty \rightarrow \bar{Q}ty \quad (2)$$

And the requirement (3) can be captured by the following formula:

$$[\chi_{PatId, Chemo, Drug, Phys}(Patient), Top(i)] Drug, Qty \rightarrow \bar{Q}ty \quad (3)$$

The temporal functional dependency can be checked by verifying whether the following query is null:

$$\sigma_{\bar{Q}ty \neq \bar{Q}ty} (\chi_{PatId, Chemo}(Patient) \diamond_{Qty = \bar{Q}ty \wedge Drug = Drug'} \rho_{W \rightarrow \bar{W}} \chi_{PatId, Chemo, Drug}(Patient)) \quad (4)$$

**Temporally mixed TFDs.** Among the temporal function dependencies,  $E - Exp(R)$  returns a relationship of the property  $U\bar{U} \cup \{VT, V\bar{T}\}$ , which is completed by means of joining operations on some subset of  $U$ . The temporal groups are determined through their  $VT$  values. With this method, the dynamic dependencies can be defined, which requires all the time points all belonging to the same temporal group. The function dependency can be described as follows:

$$[\chi_{PatId, Drug}(Patient), Month(i)] Drug, Qty \rightarrow \bar{Q}ty \quad (5)$$

To verify whether the patients meet the functional dependency, one can test whether the following query is null:

$$\sigma_{\tilde{Q}ty \neq \hat{Q}ty \wedge G_s \leq VT \wedge VT \leq G_e \wedge G_s \leq V\hat{T} \wedge V\hat{T} \leq G_e} (\iota_{PatId, Drug}(Patient)) \diamond_{Qty = \tilde{Q}ty \wedge Drug = Drug'} \rho_{W \rightarrow \hat{W}} \iota_{PatId, Drug}(Patient)) \quad (6)$$

**Temporally hybrid TFDs.** Among the temporal function dependencies,  $E - Exp(R)$  returns a relationship of the property  $U\bar{U} \cup \{VT\}$ , which is completed by means of join operations on some subset of  $U$  and further renaming, project, and union operations. The temporal groups are determined through their  $VT$  values. Such class of requirements is captured neither by dynamic dependencies nor the other grouping TFDs proposed in the literature. It can be described as following functional dependency:  $[He^{Patient}, Top(i)]Chemo, Drug \rightarrow Qty$ , where

$$\begin{aligned} He^{Patient} = \{ & t | \exists t' (t' \in \iota_{PatId, Chemo, Drug}(Patient) \wedge t'[VT] = t'[VT] \wedge \\ & t[PatId, Chemo, Drug] = t'[PatId, Chemo, Drug] \wedge \\ & ((t[BG, Phys, Qty] = t'[BG, Phys, Qty] \wedge t[VT] = t'[VT]) \vee \\ & (t[BG, Phys, Qty] = t'[BG', Phys', \tilde{Q}ty] \wedge t[VT] = t'[VT])) \} \end{aligned} \quad (7)$$

To verify whether the functional dependency is met, one can test whether the following query is null:

$$\sigma_{\tilde{Q}ty \neq \hat{Q}ty} (He^{Patient} \diamond_{Chemo = Chemo' \wedge Drug = Drug'} \rho_{W \rightarrow \hat{W}} He^{Patient}(Patient)) \quad (8)$$

## 6 Conclusion

In this paper we analyze the requirements of the digital continuity of electronic record according to the data quality theory. Moreover, the protection theory and technology system for digital continuity of electronic record are constructed based on data quality theory. Thirdly, this paper focuses on the study of the integration method to insure the consistency, completeness and timeliness of electronic record. In addition, according to the actual needs of data quality, the corresponding functional dependency technology is provided to construct the first scheme of digital continuity guarantee for electronic record.

**Acknowledgement:** This work is supported by the NSFC (Nos. 61772280, 61772454), the Changzhou Sci & Tech Program (No. CJ20179027), and the PAPD fund from NUIST. Prof. Jin Wang is the corresponding author.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

- An, X.** (2016): Accelerate the formulation of the government's digital continuous action plan to modernize the state's governance capacity. *China Archives*, vol. 2868, no. 3.
- Archives New Zealand.** (2016): Digital continuity action plan: managing information for public sector efficiency [EB/OL].
- Cao, D.; Zheng, B.; Ji, B.; Lei, Z.; Feng, C.** (2018): A robust distance-based relay selection for message dissemination in vehicular network *Wireless Networks*.

- Cao, L.; Zhang, J.; Dong, X.; Xi, C.; Wang, Y. et al.** (2019): A based on blinded CP-ABE searchable encryption cloud storage service scheme. *International Journal of Communication Systems*, vol. 31, no. 10, pp. e3566.
- Chen, Y.; Wang, J.; Xia, R.; Zhang, Q.; Cao, Z. et al.** (2019): The visual object tracking algorithm research based on adaptive combination kernel. *Journal of Ambient Intelligence and Humanized Computing*.
- Fu, Y.; Wen, S.; Ma, L.; Shu, J.** (2018): Survey on single disk failure recovery methods for erasure coded storage systems. *Journal of Computer Research and Development*, vol. 55, no. 1, pp. 1-13.
- Ge, C.; Liu, Z.; Xia, J.; Fang, L.** (2019): Revocable identity-based broadcast proxy re-encryption for data sharing in clouds. *IEEE Transactions on Dependable and Secure Computing*.
- Gong, L.; Bo, Y.; Tao, X.; Chen, J.; Wang, W.** (2018): Secure rational numbers equivalence test based on threshold cryptosystem with rational numbers. *Information Science*, vol. 46, pp. 44-54.
- Gu, K.; Yang, L.; Yin, B.** (2018): Location data record privacy protection based on differential privacy mechanism. *Information Technology and Control*, vol. 47, no. 4, pp. 639-654.
- He, D.; Kumar, N.; Wang, H.; Wang, L.; Choo, K.** (2017): Privacy-preserving certificateless provable data possession scheme for big data storage on cloud. *Applied Mathematics and Computation*, vol. 314, no. 12, pp. 31-43.
- Huang, Y.** (2014): Research on the connotation and management of trusted electronic records. *Zhejiang Archives*, vol. 31, no. 5, pp. 12-15.
- He, P.; Yu, G.; Zhang, Y.; Bao, Y.** (2017): Survey on blockchain technology and its application prospect. *Computer Science*, vol. 44, no. 4, pp. 1-7.
- ISO.** (2010): *Information and Documentation-Principles and Functional Requirements for Records in Electronic Office Environments* (ISO 16175).
- ISO.** (2008): *Information and Documentation-Work Process Analysis for Records* (ISO/TR 26122).
- Jiang, Q.; Zeadally, S.; Ma, J.; He, D.** (2017): Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access*, vol. 5, pp. 3376-3392.
- Jia, X.** (2016): Analysis and implications of the New Zealand digital continuity action plan. *Library and Information Work*, pp. 45-51.
- Juels, A.; Kaliski, B.** (2007): PORs: proofs of retrievability for large files. *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 598-609.
- Kaur, J.; Kaur, K.** (2017): A fuzzy approach for an IoT-based automated employee performance appraisal. *Computers, Materials & Continua*, vol. 53, no. 1, pp. 23-36.
- Liu, Q.; Feng, D.; Li, B.** (2014): Ustor: cloud storage system based on regenerating codes. *Journal of Communications*, vol. 35, no. 4, pp. 166-173.

- Li, W.; Liu, H.; Wang, J.; Xiang, L.; Yang, Y.** (2019): An improved linear kernel for complementary maximal strip recovery: simpler and smaller. *Theoretical Computer Science*, vol. 786, no. 27, pp. 55-66.
- Li, X.; Niu, J.; Kumari, S.; Wu, F.; Sangaiah, A. et al.** (2018): A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *Network and Computer Applications*, vol. 103, pp. 194-204.
- NAA: National Archives of Australia** (2015): *Digital Continuity 2020 Policy* [EB/OL]. <http://www.naa.gov.au/records-management/digital-transition-and-digital-continuity/digital-continuity-2020/index.aspx>.
- Qian, Y.** (2014): Study on the long-term preservation standard of trusted electronic records in China. *Archives Science Bulletin*, vol. 3, pp. 75-79.
- Qian, W.; Shao, Q.; Zhu, Y.; Jin, C.; Zhou, A.** (2018): Research problems and methods in blockchain and trusted data management. *Journal of Software*, vol. 29, no. 1, pp. 150-159.
- Ren, Y.; Shen, J.; Liu, D.; Wang, J.; Kim, J.** (2016): Evidential quality preserving of electronic record in cloud storage. *Journal of Internet Technology*, vol. 17, no. 6, pp. 1125-1132.
- Ren, Y.; Shen, J.; Wang, J.; Han, J.; Lee, S.** (2015): Mutual verifiable provable data auditing in public cloud storage. *Journal of Internet Technology*, vol. 16, no. 2, pp. 317-323.
- Rostami, S. M. H.; Sangaiah, A. K.; Wang, J.; Liu, X.** (2019): Obstacle avoidance of mobile robots using modified artificial potential field algorithm. *Eurasip Journal on Wireless Communications and Networking*, vol. 2019, no. 1.
- Shin, Y.; Koo, D.; Hur, J.; Yun, J.** (2017): Secure proof of storage with deduplication for cloud storage systems. *Multimedia Tools & Applications*, vol. 76, no. 19, pp. 19363-19378.
- Shen, J.; Zhou, T.; Chen, X.; Li, J.; Susilo, W.** (2017): Anonymous and traceable group data sharing in cloud computing. *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 912-925.
- Upword, F.; Reed, B.; Oliver, G.; Evans, J.** (2013): Record keeping informatics: re-figuring a discipline in crisis with a single minded approach. *Records Management Journal*, vol. 23, no. 1, pp. 47-54.
- Wang, J.; Cao, J.; Li, B.; Lee, S.; Sherratt, R.** (2015): Bio-inspired ant colony optimization based clustering algorithm with mobile sinks for applications in consumer home automation networks. *IEEE Transactions on Consumer Electronics*, vol. 61, no. 4, pp. 438-444.
- Wang, J.; Zuo, L.; Shen, J.; Li, B.; Lee, S.** (2015): Multiple mobile sinks based routing algorithm for data dissemination in wireless sensor networks. *Concurrency and Computation: Practice and Experience*, vol. 27, no. 10, pp. 2656-2667.
- Wang, Y.; Xu, F.; Pei, X.** (2017): Research on erasure code-based fault-tolerant technology for distributed storage. *Chinese Journal of Computers*, vol. 40, no. 1, pp. 236-255.
- Wang, Y.; Zhao, Y.; Hou, F.** (2012): Minimum bandwidth regeneration code of distributed storage system. *Journal of Chinese Computer Systems*, vol. 33, no. 8, pp. 1710-1714.

- Wei, F.; Zhang, R.; Ma, C.** (2018): A provably secure anonymous two-factor authenticated key exchange protocol for cloud computing. *Fundam*, vol. 157, no. 1-2, pp. 201-220.
- Wang, J.; Gao, Y.; Yin, X.; Li, F.; Kim, H.** (2018): An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks. *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1-9.
- Wu, Z.; Li, W.; Jiang, S.** (2017): Research and application of the provenance information packaging strategy based on the OAIS information model. *Library and Information Service*, vol. 61, no. 18, pp. 113-118.
- Wang, J.; Cao, J.; Ji, S.; Park, J. H.** (2017): Energy efficient cluster-based dynamic routes adjustment approach for wireless sensor networks with mobile sinks. *Journal of Supercomputing*, vol. 73, no. 7, pp. 3277-3290.
- Wang, J.; Gu, X.; Liu, W.; Sangaiah, A. K.; Kim, H.** (2019): An empower hamilton loop based data collection algorithm with mobile agent for WSNs. *Human-Centric Computing and Information Sciences*, vol. 9, no. 18.
- Xiao, Q.; Wu, L.** (2015): Research on digital continuity plan of Australian National Archives. *Journal of Information Resources Management*, vol. 5, no. 4, pp. 19-23.
- Xie, L.; Wang, J.; Ma, L.** (2017): The project of InterPARES: where it has been and where it is going. *Archives Science Study*, vol. 4, pp. 14-20.
- Xie, L.; Wang, J.; Ma, L.** (2017): Trusting records: findings of team Asia InterPARES. *Archives Science Study*, vol. 4, pp. 8-13.
- Yan, C.; Zhang, S.; Wan, G.; Yan, L.; Zhang, Y. et al.** (2018): Practical two-way QKD-based quantum private query with better performance in user privacy. *International Journal of Theoretical Physics*, vol. 58, no. 7, pp. 2069-2080.
- Yin, C.; Shi, L.; Wang, J.** (2019): Improved collaborative filtering recommendation algorithm based on differential privacy protection. *Journal of Supercomputing*, pp. 1-14.
- Yuan, Y.; Wang, F.** (2016): Blockchain: the state of the art and future trends. *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481-494.
- Zeng, D.; Dai, Y.; Wang, J.; Li, F.; Sangaiah, A. K.** (2019): Aspect based sentiment analysis by a linguistically regularized CNN with gated mechanism. *Journal of Intelligent Fuzzy*, vol. 36, no. 5, pp. 3971-3980.
- Zeng, S.; Mu, Y.; He, M.; Chen, Y.** (2018): New approach for privacy-aware location-based service communications. *Wireless Personal Communications*, vol. 101, no. 2, pp. 1057-1073.
- Zhang, J.; Jin, X.; Sun, J.; Wang, J.; Sangaiah, A. K.** (2018): Spatial and semantic convolutional features for robust visual object tracking. *Multimedia Tools and Applications*.
- Zhang, N.; Wang, C.; Liu, Z.; Wang, W.** (2015): Study on the evaluation strategy of electronic document authenticity based on digital continuity thought. *Archives Research*, vol. 6, pp. 69-72.
- Zhu, L.; Gao, F.; Shen, M.; Li, Y.; Zheng, B. et al.** (2017): Survey on privacy preserving techniques for blockchain technology. *Journal of Computer Research and Development*, vol. 54, no. 10, pp. 2170-2186.