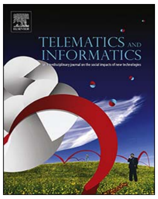
Telematics and Informatics xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele



Recovery of business intelligence systems: Towards guaranteed continuity of patient centric healthcare systems through a matrix-based recovery approach

Ramzi A. Haraty[a,*], Sanaa Kaddoura[b], Ahmed Sherif Zekri[c,d]

[a] Department of Computer Science and Mathematics, Lebanese American University, Beirut, Lebanon
[b] Department of Mathematics and Computer Science, Beirut Arab University, Beirut, Lebanon
[c] Department of Mathematics and Computer Science, Faculty of Science, Beirut Arab University, Egypt
[d] Department of Mathematics and Computer Science, Faculty of Science, Alexandria University, Egypt

ARTICLE INFO

Keywords:
Damage assessment
Data dependency
Healthcare data
Recovery
Transaction depedency

ABSTRACT

With the intensive use of the internet, patient centric healthcare systems shifted away from paper-based records towards a computerized format. Electronic patient centric healthcare databases contain information about patients that should be kept available for further reference. Healthcare databases contain potential data that makes them a goal for attackers. Hacking into these systems and publishing their contents online exposes them to a challenge that affects their continuity. Any denial of this service will not be tolerated since we cannot know when we need to retrieve a patient's record. Denial of service affects the continuity of the healthcare system which in turn threatens patients' lives, decreases the efficiency of the healthcare system and increases the operating costs of the attacked healthcare organization. Although there are many defensive security methods that have been devised, nonetheless malicious transactions may find a way to penetrate the secured safeguard and then modify critical data of healthcare databases. When a malicious transaction modifies a patient record in a database, the damage may spread to other records through valid transactions. Therefore, recovery techniques are required. The efficiency of the data recovery algorithm is substantial for e-healthcare systems. A patient cannot wait too long for his/her medical history to be recovered so that the correct medication be prescribed. Nevertheless, in order to have fast data recovery, an efficient damage assessment process should precede the recovery stage. The damage assessment must be performed as the intrusion detection system detects the malicious activity. The execution time of the recovery process is a crucial factor for measuring the performance because it is directly proportional to the denial of service time of any healthcare system. This paper presents a high performance damage assessment and recovery algorithm for e-healthcare systems. The algorithm provides fast damage assessment after an attack by a malicious transaction to keep the availability of the e-healthcare database. Reducing the execution time of recovery is the key target of our algorithm. The proposed algorithm outperforms the existing algorithm. It is about six times faster than the most recent proposed algorithm. In the worst case, the proposed algorithm takes 8.81 ms to discover the damaged part of the database; however, the fastest recent algorithm requires 50.91 ms. In the best case, the proposed algorithm requires 0.43 ms, which is 86 times faster than the fastest recent work. This is a significant reduction of execution time compared with other available approaches.

[*] Corresponding author.
E-mail addresses: rharaty@lau.edu.lb (R.A. Haraty), a.zekri@bau.edu.lb, ahmed.zekri@alexu.edu.eg (A.S. Zekri).

https://doi.org/10.1016/j.tele.2017.12.010
Received 17 October 2016; Received in revised form 13 November 2017; Accepted 11 December 2017

Saving the damage assessment time means shorter denial of service periods, which in turn guarantees the continuity of the patient centric healthcare system.

1. Introduction

The advances in health care systems are tailored towards patient centric healthcare systems. A patient centric healthcare system is an approach where patients' records and other health information are easily accessible via the Internet. The patient has the right to access his/her medical records at any time and they should be available. The availability and integrity of patients' information is a crucial issue when talking about online data for patients because at times, their medical history will save their lives. Availability of patient information saves time and money from re-conducting some of the medical experiments that were previously done. Hence, it is important that the healthcare system be always available. Consider, for example, the case where a patient had certain disease *d* and she is not allowed to take medicine *X*. If a malicious transaction updated this patient's data and deleted the record saying that she is not allowed to take medicine *X*, the nurse will read wrong information and probably give the patient wrong medicine that may be life-threatening. Thus, any updated data by malicious transactions should be recovered and restored to its correct values in the minimum possible time.

Healthcare systems are sharply growing and shifting towards the electronic and online arena (Menachemi and Collum, 2011). Paper-based healthcare systems are not efficient anymore and do not satisfy patient's needs. Providing patient's history online helps improving the diagnoses of medical cases for people. Doctors can refer to the patient medical history to give the best medication. Moreover, electronic healthcare systems can reduce the cost on patients because many experiments and treatments will not be required to be repeated. Nevertheless, computerizing these systems unveiled the problem of securing patient's records. Online healthcare systems are now exposed to cyber-attacks that may affect the availability of these systems for user. A malicious attacker's goal is, more often than not, the denial of service of any healthcare information system. There should always be a security plan for e-healthcare systems. One example of these plans is suggested in Cankava and Kywe (2015), which is an approach for encrypting the healthcare data to make it secure. However, the history of information security shows that the system is always vulnerable to malicious activity, even when the data is encrypted. Thus, the system is not always secure. At some point, it will be attacked. Hence, recovery plans should be available.

Any data security system proceeds in three steps: prevention, detection and recovery. Prevention is the first step where many techniques are used like antiviruses, firewalls, authentication, authorization and others. However, there is always a chance for a malicious behavior to penetrate a system. The second step is the intrusion detection system (IDS). The IDS specifies the set of malicious transactions. There is a lot of work in this domain (Lunt, 1993). When an IDS detects a malicious transaction, the third step should be performed, which is the damage assessment and recovery step. This step starts to wipe out the damage from the healthcare database and bring it back to its original state.

Upon recovery, the healthcare information system will be either completely or partially offline and users cannot access it. This leads to a denial of service problem, which is the main target of any intruder. For this reason, the damage assessment and recovery steps should be fast and accurate.

This paper presents a high performance database damage assessment and recovery approach that follows the data dependency paradigm. In any healthcare system, there is a lot of data inter-dependency because the data items read by a transaction are already written by other transaction and will be used to write new values. These new values will also be read and used by other transactions, and so on. An affected transaction may spread the damage to a large portion of the database. The size of the affected portion depends on how fast the IDS provides the recovery stage with the malicious transactions. All the affected transactions, whether they are affected in a direct way or indirect one, should be rolled back in the shortest possible time so that the database is restored to its consistent state. Recall that the consistent state of the database is the state that the database would have received if no malicious behavior occurred.

The proposed recovery approach is matrix-based. Contrary to other approaches, our algorithm needs only one matrix that holds all the dependent data items. The matrix stores integers in the cells. Each integer represents the data item ID. During the damage assessment stage, there is no need for reading the log file since the matrix contains the necessary information. The matrix rows represent the committed transactions. The columns are the data items used by the committed transactions. As the transaction reaches the commitment point, we add a row to the matrix. When a data item is used, a new column will be added. Because the matrix is an indexed structure, the algorithm will not need to traverse all the data. However, the index will help in pointing out the data directly in a single step. This saves execution time. Having a single matrix will also save memory compared to the algorithms that uses more than one data structure.

Although the algorithm can be applied to electronic systems other than e-health, not all systems care for the time issue. Some systems has a problem with the space of the data and others with the needed resources. E-healthcare systems are the systems that mostly need to consider the recovery time. For this reason, we choose to apply this algorithm on e-healthcare systems.

The remainder of the paper is structured as follows. Section 2 presents a survey of the related works. Section 3 gives a detailed description of the proposed algorithm. Section 4 presents the experimental results and discusses performance analysis of the proposed algorithm. And Section 5 presents the conclusion and gives directions for future work.