Gulara I. Muradova
Azerbaijan Technical University, Baku, Azerbaijan
gulara_m@hotmail.com

SECURITY OF PERSONAL MEDICAL DATA FOR THE REDIS CONCEPT

During processing personnel data, security is provided by personnel data protection system which neutralizes actual treats. In the article, techniques and tools of Redis are oriented to speedy data processing for online coming and rapidly changing personal medical data. Application of Redis technology eliminates uncontrolled access to confidential information.

Keywords: *E-health, protection of information, security, confidentiality, personnel medical data, data base, cache management.*

Introduction

In healthcare, informatization is needed at the stages of the medical diagnostic process for collecting information about a patient, diagnosing, deciding on the necessary actions, their implementation and organization of medical care for the population and health management. Informatization is a set of measures for the full and timely provision of participants with necessary information, processed and, if necessary, transformed. Informatization of health care is carried out through the creation and implementation of computerized systems. The use of information technology tools in medical practice allows not only to improve the quality and accessibility of services, but also to transform the model of medical care delivery. The increasing expectations of citizens to improve the quality of medical care are stimulated by the use of health care applications. In addition, the modern health care system is based on the concept of patient empowerment, joint services and continuity of services. The use of computer solutions is now perceived as one of the effective remedies [1]. Traditional methods cannot respond to the rapidly growing needs for patient confidentiality in an e-health environment [2].

Electronic Health

E-health is aimed at solving all the problems of public health protection. It is based on general electronic document circulation, including personal medical data, on-line access to patients' data, availability of its joint remote analysis by physicians, and physician-patient communication. Now, attention is more paid to the problem of the patient's attitude to his/her health. This implies an integral characteristic of the physical, psychological, emotional and social state of patient based on his/her personal perception. The right of a human being to life and health is an inalienable right of everyone. The state guarantees citizens protection of health irrespective of gender, race, nationality, language, social origin, official position, place of residence, religion, beliefs, membership in public associations, and other circumstances.

The modern concept of attitude towards one's health is based on the following three components:

- multidimensionality - application of techniques related and unrelated to disease, which allows differentiating the impact of disease and treatment on the patient's condition;
- time variability - constant monitoring of the patient's condition helps to correct treatment depending on the changing state of patient over time;
- participation of patient in the assessment of his/her condition - indicator of the general condition made by the patient himself/herself. Along with the traditional medical conclusion, a more complete picture of disease is drawn up and a prognosis of its progression is provided [3, 4].

A large number of clinical research programs are aimed at choosing the optimal algorithm for disease treatments. At the same time, the quality of life is considered as an important integral criterion for the treatment's effectiveness. The patient's data obtained before the treatment is used

to predict the disease and its consequences helping the doctor to choose the most effective treatment program. Research on the quality of life of patient plays an important role in controlling the quality of medical care provided to the population. These studies are an additional tool for assessing the effectiveness of medical care based on the judgments of its main consumer, namely the patient [5, 6]. In this regard, the widespread use of technologies for remote data analysis in the operational mode assumes the presence of e-health, which is often called "distributed health care", emphasizing the absence of fundamental importance of the location of patient and doctor.

The main areas of health care that e-health aims at are:
- assessment of patient's condition and dynamics on the basis of operative access to all information about the patient:
- monitoring of patient's condition from home;
- remote consultations and discussions;
- remote access of patient to the resources of treatment-prevention institutions and services provided at various administrative levels;
- Data analysis based on prompt access to medical and statistical data on nosological, gender and age and social structures;
- Organization of forums for health professionals on a wide range of issues, including joint analysis and discussion of health data [7].

E-health requires concerted efforts at the national level on a number of issues:
- regulatory and legal support;
- information and communication infrastructure;
- unique patient identification system;
- development and application of international standards for the structure of medical documents and protocols for their sharing;
- unified principles of data storage [8].

Relations between patients and hospitals have traditionally been random, i.e., people used to visit healthcare facilities only when they were ill, and stopped visiting them as soon as they got recovered. Today, the emphasis is replaced by the preventive measures in order to prevent illness and keep good health at old age [9]. This is so-called "Medicine 4 P": Predictive, Personalized, Preemptive and Participatory [10]. Medical services provide a number of services via the Internet and other modern communication channels, such as interactive digital television, call centers and public booths. In this connection, special means are being distributed, in particular, electronic prescribing, electronic treatment and access to medical information through electronic medical cards. The provision of services online allows patients to interact with medical services at any time, through any communication channel of their choice. In the developing electronic medicine, the widespread introduction of computer technologies for the processing of personal medical data and cross-border data sharing, a comprehensive innovative approach is required to develop legal, organizational and technological guarantees for the protection of health data and medical secrets from unauthorized access.

Data Privacy Policy

The question of ensuring the confidentiality of personal health data is of great importance in all countries that have introduced e-health. Ensuring the protection of human and civil rights and freedoms while processing his/her personal data, including the protection of privacy rights, personal and family secrets, is also an important issue. Personal data is any information related to an individual, including last name, first name, patronymic, date and place of birth, address, marital, social and property status, education, profession, income, lifestyle and other information. To monitor all details and solve complex health problems, while giving users the opportunity to choose which data they are willing to provide and which ones they do not, is complicated. In addition, such data may not always be made anonymous. It is difficult to work with personal data and find the right and 100% reliable information, which is constantly updated. Analysis of personal data enables one to identify the impact of various

causes on incidence and identify risk factors. The presence of a risk factor indicates an increased probability of any adverse event, whereas its magnitude shows the level of this probability. The emergence of various types of mobile applications helps the patient to perform diagnostics and facilitates the process of self-treatment or treatment with the help of a remote consultant.

The frequency of data acquiring, reducing the period of time from the query to data acquiring give the best results, namely, quality, reliability, simplicity, visibility, and completeness of information. Monitoring the status of patients at home reduces the the costs and the number of visits of the medical personnel reducing. Remote assessment of the dynamics of patient's condition at home assumes a wide range of tasks to be solved - from monitoring of physiological parameters to psychotherapeutic assistance to different categories of patients (bedridden patients, elderly people, disabled, pregnant women, etc.).

Data sensed from smart devices allow real-time monitoring of chronic diseases, optimization of the dose of drugs, and improvement of the treatment results. With the help of special equipment that transmits the electrocardiogram data to the doctor, the patient suffering a stroke or brain trauma can receive round-the-clock consultations and home testing sessions. Responding to the changes is more important than following a plan. This enables evaluating the patient at a moment and comparatively assessing the impact of various medications. These devices can also allow tracking the changes in the state of patient occurred within a couple of minutes. They are used to assess the effectiveness of treatment regimens for a particular disease. For example, in case of bronchial asthma and for patients with acute myocardial infarction, etc. The dose of drugs can be corrected and then compared. In the course of treatment not the severity of the course of the disease is determined, but how the patient tolerates it. The operator, who collects personal data using information and telecommunication networks, publishes documents in the relevant information and telecommunications network. These documents define security policy regarding the processing of personal data, and information about the current requirements for the protection of personal data. For example, local hospital stores health records. But if one has an accident in another country, the first aid doctor will require important information about chronic illnesses or allergies to medicines. Easy and fast search of such data with automatic prompts will help to render the qualified aid. Data confidentiality means that the data belonging to an individual will never be disclosed to anyone [12]. Potential threats to confidentiality and security of personal health data are associated with the danger of misuse of the latter. Another serious threat to the safety of personal health data emerged after the widespread availability of genetic information that unambiguously indicates a specific patient. Since this information is almost impossible to anonymize, and the de-identified genomic data is easy to recover, the confidentiality issues should be resolved at the legislative level. Will people allow companies to process their personal data and all the information that comes from customers? Information is provided for free, and then analyzed, processed by on computer; a new product is produced, which is then sold to people again. The question is whether it is correct to use the "property" of the client in this way? [13-15]. Patients do not realize that their data and the data about their actions can be reused for other purposes. Communication avoids social control, which negatively influences on a person. The American Association for Health Information Management estimates the most common causes of large-scale leakage of health data and respective pie chart is given in Fig.1. These include theft (55%), unauthorized access (20%), information loss (11%), hacking (6%), misuse (5%) and other unknown reasons (3%).
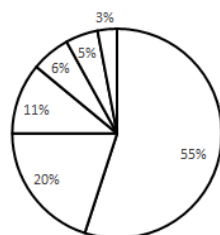

Figure 1. Personal data leaks [16]

Data security and privacy have become a serious problem. Stored and used confidential raw data is the main obstacle to the introduction of various techniques, such as collecting, organizing, accumulating and storing biometric data. Analysis of modern scientific literature has made it possible to identify the following measures, such as password protection, data encryption, access rights delineation, including secure virtual networks. In many cases, these tools are not enough, and then a variety of methods of protection are used. These methods include design of database management systems with built-in protection mechanisms and the integration of the latter with special software products to protect information [17, 18]. These difficulties source a number of the following problems:

1. It is difficult for database administrators to correctly define access rights, which generates errors.
2. It is more difficult for another database administrator to subsequently maintain access restrictions.

There is an increased possibility of unforeseen side effects when complex rights are interpreted by the system.

Additional measures are taken to calculate and eliminate inefficiencies at runtime, when it is necessary to check the privileges for this query [19, 20].

Redis cache techniques and tools

Caching today is an integral part of any web project. Web applications can not respond instantly to the user, as it takes time to communicate with the applications' servers, and some calculations must be made before responding. This includes the time required to transfer data from server to client and to find the right data on the disk, and network delays, and processing of query queues, and mechanisms for regulating the networks' bandwidth, etc. If we consider that all this can happen on the set of computers located between client and server, then we can say that all these delays can seriously increase the time required for the receipt of the query by the server and for the receipt of the response by the client.

A properly configured caching system can significantly improve the overall performance of the server. Caches reduce the delays that inevitably occur when data is transferred over the network, help to save network traffic and. As a result, the caches reduce the time required for the browser to display the web page requested from the server. Queries to databases can be slow and require serious system resources to generate a response. If the requests are repeated, their caching through the database will help reduce the response time. Caching is beneficial when several computers are working with a database and performing the same queries. Most database servers are configured by default with the optimal caching parameters.

However, there are many settings that can be modified to make the database sub-system better suited to the particular application. Web server responses are cached in RAM. The cache application can be stored either locally in memory, or on a special caching server. Redis is a sort of caching used to optimize the work with resource-intensive functions.

Redis - remote dictionary server - storage of objects in memory - a fairly simple and fast way to cache data [21]. Advantage of caching data in web applications using a separate Redis caching service is that the data comes from different sources. Once the generated code is stored in RAM, and when accessing, instead of generating everything anew each time, it issues a copy (cache) stored in RAM. The main advantage is that it is a simple cache with a simple structure, and the query takes no more than 10 ms.

The software designed to cache data in Redis memory provides a service for storing the values associated with keys. The cache access is obtained through a simple network protocol. The client can be a program written in a random programming language. This is a network journal of key-value type data warehouse with open source code, which is oriented at high-speed data processing [22]. The key is what we label the pieces of information with. Value is the data associated with the key.

Redis saves database snapshots to disk, depending on how many keys have been changed. The process is configured so that if X is the number of changed keys, then the database must be saved every Y seconds. Redis saves the database at intervals of 60 seconds by default, if 1000 or more keys have been changed. This interval rises up to 15 minutes, if at least 9 keys have been changed. In addition, Redis can be enabled in append mode. Each time the key changes, an entry in the file opened in append mode is recorded to the disk (new entries are appended to the end of the file) [23]. Redis-service for caching data in RAM achieves high performance. In general, caching is performed as follows: if the query results in retrieving some sample data, then the fast Redis server is accessed (*get*-query) and the corresponding key is found. Otherwise, the database is accessed. Obtained result is immediately written to Redis as a cache (*set*-query). In this case, the key is given the maximum life cycle (expiry date). The operations include: get the value of the specified key (*get*), set the value of the key (*set*) and delete the key (*del*).

The concept of Redis for the implementation of certain functions is reviewed below. Redis cache is a favorable for applications that require fast data view, and helps to correct patient's information according to minutely changing device records:

1. Personal information about the patient's condition is displayed as an access request, then it is automatically redirected to Redis.
2. After processing in Redis the result of the request is obtained - recommendations for the patient. If the doctor needs additional information for diagnosis, then another request is made in Redis. In this case, the unification of these sets is accepted and a user receives the required data.
3. All the necessary information is cached for certain and predetermined short period of time (in our code this is 1 minute).
4. After solving the task, the personal information disappears and the updated data appears in 1 minute.

The advantages of using the Redis concept in medical applications are that the necessary information is cached much faster than that with MySQL.

The code is provided below:

```
// Save patient info for (TTL)1 minute
   string patientAsString = JsonConvert.SerializeObject(firstPatient);
   cache.StringSet("patient-id-" + firstPatient.Id, patientAsString,
       new TimeSpan(0 /* hours */, 1 /* minutes */, 0 /* seconds */));
   // Read patient info
   Patient patient1 = JsonConvert.DeserializeObject<Patient>(patient1AsString).
```

An entry with the specified TTL (Time to live) can be deleted after a specified time. All TTL records are guaranteed within 60 seconds and outdated data - no longer than a minute.

It would be better to have simpler solution that is easier to be reliably configured, maintained and enabled. This article focuses on limiting the data access time. In all these cases, the best way of data protection is "to implement policies and procedures" regarding the final elimination of electronic patient data. Therefore, the best methods are, in this article, the provision of exact deletion and the inability of re-restoration, including from backup copies. This is done through the controlled Redis cache service, which allows binding the term to its value. Data access technologies are constantly being improved and this is proved by Redis concept. Here, a specific class of problems is solved. At the same time, these problems are sufficiently universal. Traditional disk databases require cyclic access to the disk for most operations. Data wharehouses in memory, such as Redis, avoid this restriction, and therefore can perform more operations per unit of time and provide better response time. Due to its speed and convenience, Redis web technology is often used for gaming and advertising applications, financial services, and applications for healthcare industry.

Redis is distinguished by its exceptional speed, which makes it an optimal choice for a certain class of tasks:

1. The diagnosis based on the online received data with the participation of specialists. More and more patients acquire wearable electronics, and mobile devices constantly develop and increase functions (glucose level, heart rate, pressure, activity, diagnostic tests, etc.). There are also gadgets for early diagnosis of diseases and daily health monitoring. Diabetes patients can use a variety of devices connected to a network that would enable patients periodically send data such as blood sugar levels. Thus, the information received in real time is monitored in accordance with the patient's current condition, decisions are made, and then the intermediate data is cleared.

2. The medical company has a website, which enables customers to interact online through a computer. Patients can safely enter their details (for example, addresses) on the website. Customers benefit from the improved interactive capabilities of the site, for example, they can safely communicate their administrative details via the Internet. As a result, people are given the opportunity to quickly and easily find the necessary information about the instructions of doctors, as well as to be sure that confidential information will be deleted.

3. Processing of phone calls to the first aid service. Once the time is expired, personal data is deleted.

4. The key aspects in health data sharing in virtual communities are the safety and reliability of health information. The communication ways are controlled and personal message is temporary.

5. The use of screening - with a mass survey of the population and identification of persons with diseases for which personal medicines are prepared. In this case, the results of patient examinations are withdrawn.

6. Healthy people can embed to USB ports for diagnostics. Analyzes are done at home on their own, the clinical representation is stored in cloud, and communication with the doctor is realized remotely - via the Internet. The data measured at home can be removed in a timely manner.

In large and heavily loaded projects, Redis caching tools are advisable to reduce the load on databases. The use of a controlled Redis cache ensures the timely removal of confidential information, while hardware, software and other solutions do not always guarantee the reliability and security of personal data in computer networks.

Conclusion

The analysis of personal data in dynamics allows revealing the influence of various causes on morbidity and mortality of the population, and identifying the risk factors. An obligatory condition for the provision and assignment of personal data processing to another person is the obligation of the parties to ensure confidentiality and safety of personal data during their processing. The article described the method of protection against illegal actions in relation to personal data, allowing timely destruction of the latter. A code was provided that provided a response time at fractional seconds and allowed real-time applications to execute millions of requests per second. Summarizing the above, it could be concluded that the personal data protection system based on the Redis-cache allowed speeding up the execution of queries and improving the scaling capabilities, reducing the load on the main database. Companies like Redis Labs, Amazon, Microsoft Azure and others offer many useful tools and services to Redis. Redis Web technologies can be successfully used in mobile and Internet applications, as well as in e-health applications.

References

1. Duplaga M. The Impact of Information Technology on Quality of Healthcare Services Computational Science - ICCS 2004, vol. 3039. Springer, Berlin, Heidelberg, pp.1118–1125.
2. Muradova G.I. Large data in the health care system // Problems of Information Technologies,

Baku, 2016, No 2, pp.98-105.

3. Fekri O., Macarayan E., Klazinga N. Health system performance assessment in the WHO European Region: which domains and indicators have been used by Member States for its measurement? Copenhagen: WHO Regional Office for Europe; 2018 (Health Evidence Network synthesis report 55), pp.4-6.

4. Global strategy and plan of action on public health, innovation and intellectual property ISBN: 978 92 4 150290 0 World Health Organization 2011 www.who.int

5. Wilson I., Cleary P. Linking Clinical Variables With Health-Related Quality of LifeA Conceptual Model of Patient Outcomes 1995,vol.27,N1, pp.59-65.

6. Spil T., LeRouge C.,Trimmer K.,Wiggins C. Back to the future of IT adoption and evaluation in healthcare International Journal of Healthcare Technology and Management ,2011,vol.12, Issue 1, pp.85–109.

7. Usanov V. Federal Law "On Personal Data", Publisher: Eksmo-Press, 2018, pp.12–20.

8. Keeping Promises, Measuring Results. Commission on Information and Accountability for Women's and Children's Health. Geneva. World Health Organization. 2011, p.12.

9. Sibona C., Walczak S., Brickey J., Parthasarathy M.Patient perceptions of electronic medical records: physician satisfaction, portability, security and quality of care, International Journal of Healthcare Technology and Management 2011 12:1, pp.62–84.

10. Bradley W.,Golding S. Globalization of P4 Medicine: Predictive, Personalized, Preemptive, and ParticipatoryRadiology, 2011,vol. 287 No. 2, pp.571–582.

11. Mamedova M.G. Information security of personal health data in the electronic environment // Problems of Information Technologies, Baku, 2015, No2, pp.6-30.

12. Kuchin I.Yu. "Protecting the privacy of personal data by means of depersonalization." Bulletin of the Astrakhan State Technical University. Series: Management, Computer Science and Informatics, 2010, no. 2, pp. 158-162.

13. Predictive medicine and Big Data. http://apptractor.ru/info/articles/lektsiya-lorensa-dzheykobsa-prediktivnaya-meditsina-i- bolshie-dannyie.html

14. Magnusson R.S. The Changing Legal and Conceptual Shape of Health Care Privacy// Journal of Law, Medicine & Ethics, 2004, vol.32, pp.685–689.

15. Koufi, V., Malamateniou, F., & Vassilacopoulos, G. Towards Clinical and Operational Efficiency through Healthcare Process Analytics. International Journal of Big Data and Analytics in Healthcare (IJBDAH), 2016, 1(1), pp.1–17.

16. Gilmer E. Confidentiality and safety of patient data in cloud https://www.ibm.com/developerworks/ru/library/cl-hipaa/index.html

17. Stephen S. Yau, Ho G. An, and Arun Balaji Buduru. 2012. An Approach to Data Confidentiality Protection in Cloud Environments, International Journal of Web Services Research 2012, vol 9 Issue 3, pp.67–83.

18. Poltavtseva M.A., Khabarov A.R. "Security of databases: problems and prospects." Software products and systems, 2016, no. 3 (115), pp.36–41.

19. Omran E., Grandison T., Nelson D., Bokma A. A Comparative Analysis of Chain-Based Access Control and Role-Based Access Control in the Healthcare Domain, International Journal of Information Security and Privacy (IJISP), 2013, 7(3), pp.36–52.

20. Mayuri R. Gawande et al, Analysis of Data Confidentiality Techniques in Cloud Computing, International Journal of Computer Science and Mobile Computing, vol.3 Issue.3, March-2014, pp.169–175.

21. Carlson J., Redis in Action, ManningBooks, 2013, pp.89–110.

22. https://azure.microsoft.com/en-gb/services/cache/

23. Seguin K. The Little Redis Book,2012 http://openmymind.net/redis.pdf