Security of the Telemedicine System Information Infrastructure

Aksinya V. Sokolova [1], Tatiana I. Buldakova [1]

[1] *Bauman Moscow State Technical University, 5/1 2nd Baymanskay ul., Moscow, 105005, Russia*

Abstract

The requirements for the security of telemedicine systems are considered. The assessment of the health status of a person with dementia is performed based on medical data that is registered by sensors and transmitted to a cloud-based medical information system. Based on the data obtained, the attending physician forms recommendations. Because medical consultations are provided at a distance, there is a need to ensure the reliability of storing and transmitting the patient's medical data. The solutions and methods of protecting the transmitted data that help bringing the developed telemedicine system to the required security standards are determined. It is noted that the presented methods are necessary, but insufficient and additional methods of protecting the transmitted data are required.

Keywords

Telemedicine, network access, information infrastructure, data protection

1. Introduction

Improvements in the health sector contribute to the fact that people's lives become longer and healthier. The most popular direction of healthcare today is telemedicine. Within the framework of this direction, many telemedicine systems are being created that can improve the quality and speed of receiving medical care through remote interaction with a doctor.

Telemedicine is a developing type of information technology that does not have many years of experience. Therefore, some users may be suspicious of telemedicine systems. In addition, some people are concerned about the safety of information about their medical records, but they will not avoid using the health system because of these problems. However, for some users, especially doctors, this is the reason that they do not want to use virtual health at all. That is why the security of the telemedicine network is an important task.

Taking the described steps to strengthen security in telemedicine is a complex challenge encompassing clinical technology, digital technology and legal compliance [1]. Answering that challenge will require provider organizations to offer innovative new services, protect data, and develop new applications, business processes, and cloud strategies all at once. And of course, this entire undertaking is only one of the competing investment needs a provider must balance.

Using telemedicine technologies in the provision of medical care is carried out in compliance with the requirements established by the legislation of the Russian Federation in the field of personal data and compliance with medical secrecy. However, because the medical consultation is carried out in a remote format, there is a risk of non-compliance with medical secrecy – the patient's medical data may end up with third parties. To avoid this, the telemedicine system needs to ensure data protection when transferring them between the patient and the doctor and storing them in the system [2].

This article will identify the requirements for telemedicine systems security and their implementation on the example of a telemedicine system being developed that can assess people's with dementia conditions.

BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies, April 6-7, 2021, Moscow, Russia
EMAIL: aksinya.sokolova@yandex.ru (A. 1); buldakova@bmstu.ru (A. 2)
ORCID: 0000-0002-4643-0060 (A. 1); ORCID 0000-0002-4607-0544 (A. 2)

2. Telemedicine system architecture

The developed telemedicine system is presented as a client-server application. It will allow the patient to communicate with the doctor, providing the system with different research results which are necessary for the diagnosis of dementia. It is assumed that the system will process the research results received from the patient and provide this information to the attending physician [3]. In addition to research, the patient can take neuropsychological tests, which are an effective tool for detecting dementia. In turn, the doctor, using the results of the study and tests, will be able to more accurately diagnose dementia if it is present and form individual recommendations for the treatment and support of the patient's condition, based on the received anamnesis. The system makes it easier and faster to process medical data in order to identify dementia as early as possible and already start planning therapy, which will be more effective in the early stages.

The developed system is planned to be used as an assistant to facilitate and accelerate the processing of patient tests by a doctor remotely. Its structure is shown in Figure 1.

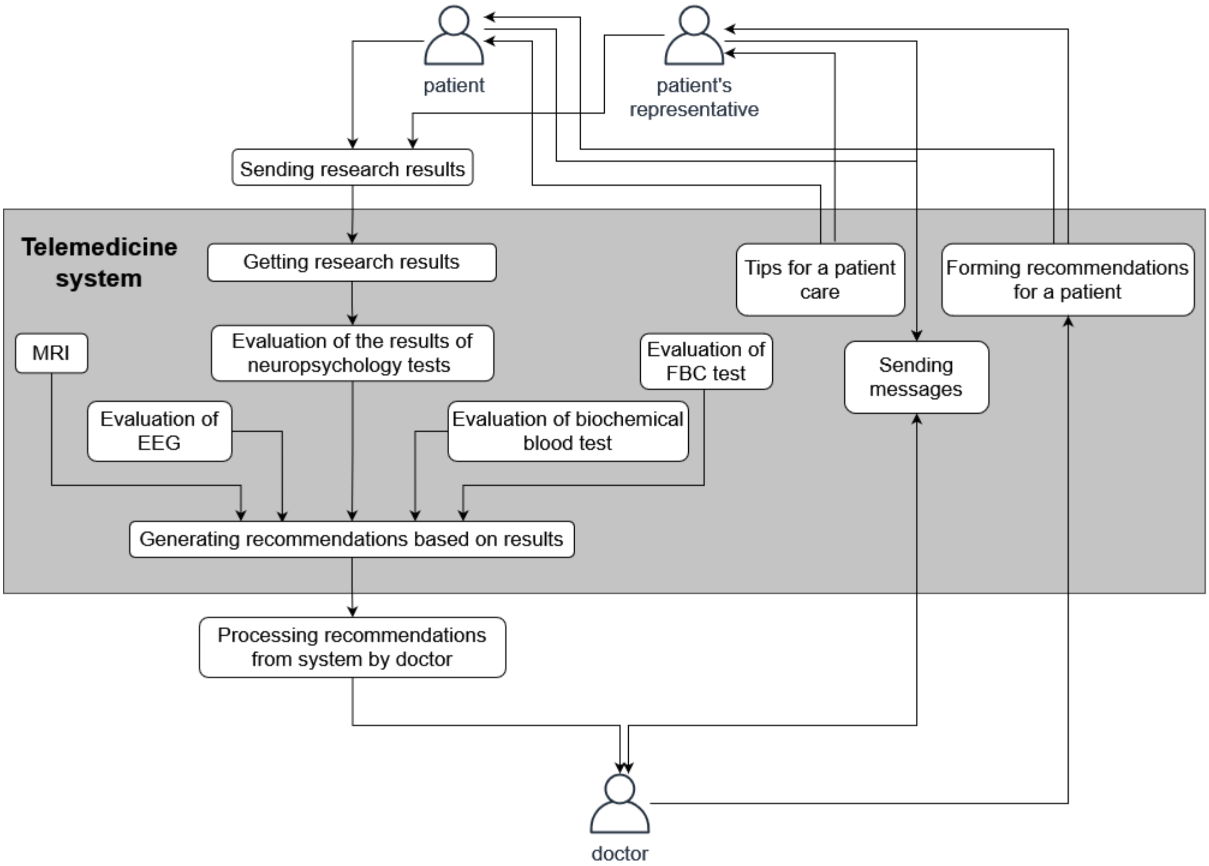
patient
patient's representative
Sending research results
Telemedicine system
Getting research results
Tips for a patient care
Forming recommendations for a patient
MRI
Evaluation of the results of neuropsychology tests
Evaluation of FBC test
Sending messages
Evaluation of EEG
Evaluation of biochemical blood test
Generating recommendations based on results
Processing recommendations from system by doctor
doctor

Figure 1: The structure of the telemedicine monitoring system for patients with dementia

3. Telemedicine system security law

To ensure that the telemedicine system meets all the requirements of the Ministry of Health, it is necessary to carry out measures to ensure the security of information systems [4]. The requirements for information security are supplemented by the need to comply with Federal Law 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation".

Based on the regulatory documents, the main security measures that should be implemented in the telemedicine system were identified:

An example of a bulleted list is as follows.

- prevention of unauthorized access to information, its modification, blocking, copying, provision and distribution (exclusion of access to unauthorized users);
- the possibility of access to personal medical information within the medical institution itself should be limited and separated (management and differentiation of access to the system should be carried out on the basis of user roles);
- the possibility of restoring the information infrastructure by creating and storing backups (telemedicine systems should function in specialized internal networks, using a backup system in case some of the data is lost);
- transfer of information to medical institutions or organizations only in encrypted form.

Below are the solutions, the implementation of which will ensure that the system complies with the listed safety standards.

4. Measures to ensure the security of the system

Since telemedicine systems deal with personal medical data of patients, it is necessary to apply measures to ensure their protection in order to comply with medical secrecy.

The primary task of data security is the need to protect the personal account of the telemedicine system. In addition, patients should be sure that only their attending physicians have access to their medical data.

There are several ways to organize such protection. A role-based access control model is configured for the system, which distributes the existing functionality according to the roles of the system users. And the use of Multifactor authentication allows you to minimize the risk of authorization of persons who do not have permission to access the system.

The second task is to control system vulnerabilities with a resource that ensures the operability of the service itself. This will prevent possible threats and speed up the time to eliminate the vulnerability that has arisen. Also, do not forget about data protection during their transfer, in such a task, depersonalization of data will be a good solution. Even if a hacker can get hold of the data, he will not have the opportunity to understand who this data belongs to [5-7].

4.1. Role-based access control

Role-based access control (RBAC) refers to the idea of assigning permissions to users based on their role within a clinic. It offers a simple, manageable approach to access management that is less prone to error than assigning permissions to users individually. Also, RBAC helps to comply more effectively with regulatory and statutory requirements for confidentiality and privacy [8].

The main task of a telemedicine system data transfer security is to ensure the protection of the personal account of the system users. It is assumed that only the patient, the patient's representative, the consultant doctor, the staff of the medical institution, as well as the system administrator can log in [9-10]. In this regard, five roles were implemented based on the functional model of the system, which have the following properties (Table 1).

Table 1
The role model of the system

role	Adding information	Editing information	Viewing information	Creating medical recommendations for a patient
patient	+	+	+	-
patient's representative	+	-	+	-
doctor	+	-	+	+
medical staff	+	-	+	-
administrator	+	+	+	+

Working with the system's functionality falls on a web application, after logging in to which the user opens all the functionality provided for his role. This role model allows audit of user privileges and correct identified issues easily, quickly add and change roles, and realize primary functions [11].

4.2. Identification of the system user

Identification is the starting point for ensuring access security, especially for telemedicine systems. The virtual system being developed requires proof of identity. With so much sensitive medical data stored within a telemedicine infrastructure, it is critical to be able to tell users apart with the same degree of accuracy as it is possible with physical identities.

When a telemedicine system is deployed, the primary goal is to correctly and with the highest confidence level identify each user wishing to connect to the system. Therefore, users are given unique identifiers and are known by these personal credentials: their username and password.

Nowadays, the stealing of user credentials is all too common. Simple credentials on their own are not sufficient to keep a network secure, as it leaves a system vulnerable to dishonest users laying claim to somebody else's identity. Accurate, reliable identification of users is key to enforcing security policies and protecting data, and this is why every system user needs to authenticate [12, 13].

4.2.1. Multifactor authentication

When delivering virtual health, a health care professional must be confident the people on the other end of the line are really who they say they are. Multifactor authentication (MFA) is the way to confirm patient identity over digital channels. MFA can be expanded with biometrics (touch or facial recognition in a mobile application), short message service texts, or device fingerprinting. For patients, an additional benefit of MFA is that it can remove the need for a password as part of using a telemedicine system [14].

MFA works by requiring additional verification information (factors). One of the most common MFA factors that users encounter is receiving a is a one-time password (OTP) via SMS. But SMS is not a safe way to transfer personal data. Intruders can intercept SMS messages using vulnerabilities in the SIM card itself or in the phone. In that case, it is better to generate OTP using special physical OTP tokens. They create a six-digit code periodically, every 30 seconds. The code is generated based upon a seed value that is assigned to the user when they first register and some other factor which could simply be a counter that is incremented or a time value [15].

The developed telemedicine system is based on the following algorithm. A user is entering username and password, and then he must enter a twelve-character code that consists of two parts – a stable code and a code generated by OTP token (Figure 2). If the code matches, the user can start work with the system.

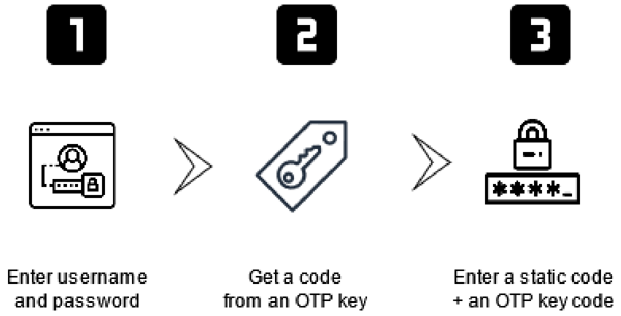
1
2
3
****_
Enter username and password
Get a code from an OTP key
Enter a static code + an OTP key code

Figure 2: The authorization using a multi-factorial authentication

4.2.2. Electronic digital signature

Since medical services in telemedicine are provided at a distance, there is a need to switch to electronic document management. The patient or his legal representative will be able, upon request, including in electronic form, to receive medical documents reflecting the state of his health, including extracts from them, and copies of medical records, in the form of electronic documents signed with an enhanced qualified electronic signature of the doctor [16].

An electronic digital signature (EDS), a cryptographic software that provides a high degree of data protection, allows you to identify the system user who signed the document.

As an algorithm for an electronic signature, a public-key encryption method is used, in which a pair of keys – public and private-is selected in a particular way for the user (Figure 3). At the same time, the key selection algorithms ensure that only those documents that were encrypted with the corresponding private key can be decrypted with a public key. Thus, if the public key of the EDS owner is known and the document received from him was decrypted, then it is worth asserting that the user is identified [17].

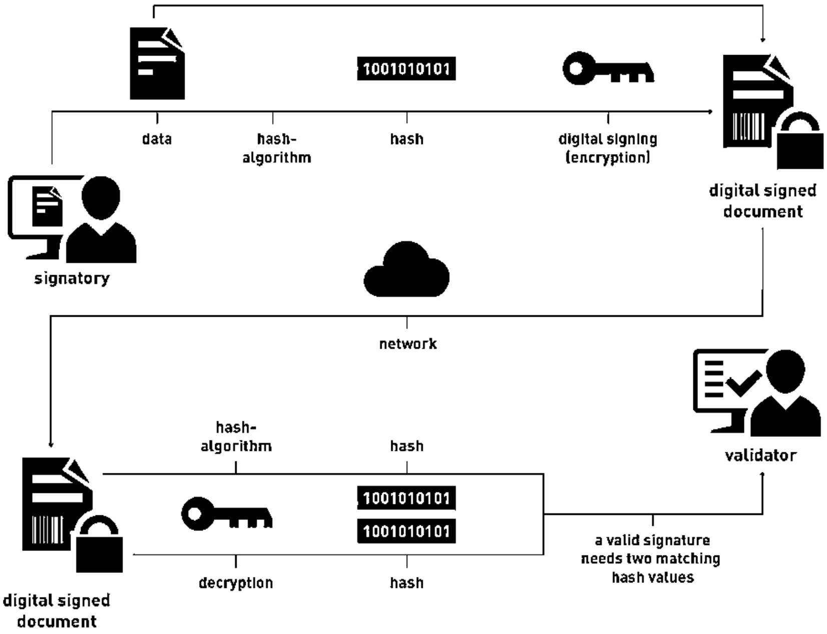

Figure 3: An algorithm of an electronic digital signature

EDS provides a high degree of data protection and allows you to exclude the possibility of unauthorized access to the system. Therefore, each user of the system must have a certificate and an electronic signature key in order to be able to use telemedicine services.

4.3. Intrusion Detection System

Wireless Sensor Networks (WSNs) can be defined as self-configured and infrastructure-less wireless networks to monitor physical conditions, such as temperature, sound, vibration, pressure or motion and to cooperatively pass their data through the network to the main location or sink where the data can be observed and analyzed [18]. WSNs are subject to several types of security attacks at various levels due to an open wireless channel, a decentralized architecture, and deployment in physically unprotected zones.

The developed telemedicine system of assessing the condition of people with dementia contains several parts. The part of the system, which helps to collect medical data from body sensors, is a kind of WSNs - Wireless Body Area Network (WBAN). It is a network focused on the human body, which is formed by connecting body sensors. The network is able to continuously monitor various physiological parameters of the human body (pulse, body temperature, blood pressure, electroencephalogram (EEG) and electrocardiogram (ECG), as well as the state of body movement [19, 20]. Data from the network sensors is transmitted to the controller (Figure 4). It is considered the central command post of a wireless body network. After receiving the data, he pre-processes and sends it to a remote server via a network gateway.

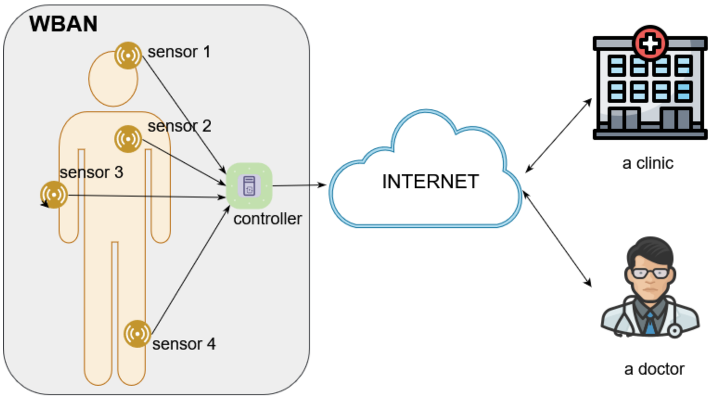

Figure 4: The scheme of Wireless Body Area Network in the telemedicine monitoring system for patients with dementia

Today, a wide range of penetration detection products are available, addressing a wide range of security purposes. One of them is the Intrusion Detection System (IDS), the main function of which is to monitor network behavior and user actions at different network levels.

An Intrusion Detection System (IDS) is software, based on an application designed to monitor computer or network activity in order to detect any unauthorized actions of intruders and protect information systems in the WSNs. Monitoring network behavior and user actions at different levels is the primary function of IDS [21].

Intrusion detection systems are divided into two main types: network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). In a Figure 5 you can see the difference between this types of intrusion detection systems.

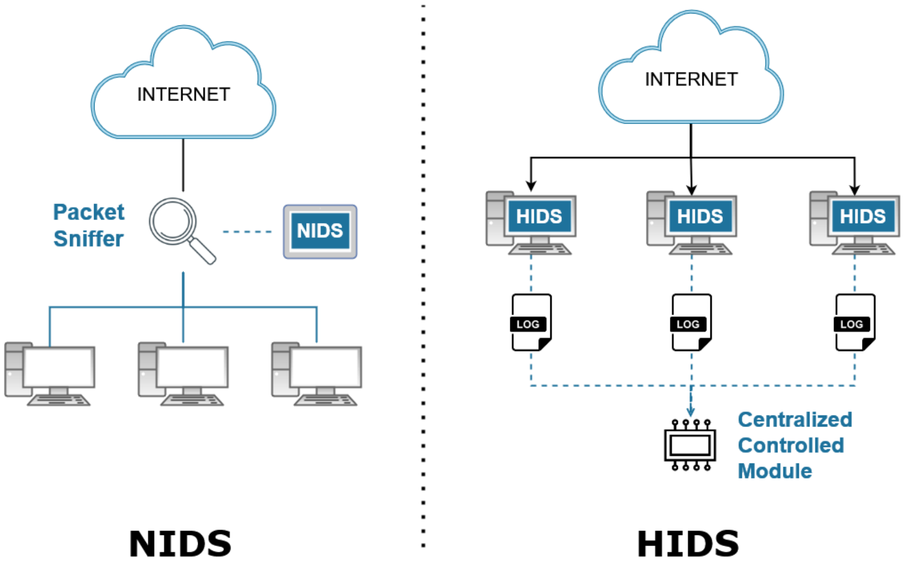

Figure 5: The difference between NIDS and HIDS usage

The NIDS (Network Intrusion Detection System) technology makes it possible to install the system in strategically important places of the network and analyze the incoming/outgoing traffic of all network devices. NIDS analyze traffic at a deep level, "looking" into each packet from the channel layer to the application layer. NIDS detects any malicious network activity using devices on the network card. The devices used are passive network sensors that are specially designed to monitor suspicious activity. It checks the moving traffic on the subnet and compares the traffic transmitted over the subnets with the library of identified attacks. If an attack is detected or if any suspicious activity is detected, a warning is sent to the administrator.

NIDS differs from a firewall in that the firewall captures only attacks coming from outside the network, while NIDS can also detect an internal threat.

Network intrusion detection systems are a universal solution because they allow you to control the entire network and not spend money on additional solutions. But this solution has a significant drawback: NIDS consumes many resources to track all network traffic. CPU and RAM. This leads to noticeable delays in data exchange and a decrease in network speed. And you also need to be prepared for the fact that with large amounts of information, NIDS will be forced to skip some packets, which makes the network vulnerable.

HIDS (Host Intrusion Detection System) acts on the basis of information collected from individual hosts, devices or servers, and not from the entire network, and detects and monitors any visual activity and notifies the administrator. It is a software-based software application and provides deep visibility of a critical security system. HIDS also analyze all incoming and outgoing packets, but only for one device.

The HIDS system works on the principle of creating snapshots of files: it takes a snapshot of the current version and compares it with the previous one, thereby identifying possible threats. It is better to install HIDS on critical machines in the network that rarely change the configuration.

4.3.1. Deploying IDS

After the NIDS are placed and functioning, the use of HIDS can additionally be considered to increase the level of protection of the system. However, installing host intrusion detection systems on each host of the network may require significant time costs. Therefore, it is recommended that HIDS be installed on critical servers first of all. This can reduce the overall cost of deployment and will allow you to focus on responding to alarms concerning the most important hosts. After host-based IDS have started functioning normally, organizations with increased security requirements can discuss the possibility of installing host-based IDS on other hosts.

In the case of providing protection in a telemedicine system, the choice of the method of providing protection was made in favour of HIDS systems that have centralized management and reporting functions. Such features can significantly reduce the complexity of managing alarm messages from a large number of hosts.

It is also essential to set a schedule for checking IDS results since changing IDS settings during a malicious attack [22].

4.4. Depersonalization of personal data

Patients' health information plays a significant role in conducting medical research for improving healthcare quality. Abrupt diagnosis and identification of certain diseases besides preventing misdiagnosis leads to extensive societal and financial impact, obviously depicting the necessity for efficient circulation of patient information among experts.

However, disclosure of health information to researchers raises concerns about privacy violations. A large volume of personal data (PD) of various security classes is processed in modern automated systems. Provision of information security requires significant material costs. For cost minimization, the opportunity of personal data depersonalization in information systems is provided. Depersonalized data is data stored in information systems in electronic form, the ownership of which cannot be determined by a specific subject of personal data without additional information. Each data type changes according to the rules that can be used in the code. For example, if the full name is replaced with a random hash with special characters and numbers, then the first check of the correctness of the data will immediately give an error in real testing.

The following methods of depersonalization are among the most promising and convenient for practical use [23].

- introduction of identifiers – replacing part of the information with identifiers with the creation of a table of matching identifiers to the source data;
- changing the composition or semantics – changing the design or semantics of personal data by replacing the results of statistical processing, generalization or deletion of part of the information;
- decomposition – splitting a set of personal data into several parts, followed by separate storage of subsets;
- shuffling – rearrangement of individual records and groups of records in the personal data array.

It usually takes a long time to convert confidential personal data into the anonymous - confidential sequence. It also has low resistance to attacks and has limits the process of working with a large amount of personal data. At the same time, anonymous data are used for archival storage without a possibility of confirming whether they are true and their analytical purposes. The most exciting things are methods of depersonalization which allow dividing all data into two groups: confidential and anonymous, with the possibility of checking their data in an anonymous form. It reduces the costs of creating an information security system at the automation facility; that's why developing a method, an algorithm, and a software module of personal data's depersonalization is an urgent scientific and technical task.

4.4.1. Watermarking images

Confidentiality, integrity and authenticity are of prime concern during transmission of medical images through the public network and must be simultaneously satisfied. Confidentiality of the transmitted medical images is ensured so that only authorized users can access them. Integrity validates whether the digital medical image is intact or tampered with. Authenticity verifies whether the medical image is from the correct source and belongs to the claimed patient. In the present scenario, the two significant methodologies, i.e. cryptography and medical image watermarking, are used popularly to meet these requirements.

The use of watermarks allows to hide the user's personal information in the image belonging to him.

The main preference when working with medical images is given to ensuring the security of the patient's documents as opposed to actions on the part of illegal persons. Telemedicine systems, including the one being developed, work with different data types, and it is important not to forget to protect each type used [24].

Regarding image protection, there are two designed watermark schemes for applying to medical images: irreversible schemes and reversible schemes. Irreversible watermark schemes are not suitable for use in the field of telemedicine, since changes caused by the procedure for applying watermarks to images entail irreversible functions that include bit exchange or truncation. In contrast, Reversible watermarking schemes re-establish the watermarked images to their original pixel values, thus permitting for exact diagnosis of medical.

The information enclosed in the images is not equally disseminated across images. Certain parts of the images comprise more information compared to other ones. Several schemes are practiced for separating dissimilar objects/regions in images. From a diagnosis point of view, a medical image is alienated into two regions; Region of Interest and Region of Non-Interest. The more useful and valuable part of the medical image is the Region of Interest, which is used for the diagnosis and has to be taken care of. Therefore, it is correct to insert the watermark in the Region of Non-Interest [25].

5. Conclusion

In the course of the work, the requirements for the security of telemedicine systems were considered, various necessary security methods were analyzed.

In practice, it was determined that the measures to organize the security of the system provided access to the system only to authorized and verified users and also allowed for a secure document flow between the patient and the staff of the medical institution providing consultations. And using depersonalization of data, their protection will be ensured during transmission; if an attacker gets hold of the data, he will not have the opportunity to understand who they belong to.

The specified security requirements were met when designing the client-server architecture of the system under development, internal services and database structure, as well as their normalization, and actions were taken to manage vulnerabilities and maintain reports on all user actions in the system.

The work showed the organization of security measures for a system capable of assessing the condition of people with dementia, but these measures will be relevant for all telemedicine systems [26].

6. References

[1] S. Suyatinov. Bernstein's Theory of Levels and Its Application for Assessing the Human Operator State. In: Dolinina O. at al. (Eds.) Recent Research in Control Engineering and Decision Making. ICIT-2019. Studies in Systems, Decision and Control. Vol. 199, Springer, Cham, 2019, pp. 298-312. doi:10.1007/978-3-030-12072-6_25

[2] R. Maximov, S. Sokolovsky, A. Telenga. Model of client-server information system functioning in the conditions of network reconnaissance. CEUR Workshop Proceedings. Vol-2603, 2019, pp. 44-51. URL: http://ceur-ws.org/Vol-2603/short1.pdf.

[3] Pijush Kanti Dutta Pramanik, Gaurav Pareek, Anand Nayyar. Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards.Telemedicine Technologies: big data, deep learning, robotics, mobile and remote applications for global healthcare, 2019, pp. 201-225.

[4] T. Buldakova and D. Krivosheeva. Data Protection During Remote Monitoring of Person's State. In: Dolinina O. at al. (Eds.) Recent Research in Control Engineering and Decision Making. ICIT-2019. Studies in Systems, Decision and Control. Vol. 199, Springer, Cham, 2019, pp. 3-14. https://doi.org/10.1007/978-3-030-12072-6_1.

[5] R. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems, 3nd. ed., Wiley, New York, NY, 2020.

[6] A. Appari and M.E. Johnson. Information Security and Privacy in Healthcare: Current State of Research. International Journal of Internet and Enterprise Management. Vol. 6(4), 2010, pp. 279-314. 2010.

[7] V. Varenitca, A. Markov, V. Savchenko. Recommended Practices for the Analysis of Web Application Vulnerabilities. CEUR Workshop Proceedings. Vol-2603, 2019, pp. 75-78. URL: http://ceur-ws.org/Vol-2603/short1.pdf.

[8] Auth0 Documentation. Role-Based Access Control. 2021. URL: https://auth0.com/docs/authorization/rbac

[9] T.I. Buldakova, A.V. Sokolova. Network Services for Interaction of the Telemedicine System Users. Proceedings of 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA). 2019, pp. 387-391. doi:0.1109/SUMMA48161.2019.8947552.

[10] T. Buldakova, D. Krivosheeva, S. Suyatinov. Hierarchical Model of the Network Interaction Representation in the Telemedicine System. XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP), Samara, Russia, 2019, pp. 379-383. doi:10.1109/CSCMP45713.2019.8976743.

[11] T.I. Buldakova, A.V. Lantsberg, S.I. Suyatinov. Multi-Agent Architecture for Medical Diagnostic Systems. Proceedings - 2019 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA), 2019, pp. 344-348. doi:10.1109/SUMMA48161.2019.8947489.

[12] Wallix Cybersecurity. Identify, Authenticate, Authorise: The Three Key Steps in Access Security, 2019. URL: https://www.wallix.com/blog/identify-authenticate-authorize-the-three-key-steps-in-access-security/

[13] H. Cai and K.K. Venkatasubramanian. Patient Identity Verification Based on Physiological Signal Fusion. 2017 IEEE/ACM International Conference on Connected Health:

Applications, Systems and Engineering Technologies (CHASE), Philadelphia, PA, 2017, pp. 90-95. doi:10.1109/CHASE.2017.65.

[14] Deloitte, Telemedicine privacy risks and security considerations, 2019. URL: https://www2.deloitte.com/us/en/pages/advisory/articles/telemedicine-privacy-risks-security-considerations.html

[15] Onelogin, What is Multi-Factor Authentication (MFA) and How Does it Work?, 2021. URL: https://www.onelogin.com/learn/what-is-mfa

[16] Asma Jebrane, N. Meddah, A. Toumanari, M. Bousseta New Real Time Cloud Telemedicine Using Digital Signature Algorithm on Elliptic Curves. International Conference on Advanced Information Technology, Services and Systems (AIT2S) 2017: Advanced Information Technology, Services and Systems, 2017, pp 324-332. doi:10.1007/978-3-319-69137-4_29

[17] A I Dzhangarov, M A Suleymanova. Electronic digital signature. IOP Conference Series Materials Science and Engineering, Vol. 862, 2020. doi:10.1088/1757-899X/862/5/052054

[18] M.A. Matin, M.M. Islam. Overview of Wireless Sensor Network. Wireless Sensor Networks - Technology and Protocols, 2012. doi:10.5772/49376

[19] S.-J. Lee, G.-Y. Cho, and T.-R. Lee. N-WRETS: Near-Lossless Wireless Real-time Efficient Electroencephalogram Transmission Solution to Support Sleep Disorder Monitoring Platforms. Telemedicine and e-Health. Vol. 25, no. 2, 2019, pp. 116–125. 2019. doi:10.1089/tmj.2017.0279.

[20] T.I. Buldakova, A.V. Sokolova. Structuring Information about the State of the Cyber-Physical System Operator. International Conference on Information Technologies in Engineering Education (Inforino), Moscow, Russia, 2020, pp. 1-5. doi:10.1109/Inforino48376.2020.9111654.

[21] J. Veeramreddy, K. M. Prasad. Anomaly-Based Intrusion Detection System. Computer and Network Security. IntechOpen 2020, pp. 40-55. doi:10.5772/intechopen.82287

[22] E. M. Rajaallah, S. A. Chamkar, S. Ain El Hayat. Intrusion Detection Systems: To an Optimal Hybrid Intrusion Detection System. International Conference on Advanced Information Technology, Services and Systems (AIT2S) 2018: Smart Data and Computational Intelligence, 2018, pp 284-296. doi:10.1007/978-3-030-11914-0_30

[23] D. V. Primenko, A. G. Spevakov, S. V. Spevakova. Depersonalization of Personal Data in Information Systems. Proceedings of the International Russian Automation Conference, RusAutoCon. 2019, pp. 763-770. doi:10.1007/978-3-030-39225-3_83

[24] Priyanka & Sushila Maheshkar. Region-based hybrid medical image watermarking for secure telemedicine applications. Multimedia Tools and Applications, Vol. 76, 2017, pp. 3617–3647. doi:10.1007/s11042-016-3913-1

[25] K. Swaraja. Medical image region based watermarking for secured telemedicine. Multimedia Tools and Applications. Vol. 77(2), 2018, pp. 28249–28280. doi:10.1007/s11042-018-6020-7

[26] Buldakova T., Lantsberg A., Smolyaninova K. Security Threats in Systems of the Remote Monitoring. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017, No 4(22), pp. 40-46. DOI: 10.21681/2311-3456-2017-4-40-46.