Protection of Data Transmission in Remote Monitoring Tools by Anonymization

Anatoliy Melnyk[a,b,c], Jean-Yves Le Boudec[d], Yurii Morozov[a,b], Bohdan Havano[a,b] and Petro Hupalo[a]

[a] *Intron ltd, Lviv, Ukraine*
[b] *Department of Computer Engineering, Lviv Polytechnic National University, Lviv, Ukraine*
[c] *The John Paul II Catholic University of Lublin, Lublin, Poland*
[d] *Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland*

Abstract

Data anonymization is a method of removing or encrypting personal data in a data set. At the same time, the existing data structure is maintained for further data analysis. The purpose of anonymization is to ensure the confidentiality of the subject's information. This paper examines the problems of user authorization and the protection of data transmission in remote monitoring tools. Technologies for protecting data transmission in remote monitoring tools are selected. In the presented remote monitoring tools, data pseudonymization is used to anonymize data. Pseudonymization of data consists in replacing the user ID with an encrypted JWT token. Because the JWT token is encrypted using TLS, which uses revocable symmetric keys, there is no way to detect the connection between the user and the transmitted information during data transmission. The proposed method protects the privacy of remote monitoring data by dividing the user authorization process into two network services and by anonymizing the remote monitoring data. We present the design principles and the algorithms of operation. The remote monitoring tools with data transmission protection by anonymization were implemented as the result of the conducted research.

Keywords 1

Anonymization, data protection, protection of data transfer, remote monitoring.

1. Introduction

Remote monitoring tools obtain measurements from wireless wearable devices and process them to support some applications such as health monitoring, localization, and crowd density estimation. They transmit data from wireless wearable devices to cloud services and connect these services to mobile terminals [1].

To allow interaction between users and to process the parameters of interest, users are required to enter personal data. In comparison to technical data, the feature of personal data is that they carry information by which you can identify the user. Therefore, it is necessary to obtain permission from the user to process his data and store them. In most countries, the law protects personal data. For example, in the European Union, there is a general regulation on data protection (GDPR Regulation (EU) 2016/679) [2].

However, even if authorized by users, the collected personal data can be attacked by intruders, and undesired privacy leaks can occur; so the task is to ensure their protection.

IntelITSIS'2023: 4th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 22–24, 2023, Khmelnytskyi, Ukraine
EMAIL: aomelnyk@gmail.com (A. Melnyk); jean-yves.leboudec@epfl.ch (J-Y. Le Boudec); yurii.v.morozov@lpnu.ua (Y. Morozov); havano.bohdan@gmail.com (B. Havano); gypalo911@gmail.com (P. Hupalo)
ORCID: 0000-0002-8981-0530 (A. Melnyk); 0000-0003-2357-8078 (J-Y. Le Boudec); 0000-0002-3670-411X (Y. Morozov); 0000-0002-2546-1917 (B. Havano); 0000-0003-4984-3220 (P. Hupalo)

2. Status of the problem

All of the above raises the issue of choosing an effective mechanism for data anonymization.

As demonstrated in de-anonymization methods, i.e., the restoration of personal data from anonymized data presented in scientific literature, removing direct identifiers such as full name and address is insufficient to ensure confidentiality of individuals. Data set owners must be aware of the risks of de-anonymization and apply appropriate anonymization measures before granting access to their data sets to comply with data protection regulations. To meet this need, a procedure was defined in [3] that informs data set owners of de-anonymization risks and helps them make decisions regarding anonymization measures that need to be taken to comply with the General Data Protection Regulation (GDPR). This paper demonstrates the application of the de-anonymization assessment procedure to a customer relationship management (CRM) data set provided by a telecommunications provider.

In addition, in [4], the authors evaluated the practical feasibility of anonymizing electronic health records (EHR) data with regard to their suitability for making medical decisions. In a real-world scenario, effective anonymization of data is challenging because it typically depends on the problem and requires significant expertise in the field. As the level of data anonymity increases, the convenience of using anonymous data decreases and most likely reaches a minimum convenience before achieving full anonymity.

In [5], possible schemes for publishing healthcare data that guarantee more reliable data confidentiality while preserving the usefulness of published data were proposed. Two confidentiality models were identified: identity unlinkability and attribute unlinkability, which include the possibility of unlinkability in data anonymization. The absence of the possibility of disconnection during data transmission may lead to a breach of patient confidentiality, as the patient can be tracked or linked. This prompted the authors to develop two schemes that use these confidentiality models for data anonymization in two different data transmission scenarios.

A combination of pseudonymization and anonymization methods can provide additional protection when data is first anonymized by removing any personal identifiers and then encrypted before storage [6]. When data is properly anonymized by removing all identifiers, it is no longer subject to GDPR, allowing companies to collect such data without consent and store it indefinitely.

User confidentiality is the primary criterion for allowing the transmission of confidential information. In article [7], the Privacy Preserving Data Mining (PPDM) approach is discussed, which analyzes data while maintaining confidentiality. PPDM methodologies are reviewed and classified using different approaches to modify data for anonymization. In addition, a critical comparative analysis of the advantages and disadvantages of PPDM methods is performed.

Article [8] presents a protocol for data collection with confidentiality preservation. This protocol does not restrict the type of anonymization method and does not require a private channel. It only requires k-anonymity to prevent attacks on confidentiality, and thus equivalent groups of owners of data sets function as a mechanism for preserving confidentiality.

The main problem of data exchange is the intelligent control of the security of private data [9]. In this work, a structure for evaluating data anonymization is proposed, which can evaluate typical data anonymization algorithms in terms of the level of confidentiality preservation, data usefulness, and productivity.

Therefore, as the analysis of recent scientific publications has shown, information systems require user authentication to access their data, but at the same time, the data transmitted must be anonymized. It is necessary to combine the user authentication process with the process of anonymizing the data being transmitted. This will increase the level of data anonymity while preserving the convenience of using anonymous data.

3. Selection of technologies for protecting the transmission of personal data in the remote monitoring tools

Personal data is necessary for the authorization of the user in the information system. This data must be transferred and saved. To avoid problems with processing personal data, we propose using a remote authorization service that will process personal data. Single Sign-On technology can be used to provide simultaneous access to various services [12].

The wireless wearable devices are connected to the user's mobile terminal through Bluetooth. The user enters personal data into their mobile terminal. This data should not be stored in the mobile terminal to ensure compliance with Single Sign-On technology. Therefore, the user must connect to remote authorization services from the mobile terminal.

4. Anonymization of user's personal data

Data anonymization is a method of removing or encrypting personal data in a data set. At the same time, to enable data further analysis the existing data structure is supported. The goal of anonymization is to ensure the confidentiality of the subject's information.

In accordance with the European Union's General Data Protection Regulation (GDPR), which requires pseudonymization or anonymization of stored information of persons living in the EU, anonymized data are not classified as personal data and are therefore not subject to the rules of this regulation. It allows organizations to use anonymized data without violating the rights of data subjects. Similarly, data anonymization is a core component of HIPAA requirements, a US regulatory act that governs the use of private health information (PHI) in the healthcare industry [13].

First, information that allows the identification of a person is anonymized. This includes name, as the most important identifier in the data set, credit card details, mobile numbers, photos, passwords, security questions, health data, and more.

Anonymization is used to preserve the confidentiality of the patient's information about his illness, to preserve the confidentiality of customers whose data is used in digital advertising in marketing social networks, to preserve the confidentiality of information about company employees, which is collected for the purpose of increasing productivity, optimizing work, and improving security.

The following methods are used to anonymize data [14,15,16,17]:

- Data masking by providing access to a modified version of sensitive data.
- Pseudonymization of data by replacing private identifiers with pseudonyms or fake identifiers.
- Generalization of data by excluding certain data from it to make it smaller identified.
- Shuffle or rearrange the data by changing the value of the attributes of the dataset.
- Data perturbation using rounding and random noise techniques.
- Creating synthetic data using pattern-based mathematical systems or features in the original data set.

Data in remote monitoring tools are divided into personal data and technical data. Personal data is used infrequently, so it can be separated from technical data and protected by reliable cryptographic means. Technical data in this case is classified as big data. The processing of technical data requires significant computing resources both in the mobile terminal and in the cloud service. Therefore, from a productivity point of view, it is advisable to carry out minimal protection of technical data or not to protect it at all if it can be anonymized [10].

Personal data and technical data should be linked with some user identifier. Each time the mobile terminal and cloud service interact, the user identifier is transmitted together with the technical data.

Technical data, as well as personal data, are interesting to the attacker in case they can establish the identity of a certain user. Data protection can be done using user anonymization technology, such as shown in [19] and [18]. However, these technologies are complex and require significant computing resources.

An alternative is to break the connection between personal and technical data, using the method in [21]. With this method, the mobile terminal establishes a connection with the cloud service, transmits the encrypted user identifier and date/time label, and obtains a temporary "authorization user id". The cloud service decrypts the received identifier and date/timestamp and compares this label with the running time. If time is significantly different, then the data is falsified. The authorization user id is changed periodically. With every interaction between the mobile terminal and the cloud service,

another authorization user id accompanies the technical data. This does not allow the establishment of a direct connection between technical data and the user.

4.1. User authentication

Authentication is the process of secure user identification. The authentication mechanism provides access control for systems by verifying that the user credentials match the data in the authorized user database or on the data authentication server. Authentication methods are divided depending on the type of resource, structure and method of network organization, object remoteness and technology used in the recognition process.

Remote monitoring tools operate using a client-server architecture. User authentication takes place in the cloud service, and the mobile terminal contains the user interface for this service. It is advisable to divide the processes of authentication and remote monitoring between two cloud services. One of these services deals only with authentication and informs the other service about the authenticated user.

The most reliable and rich cloud authentication services use oAuth2 technology [20]. It allows applications to exercise limited access to user accounts on HTTP services. It uses an authentication token sent to the user, allowing a third-party application to access the user's account.

OAuth2 is a widely used security standard that provides secure access to protected resources in a way convenient for the web API. As it uses HTTPS and sends the authentication token in headers, this protocol can be used in web, desktop, and mobile applications.

Given that the technology is decentralized, it does not matter how it will be used. It works in parallel and independently. Therefore, you can use several authorization services at the same time, depending on your preferences. Accordingly, the remote monitoring cloud service receives information about the authorized user of any of the cloud services built on this technology.

4.2. Protection of data transmission in remote monitoring tools

Data on the measuring device is not tied to the user. They are transmitted to the user's mobile terminal using Bluetooth technology, which provides protection against falsification and modification of transmitted data. On the other hand, energy efficiency requirements do not recommend the use of additional means of information security.

In a mobile terminal, data is associated with the user and becomes sensitive to interference. At the same time, the requirements for energy efficiency are not as strict as for metering devices. Therefore, it is advisable to apply the protection of the communication channel. Use TLS 1.3 or IPsec to protect transmitted data. Most IPsec implementations are more reliable than some TLS 1.3 implementations, but more energy intensive. Therefore, the TLS 1.3 protocol is most often used in mobile terminals and, accordingly, in cloud services [23].

This technology is used to make sure that any data transmitted between the mobile terminal and the cloud service remains impossible to read [22]. Encryption algorithms are used to encrypt data during transmission, not allowing hackers to read it when they are sent. This information may be confidential or personal, which may include technical or personal data.

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and autonomous way of safely transmitting information between parties as a JSON object [23]. JWT is a base64 encoded JSON object that is considered a secure way of transmitting information between two participants.

Improper storage of tokens leads to their potential theft and malicious actions.

Most often, JWT is used for authorization. Once the user is logged in, each subsequent request contains JWT, which allows the user to access the routes, services and resources allowed by this token. Authorization is a process that today makes extensive use of JWT through small resources and the ability to use across domains.

Compared to other standards such as Simple Web Tokens (SWT) and Security Statement Markup Language Tokens (SAML), JWT is more compact and more appropriate to use for different platforms, especially mobile terminals.

4.3. Base request structure

A typical request with technical data consists of an authorization header and payload as the request body. Figure 1 shows an example of data structure in the request.

```
POST /echo/post/json HTTP/1.1
Host: cloud-service.com
Authorization: Bearer JWT-token-value
Content-Type: application/json
Body:
{ "spo2_values": [],
  "pulse_values": []
}
```

Figure 1. An example of data structure in the request

The authorization header has the JWT access token, received from auth service. The payload is a set of technical data without any personal data in it. The JWT token is used to process data and store it in relation to a specific user in the database. Since personal data are missing, a user identifier from auth service is the only possible way to map technical data to a specific user.

Once a request from the mobile terminal goes to cloud service, this request must be authorized first. A JWT token from the authorization header is taken. The next step is to verify this token using a public key in JWKS format. If the token is verified and valid it is possible to extract some data from it.

Figure 2 shows the general structure of a decoded token.

```
{
  iss: 'issuer',
  sub: 'auth-user-id',
  aud: [],
  iat: 1589809948,
  exp: 1589896348,
  azp: 'app_ID',
  scope: ‘list of scopes’
}
```

Figure 2. General structure of the decoded token

It is also possible to add another authorization layer using allowed scopes which are also defined in the access token. Using sub value from the token object we can identify an anonymized user by id. So, even without any personal data, it is possible for an information system to transfer, process and store technical data in relation to some specific user in the database.

4.4. Protection of data transfer via VPN

Anonymization protects data from identification but does not protect against modification and unauthorized viewing. Virtual private network (VPN) technology is used to protect the transmitted data. It consists in creating cryptographically protected tunnels through open communication

networks. The essence of tunnelling is that anyone outside (for example, a cryptanalyst) does not have access to the information being transmitted.

TLS 1.3 or IPsec protocols are used to create a VPN. As it was mentioned above, most IPsec implementations are more reliable than some TLS 1.3 implementations, but more energy intensive. Therefore, the TLS 1.3 protocol is most often used in mobile terminals and, accordingly, in cloud services [23, 26].

TLS 1.3 (Transport Layer Security) is a standard technology for securing Internet connections and protecting any sensitive data that is transmitted between two systems by preventing cryptanalysts from reading and modifying any information transmitted. The handshake protocol is responsible for creating a tunnel in TLS 1.3. This protocol uses public key technology in the form of X.509 digital certificates.

Figure 3 shows what happens during the TLS 1.3 handshake.

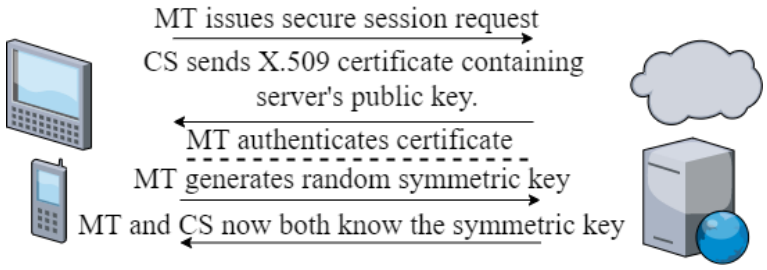

Figure 3. TLS 1.3 handshake protocol

The sequence of interaction steps is as follows:

1. Mobile terminal (MT) sends a request to the server for a secure session.
2. The cloud service (CS) responds by sending its X.509 digital certificate to the client.
3. Mobile terminal obtains the X.509 digital certificate of the server and authenticates the server using a list of known certification authorities.
4. Mobile terminal generates a random symmetric key and encrypts it with the public key of the cloud service.
5. Mobile terminal and cloud service now know the symmetric key and can use it to encrypt and decrypt the information contained in the request of the mobile terminal and the response of the cloud service.

The symmetric key obtained using the handshake protocol is used to encrypt all transmitted information. This information can be confidential or non-confidential, which may include biometric data. The lifetime of a symmetric key is limited so as not to give the cryptanalyst enough data to analyze.

This technology is used to make sure that any data transferred between the mobile terminal and the cloud service remains unreadable. Encryption algorithms are used to encrypt data in transit, preventing cryptanalysts from reading it as it is sent. This information can be of any kind, which may include biometric data.

5. Structure and operation of remote monitoring tools with data transmission protection

The proposed structure of remote monitoring tools with technical protection of data transmission is shown in Figure 4. The remote monitoring tools include the following components:

- measuring device,
- mobile terminal,
- authentication service,
- cloud service,
- database.

The measuring device consists of sensors that collect information and transmit it to a mobile terminal.

The mobile terminal consists of the sensors data receiver for data acquisition from sensors of measuring devices, a data transmission unit for data transmission to the cloud service (for interaction with the cloud service), and an authentication unit (for interaction with the authentication service).

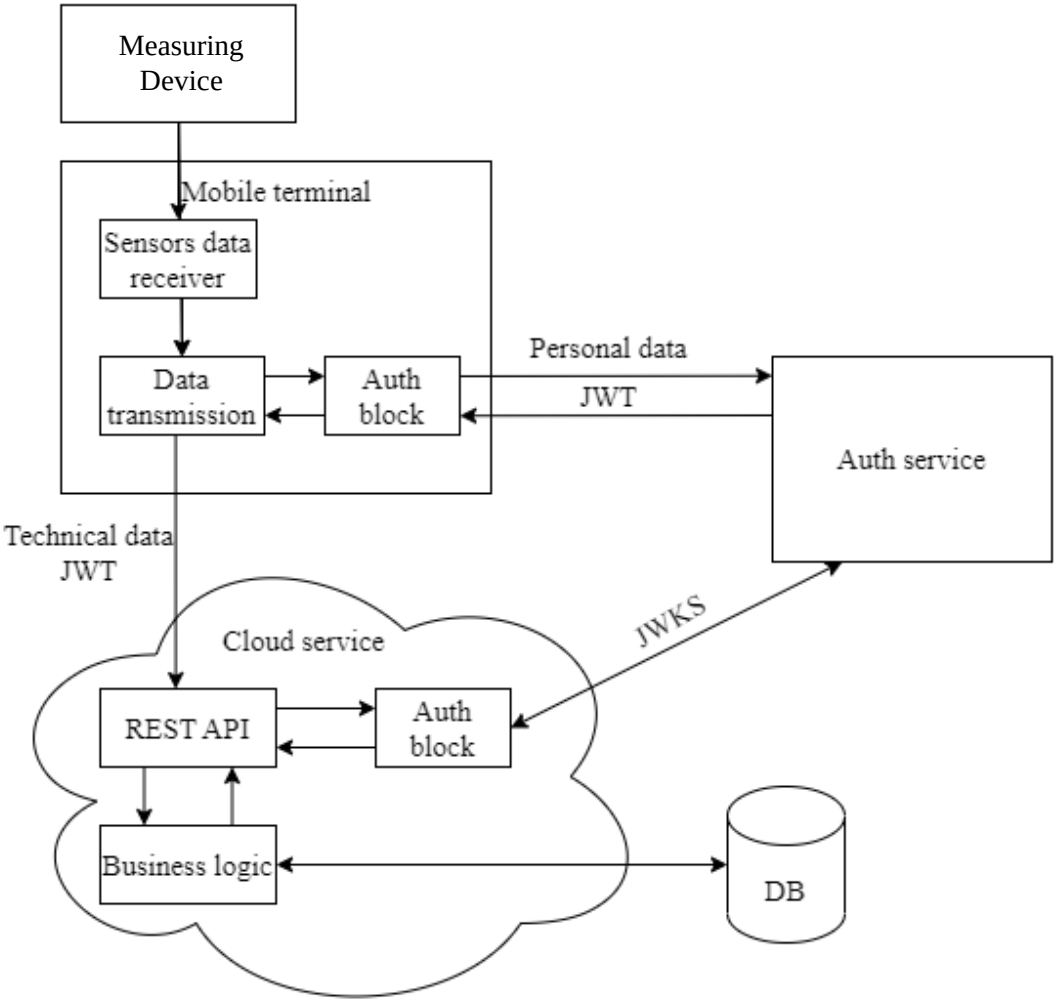

Figure 4. The structure of remote monitoring tools

In the presented remote monitoring tools, data pseudonymization is used to anonymize data. Pseudonymization of data consists in replacing the user ID with an encrypted JWT token. Because the JWT token is encrypted using the TLS 1.3 protocol, which uses revocable symmetric keys, there is no way to detect the connection between the user and the transmitted information during data transmission.

The Authentication Service includes decentralized user authentication technologies that operate independently of each other.

The cloud service receives data from the mobile terminal as a REST API. As in the mobile terminal, there is an authentication unit. The business logic block is an important part of the cloud service, which is responsible for the processing and storage of information.

The database is a repository where personal and technical data that has been processed in the business logic block is stored.

The processing and storage of user personal data in the system are absent. Personal data, such as login and password, are used for authentication. They are not saved anywhere in the information

system but passed from the mobile terminal to auth service for further authorization. The cloud service never receives or stores any personal data.

The principles of mobile terminal (MT) operation with the protection of technical data transmission are shown in Figure 5.

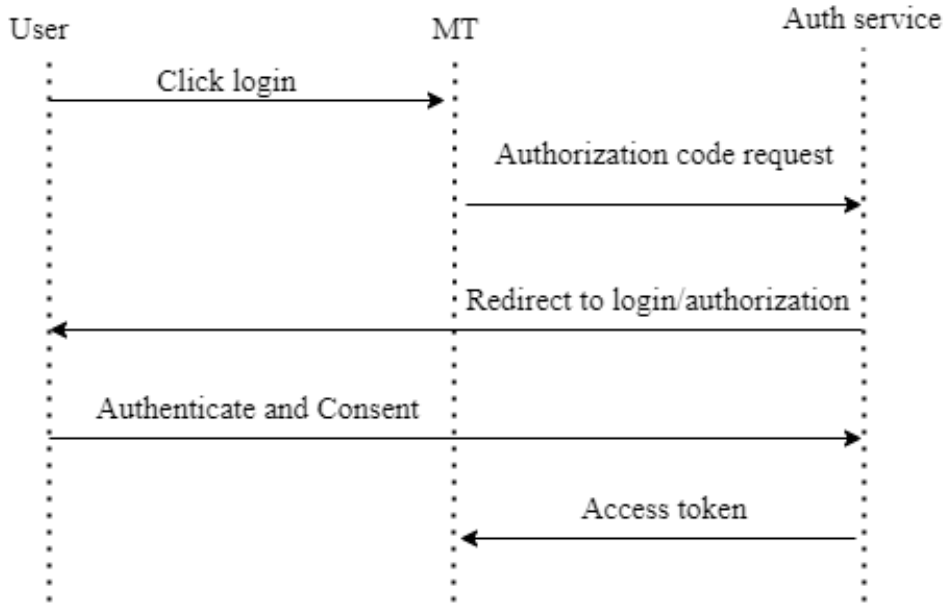

Figure 5. The flow of operation of the client application on the mobile terminal

The very first step is to authenticate the user. The client application for the mobile terminal first checks the presence of an up-to-date authentication access token in the local secret storage. If the token is missing or the expiration time has occurred, the application will require the user to authenticate to the authentication server. After successful authentication, the application switches to continuous data transfer of the parameters of interest to the cloud service. MT sends only technical data to the cloud service along with a JWT token without any personal data. The JWT token only knows the authentication user id, which is used to map data in the cloud service DB. Note that it is not possible to impersonate users using this identifier, thus every user is anonymized in the information system.

If the measuring device contains means of accessing the Internet, for example, WiFi, then the principle of operation in this form is shown in Figure 6.

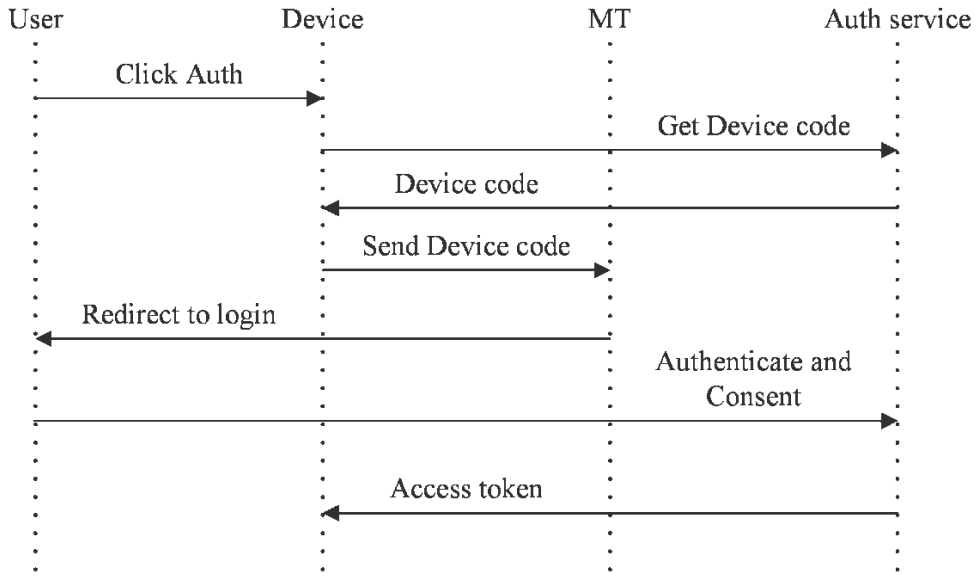

Figure 6. The flow of operation of the client application on the measuring device

Like the previous algorithm, the first step is user authentication. The Measuring device app first checks for a valid authentication access token in the local secret store. If the token is missing or expired, the application will require the user to authenticate with the authentication server. But, in this case, the Measuring device app will first receive the Device Code from the authentication server, which is transmitted by the mobile terminal. On the mobile terminal, the user enters a login and password, because there is no keyboard on the measuring device. After successful authentication, the Measuring device app receives a JWT token and switches to the constant transfer of the data of the parameters of interest to the cloud service. The measuring device sends only technical data to the cloud service along with the JWT token without any personal data.

In this way, the transmitted data is completely anonymized in the information system.

The algorithm of operation of Cloud Service (CS) for processing technical data is shown in Figure 7.

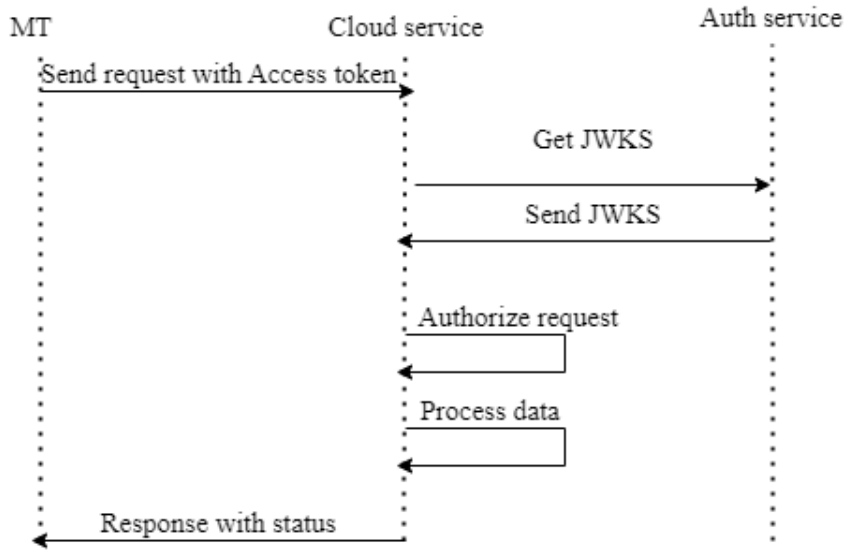

Figure 7. The flow of operation of CS for protecting the transmission of technical data

Once MT obtains the Access token it is possible to make authorized requests to the Cloud Service. Each request from MT to CS should have an authorization header with a JWT token obtained from auth service.

Auth service uses RSA Signature with SHA-256 for signing tokens. Since it uses a private/public keypair, it verifies the tokens against the public key for CS. The public key is in the JSON Web Key Set (JWKS) format.

CS should obtain JWKS with the public key to be able to verify the access token received from MT and to authorize the request and the user. It is important that CS doesn't make any requests to obtain any personal data. It means that the developed information system does not have any personal data transmission or storage.

Using JWKS, CS can authorize the request and process incoming data if authorization is successful. In other cases, MT will receive an unauthorized response. During data processing, CS retrieves the user identifier from JWT and links processed data in storage with the authentication user id. the last step is to send the response from CS to MT.

6. Device authentication process

With input-constrained devices that connect to the internet, rather than authenticate the user directly, the device asks the user to go to a link on their smartphone and authorize the device. This avoids a poor user experience for devices that do not have an easy way to enter text. To do this, device apps use the Device Authorization Flow (ratified in OAuth 2.0) [27], in which they pass along their Client ID to initiate the authorization process and get a JWT token. Flow example is presented on figure 8.

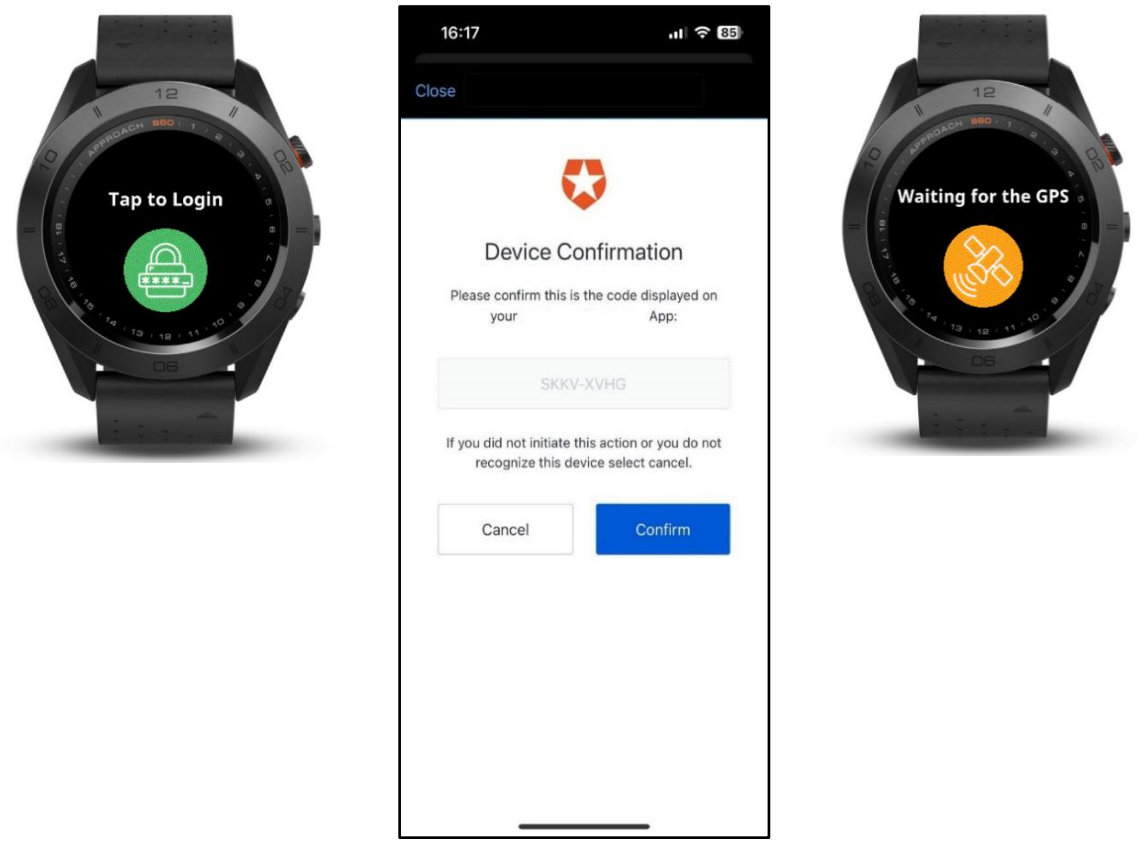

Figure 8. Device app screen (left), smartphone authorization screen (middle) and device app after successful authorization (left).

7. Conclusion

Personal data often becomes the object of attack by intruders, so the task is to ensure their protection. Personal data in remote monitoring tools should not be stored in users' mobile terminals, cloud services, but should be transferred between them. Therefore, it is necessary to protect this data in all these places. That is, it is necessary to provide means of secure authorization, both in mobile terminals and in cloud services, and to secure the transmission of this data.

A literature review has revealed that there is a problem with deanonymization of data, as well as the depth of anonymization that is related to the convenience of data usage. This is linked to the problematic non-binding of identity. However, the combination of pseudonymization and anonymization methods can provide additional protection by removing any personal identifiers. The main issue in data exchange is the intelligent control of private data security.

Based on this, it is proposed to divide data into personal and technical data. At the same time, personal data are protected as much as possible, and technical data are anonymized. In measuring devices, basic protection of technical data is achieved by using Bluetooth technology. No personal data is stored in the mobile terminal. User authentication is carried out on decentralized cloud services using oAuth2 technology. From the mobile terminal, information is transmitted to the cloud service via HTTPS (TLS) using JWT tokens to authorize requests.

The proposed method to protect the transmission of remote monitoring data is to divide the user authorization process into two network services and the subsequent anonymization of remote monitoring data. Thus, the data collection and processing service only receives anonymous data. Based on this method, the principles of design, algorithms of operation and the remote monitoring tools with the protection of data transmission have been developed.

In the future, it is planned to expand the research not only in terms of data transmission but also data storage. Anonymization of stored data is a separate task, the solution of which will allow for a comprehensive solution to the issue of personal data protection in data collection and processing systems.

8. References

[1] A. Melnyk, Y. Morozov, B. Havano, P. Hupalo. HealthSupervisor: Mobile Application for Round-the-Clock Remote Monitoring of the Human Functional State (keynote). Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS. Khmelnytskyi, Vol-2853, Ukraine, March 24–26, 2021, pp. 24-37.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), [2016] OJ L 119/1.

[3] A. Bampoulidis, A. Bruni, I. Markopoulos, M. Lupu, Practice and Challenges of Anonymisation for Data Sharing. In: Dalpiaz, F., Zdravkovic, J., Loucopoulos, P. (eds) Research Challenges in Information Science. RCIS 2020. Lecture Notes in Business Information Processing, vol 385. Springer, Cham. doi:https://doi.org/10.1007/978-3-030-50316-1_32.

[4] Z. Zuo, M. Watson, D. Budgen, R. Hall, C. Kennelly, N. Al Moubayed Data Anonymization for Pervasive Health Care: Systematic Literature Mapping Study JMIR Med Inform 2021 doi: 10.2196/29871

[5] KM Chong, A. Malip, Bridging unlinkability and data utility: Privacy preserving data publication schemes for healthcare informatics, Computer Communications, 191 (2022) 194-207, doi:https://doi.org/10.1016/j.comcom.2022.04.032.

[6] G.M.S. Ross, Y. Zhao, A.J. Bosman, A. Geballa-Koukoula, H. Zhou, C.T. Elliott, M.W.F. Nielen, K. Rafferty, G.IJ. Salentijn, Best practices and current implementation of emerging smartphone-based (bio)sensors - Part 1: Data handling and ethics,TrAC Trends in Analytical Chemistry, 158 (2023) doi: https://doi.org/10.1016/j.trac.2022.116863.

[7] M. Binjubeir, A. A. Ahmed, M. A. B. Ismail, A. S. Sadiq and M. Khurram Khan, Comprehensive Survey on Big Data Privacy Protection, in IEEE Access, 8 (2020) 20067-20079. doi: 10.1109/ACCESS.2019.2962368.
[8] S. Kim, Y. Dohn Chung, An anonymization protocol for continuous and dynamic privacy-preserving data collection, Future Generation Computer Systems, 93 (2019) 1065-1073, doi:https://doi.org/10.1016/j.future.2017.09.009.
[9] C. Ni, L. Shan Cang, P. Gope, G. Min, Data anonymization evaluation for big data and IoT environment, Information Sciences, 605 (2022) 381-392, doi:https://doi.org/10.1016/j.ins.2022.05.040.
[10] G. Zhao, D. Zheng and K. Chen, Design of single sign-on, IEEE International Conference on E-Commerce Technology for Dynamic E-Business, 2004, pp. 253-256, doi: 10.1109/CEC-EAST.2004.34.
[11] A. Jayanthilladevi, K. Sangeetha and E. Balamurugan, Healthcare Biometrics Security and Regulations: Biometrics Data Security and Regulations Governing PHI and HIPAA Act for Patient Privacy, 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2020, pp. 244-247, doi: 10.1109/ESCI48226.2020.9167635.
[12] A. Gkoulalas-Divanis, G. Loukides and J. Sun, "Toward smarter healthcare: Anonymizing medical data to support research studies," in IBM Journal of Research and Development, vol. 58, no. 1, pp. 9:1-9:11, Jan.-Feb. 2014, doi: 10.1147/JRD.2013.2288173.
[13] D. Gunawan, Y. S. Nugroho, Maryam and F. Y. Al Irsyadi, Anonymizing Prescription Data Against Individual Privacy Breach in Healthcare Database, 2021 9th International Conference on Information and Communication Technology (ICoICT), Yogyakarta, Indonesia, 2021, pp. 138-143, doi: 10.1109/ICoICT52021.2021.9527430.
[14] B. Ouafae, R. Mariam, L. Oumaima and L. Abdelouahid, Data Anonymization in Social Networks State of the Art, Exposure of Shortcomings and Discussion of New Innovations, 2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Meknes, Morocco, 2020, pp. 1-10, doi: 10.1109/IRASET48871.2020.9092064.
[15] S. Dimopoulou, C. Symvoulidis, K. Koutsoukos, A. Kiourtis, A. Mavrogiorgou and D. Kyriazis, Mobile Anonymization and Pseudonymization of Structured Health Data for Research, 2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ), Gainesville, FL, USA, 2022, pp. 1-6, doi: 10.1109/MobiSecServ50855.2022.9727206.
[16] C. Stergiou, KE. Psannis, Efficient and secure BIG data delivery in Cloud Computing. Multimed Tools Appl 76, (2017) 22803–22822, doi: 10.1007/s11042-017-4590-4.
[17] N. Elanshekhar and R. Shedge, An effective anonymization technique of big data using suppression slicing method, 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 2500-2504, doi: 10.1109/ICECDS.2017.8389902.
[18] A. Salami, J. Andreu-Perez and H. Gillmeister, "Towards Decoding of Depersonalisation Disorder Using EEG: A Time Series Analysis Using CDTW," 2020 IEEE Symposium Series on Computational Intelligence (SSCI), 2020, pp. 548-553, doi: 10.1109/SSCI47803.2020.9308273.
[19] A. Melnyk, Y. Morozov, B. Havano and P. Hupalo, Protection of Biometric Data Transmission and Storage in the Human State Remote Monitoring Tools, 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021, pp. 301-306, doi: 10.1109/IDAACS53288.2021.9661047.
[20] OAuth 2.0, May 2021, URL: https://oauth.net/2/
[21] D. Wagner and B. Schneier, Analysis of the SSL 3.0 protocol, The Second USENIX Workshop on Electronic Commerce Proceedings, vol. 1, no. 1, 1996, pp. 29-40.
[22] The SSL/TLS Handshake: an Overview, May 2021, URL: https://www.ssl.com/article/ssl-tls-handshake-overview/
[23] Jones et al. JSON Web Token (JWT). RFC 7519. RFC Editor, May 2015. URL: http://www.rfc-editor.org/rfc/rfc7519.txt.
[24] Y. Cheng, W. Kang M. Xiao, Model checking of SSL 3.0 protocol based on SPIN, 2010 2nd International Conference on Industrial and Information Systems, Dalian, 2010, pp. 401-403, doi: 10.1109/INDUSIS.2010.5565737.
[25] Denniss, et al. OAuth 2.0 Device Authorization Grant. RFC 8628. RFC Editor, August 2019. URL: https://www.rfc-editor.org/rfc/rfc8628.