Method of patients’ data protection on the instance of chemotherapy dosing data for Ewing's sarcoma treatment[*]

Yurii Baryshev[1] and Vladyslava Lanova[2,*]

1,2 Vinnytsia National Technical University, 95 Khmelnytske shose, Vinnytsia, 21021, Ukraine

Abstract

The method of patients’ data protection on the instance of chemotherapy dosing data calculation process for Ewing's sarcoma treatment which improves the protection of personal data of cancer patients is proposed in this article. While performing this work, the types of homomorphic encryption, their features and examples of applications for this subject area were analyzed. After analyzing the known solutions, it was decided to develop method which combines homomorphic encryption with a distributed data storage such as blockchain. The instance of proposed method’s implementation is presented. At the end of the work, we draw conclusions and set tasks for the future research in this area.

Keywords

Cyber security, cryptography, homomorphic encryption, smart contract, blockchain, medical data protection, critical infrastructure.

1. Introduction

The need for personal data protection of patients is relevant everywhere. In Ukraine, the Law on Personal Data Protection [1] establishes key principles for safeguarding personal information, including healthcare-related data. This law requires that healthcare organizations ensure the integrity, availability, and confidentiality of patient data.

Compliance with laws and regulations, such as the General Data Protection Regulation (GDPR) [2] in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) [3] in the United States, is essential. These regulations establish high standards for the data protection, requiring healthcare organizations to implement measures to safeguard patient confidentiality.

Nowadays, the number of cancer patients is increasing, and each patient requires an individual approach to treatment. Nowadays, patients often move, which can lead to the risk of losing critical health data. For instance, the war in Ukraine has resulted in a significant number of internal refugees. These individuals may face challenges in maintaining consistent medical records, which can affect their treatment.

To solve these problems, it is important to implement data protection, including encryption of patients’ personal data. Encrypting patient data ensures that even if records are transferred or accessed from different locations, the information remains secure and protected from unauthorized access. However the usage of encryption making it more difficult to process data, because it is needed to be decrypted before making an alterations and re-encrypted afterwards for the storing at the media.

[*] *IDDM’24: 7th International Conference on Informatics & Data-Driven Medicine, November 14 - 16, 2024, Birmingham, UK*

[*] Corresponding author.

[1] Author contributed sections 1, 4, 5, 7, proofreading and general editing.

[2] Author contributed sections 2, 3, 6, software implementation and paper formatting.

yuriy.baryshev@vntu.edu.ua (Y. Baryshev); lanovaia02y@gmail.com (V. Lanova)

0000-0001-8324-8869 (Y. Baryshev); 0009-0007-4025-1866 (V. Lanova)

Known approaches for data storing uses databases, clouds and blockchain. However each of these approaches has drawbacks in comparison to others: databases lacking availability and integrity protection of the stored data; clouds needs secure connection and complete trust to the cloud provider, thus creating problems for information security compliance; blockchains aren't designed for storing big data arrays and are open for all the peers for reading stored data, thus creating additional tasks for data privacy protection. The latter creates tasks of data protection improvement for the mediums.

The goal of this study is to improve the protection of patients' personal data by using homomorphic encryption.

To achieve the goal of this study, one should solve the following tasks:

1. Known approaches analysis.
2. Task formalization.
3. Data protection method development.
4. Software development.
5. Implementation results analysis.
6. Conclusion drawing.

The main contribution of the research is method of homomorphic encryption utilization for the blockchain as a storage medium for patients' data, which allow to avoid additional read/write operations in case of data updating.

The structure of the paper is the following: section 2 contains preliminaries in order to cover the background of the research, section 3 is devoted to the state of the art analysis followed be task formalization presented in the section 4, the main results are presented at section 5, where proposed method is presented, and section 6, where its software implementation and use-case are shown, section 7 contains further discussion and conclusions of the research.

2. Preliminaries

2.1 Homomorphic encryption

Homomorphic encryption is a form of encryption that allows computations to be performed on encrypted data without need to decrypting it beforehand. This is particularly valuable when sensitive data needs to remain confidential but still requires processing. In homomorphic encryption, an encrypted input produces an encrypted output that, when decrypted, matches the result of the operation as if it had been performed on the plaintext data [4].

There are two primary types of homomorphic encryption systems:

1. Partially homomorphic encryption [4]: these schemes allow only specific operations (either addition or multiplication) to be performed on the encrypted data. For example, Paillier encryption [5] supports additive homomorphism, meaning that we can perform additions on ciphertexts that correspond to the addition of plaintext values once decrypted, but for the multiplication one of the operands should be in the open form.

2. Fully homomorphic encryption [4]: extends the capabilities of partially homomorphic encryption by supporting arbitrary operations, including both addition and multiplication in encrypted form. Fully homomorphic encryption schemes can perform any kind of computations on encrypted data, making them extremely powerful but also computationally expensive and less practical for large-scale or time-sensitive tasks.

2.2 Paillier cryptosystem

The example of partially homomorphic encryption is Paillier cryptosystem [6]. One of the advantages of the Paillier cryptosystem is its homomorphic property in combination with non-deterministic encryption due to the random number usage.

The basic public key encryption scheme has three steps:

Step 1. Generate a public key pair (n, g). To achieve this one needs to generate large prime numbers p and q of equal bit length.

Then compute:

$$n = p \cdot q \tag{1}$$

Then one need to randomly generate g such as $g \in Z_{n^2}^{¿}$.

Step 2. The private decryption key is (λ, μ). To achieve this one needs to compute λ as:

$$\lambda = lcm(p-1, q-1), \tag{2}$$

where $lcm(.)$ means least common multiple.

Then is used to calculate the modular multiplicative inverse:

$$\mu = \left(L\left(g^{\lambda} \, mod \, n^2\right)\right)^{-1} mod \, n, \tag{3}$$

where the function $L(x) = \frac{(x-1)}{n}$ (quotient of integer division).

Pick a random number r in the range $0 < r < n \wedge gcd(r, n) = 1$.

Step 3. To encrypt the message (m), where $0 \leq m < n$, should need to compute c as:

$$c = g^m \cdot r^n, \tag{4}$$

where c – ciphertext.

Step 4. To decrypt the m should need to do the next computation:

$$m = L\left(c^{\lambda} \, mod \, n^2\right) * \mu \, mod \, n, \tag{5}$$

where c – ciphertext to decrypt and $c \in Z_{n^2}^{¿}$.

Among the operations supported by Paillier's scheme are homomorphic addition (6) and multiplication (7), but it should be noted that without knowledge of the private key there is no way to calculate the product of encrypted messages.

When two ciphertexts are multiplied, the result decrypts to the sum of their plaintexts:

$$D\left(E_{pub}(m_1) * E_{pub}(m_2) \, mod \, n^2\right) = m_1 + m_2 \, mod \, n, \tag{6}$$

where D is the multiplication need to decrypt.

When a ciphertext is raised to the power of a plaintext, the result decrypts to the product of the two plaintexts:

$$D \; mod \, n^2 = m_1 * m_2 \, mod \, n \tag{7}$$

Paillier is computationally less expensive than fully homomorphic encryption schemes like BFV [7], CKKS [8] or more recently proposed method [9]. Therefore it is more preferable for the implementation at the research due to lesser computational difficulty resulting in quicker and computationally less demanding data updating.

2.3 Chemotherapy dosing calculation methodology

For the chemotherapy calculations the main factor is body surface area (BSA) [10]. BSA based dosing is used to calculate prescribed dose of drug meeting the balance between cancer treatment efficiency and drug toxicity [11]. The main uses of BSA is – it determines the dose of chemotherapy for a patient. Formula for BSA calculation:

$$BSA=\sqrt{\frac{h*w}{3600}} \tag{8}$$

Mosteller formula for BSA dosing [12]:

$$Dose=BSA*ct\,, \tag{9}$$

where ct is the $doseCoefficien$t,

h – $height$ of the patient,

w – $weight$ of the patient.

The above preliminaries became the basis for known approaches analysis for this field.

3. Known approaches analysis

Homomorphic encryption is used in the medical field to enhance data privacy while enabling computations on encrypted datasets. One notable example is the Swiss project MedCo [13], which is a part of the Data Protection and Personalized Health initiative. MedCo leverages homomorphic encryption to facilitate secure and privacy-preserving data discovery across multiple hospitals, allowing for analytics on both genetic and non-genetic patient data without revealing raw data.

HE facilitates secure analysis of cardiovascular data, enabling encrypted computations to pinpoint high-risk individuals and forecast disease progression without compromising patient privacy [14].

On the other hand, homomorphic encryption usage in this case possess some disadvantages: high computational overhead, which can reduce performance and scalability, especially when processing large datasets.

Another important usage of homomorphic encryption is collaborative cancer research, where encrypted data from multiple hospitals is examined to identify the most efficient chemotherapy protocols based on different cancer types and patient characteristics [15]. The need for more computational resources, bandwidth, and storage for encrypted data across multiple hospitals can significantly increase operational costs.

There is known an innovative system for lung cancer diagnosis which is based on homomorphic encryption [16, 17]. This system firstly performs textual extraction from computer tomography scans and then applies deep learning techniques for the classification [16, 17]. Applying homomorphic encryption on computer tomography scan textual extraction and then running deep learning models introduces additional latency, which may delay diagnoses.

In the work [18], the author proposes a method for predicting the likelihood of a heart attack based on a few body measurements. This approach employs a client application that gathers health data and transmits it in the encrypted format using Microsoft Azure cloud services [17]. Relying on cloud-based homomorphic encryption (via Microsoft Azure) introduces security concerns around trust in third-party providers and may not comply with stringent healthcare regulations.

Another work proposed a fully homomorphic encryption algorithm for encrypting and decrypting images in healthcare is the research [19]. As the size of medical images increases (e.g., higher resolution scans), the encryption and decryption processes become less scalable requiring more memory and processing power.

These methods suffer from significant computational overhead, especially when processing large datasets or high-resolution medical images, leading to delays and increased operational costs. We address these issues by using the homomorphic encryption scheme that focuses on practical use cases, such as calculating personalized drug doses based on encrypted patient data, without exposing sensitive information.

4. Task formalization

Let's denote by D the patients' data, which is operated by the doctors and is needed for proper calculations of chemotherapy dosage for Ewing's sarcoma treatment. Let M to be the set of data storage mediums those are used to store D and S to be a set of data already stored using mediums M. Therefore it is possible that due to inaccessibility or a destruction of the mediums certain data is missing. The process of storing given amount of data $d \in D$ on the medium $m \in M$ is formalized as the following:

$$store : D \times M \rightarrow S \ or \, s_m = store(d, m). \tag{10}$$

In the formula (10) we used subscript in order to mark the fact, that sm is stored at the medium m.

The reverse process of stored data retrieving is the following:

$$retrieve : S \times M \rightarrow D \ or \, d = retrieve(s_m, m). \tag{11}$$

Due to the criticality of correct dosage and number of sessions the stored data should be updated over time. Consequently there should be updating process:

$$update : S \rightarrow S \ or \, s'_m = update(s_m). \tag{12}$$

The mathematical description of the research field is the following:

$$MathematicalDescription = \{D, S, M, \{store(d, m), update(s_m), retrieve(s_m, m)\}\}. \tag{13}$$

Thus the task of the research is to develop such method of data protection with the following conditions:

1. ***M*** should be robust to the denial of service attacks.
2. Destruction of given medium $m \in M$ shouldn't lead to losses of ***S***.
3. Only authorized persons (the respective patient and doctors, whom the patient granted access) can yield ***D*** from ***S***, i.e. there should be limitations to the persons, who is able to perform data retrieving process *retrieve*().
4. ***S*** must be updated without a disclosure of ***D***, *update*() can be performed arbitrary from *store*() and *retrieve*() processes.

These conditions are to be met by the patient's data protection method.

5. Data protection method

In order to meet above-mentioned conditions sets, stated at the mathematical description (13) are to be identified for the case of data, which is used for chemotherapy dosing calculations in case of Ewing's sarcoma treatment. According to the methodology of the dosage calculations [8] the set ***D*** is a set of vectors, where each vector is associated with a given patient, and the chemotherapy methodology-related constant. Thus ***D*** is defined in the following form:

$$D=\{\{height, weight, chemotherapySessions\}, ct\}, \tag{14}$$

where *height* – a given patient's height, which is used for the BSA computation;

weight – a given patient's weight, which is used for the BSA computation;
chemotherapySessions – a number of already passed chemotherapy sessions;
ct – the scalability coefficient used by the methodology [9, 11].

The chemotherapySessions parameter is needed in order to allow doctors to assign proper number of sessions. This parameter is essential for the considered case of warfare refugees, whom shouldn't be expected to maintain proper medical records or correctly remembering the exect number, because of experienced extreme stress. Moreover the parameter is to be updated after each session, while height and weight might change as well between sessions. Therefore used mediums are to be open for data updates.

In order to meet conditions 1 and 2 defined in the previous section we choose Ethereum-like blockchain [19] as a medium. Usage of multiple nodes at the blockchain any of each can be used for stored data accessing provides robustness to the denial of service attacks thus meeting the condition 1. The very property allows to meet the condition 2, because any node's destruction doesn't lead to data losses. Moreover, the data loss in case of blockchain utilizing as a medium is possible only in case of all nodes destruction, which can be omitted by organizational means such as running several nodes outside warfare territory (abroad in partner countries, for instance) or minimizing the risk by placing nodes in different missile/drone protected areas.

The choice of this type of blockchain is motivated by the scalability of these types of blockchains due to smart contracts as a data structure. Consequently, in case of either chemotherapy dosage calculations methodology alterations, or proposed method usage in similar areas programmability of smart contracts allows to adapt this medium's data structure as well.

Therefore, the set of mediums is:

$$M=BlockchainNodes, \tag{15}$$

where ***BlockchainNodes*** is a set of all blockchain's nodes.

Due to data openness caused by chosen medium and the need of meeting condition 3 stored data ***S*** should be presented in the encrypted form. Therefore, ***S*** is defined in the following form:

$$S=\{\{height^e, weight^e, chemotherapySessions^e\}, ct^e\}, \tag{16}$$

where *height*^{e} – an encrypted value of given patient's height;
weight^e – an encrypted value of weight;
chemotherapySessions^e – an encrypted value of number of already passed chemotherapy sessions by given patient;
ct^e – an encrypted value of *ct*.

The latter parameter is to be encrypted, because its value can help determine what kind of treatment is performed. This will be helpful for scalability reasons as well in case the proposed method and tool would be used for other cases of chemotherapy treatment.

After all data had been defined, the implementation of the processes should be performed. We propose to conduct *store()* process by the following steps:

1. Gather patients identification data *patientID* (such as number of medical record, eHealth account etc) and relevant parameters such as *height* and *weight.*

2. Perform hashing of the *patientID* in order to protect them from the exposure. In case of Ethereum-like blockchain usage it would be natural to use Keccak-256 hash function:

$$path = keccak(patientID). \tag{17}$$

3. Using homomorphic encryption, Paillier scheme in particular, encrypt with a patient's public key *height* and *weight* parameters in order to obtain $height^e$ and $weight^e$ respectively.
4. Access patient's profile or create one at the smart contract ran in blockchain by using mapping of the following kind path ⟶ { $height^e$, $weight^e$, $chemotherapySessions^e$}. In case of profile creation encrypt 0 using patient's public key in order to get $chemotherapySessions^e$.
5. Set obtained at step 3 values of $height^e$, $weight^e$ parameters.

Stored encrypted parameters can be read directly from blockchain in case of correct path parameter computation. Therefore *retrieve()* process is easy to implement for this case. However it doesn't have sense in the research, because the main goal of the *retrieve()* process is to provide respective chemotherapy dose value. Therefore we propose to perform *retrieve()* by the following steps:

1. Gather patients identification data *patientID*.
2. Obtain *path* value using (17).
3. Call smart-contract's method, which computes in encrypted form value of a respective chemotherapy dose using homomorphic transformations and receive $dose^e$.
4. Using patient's private key decrypt $dose^e$ and obtain proper dose value.

After administrating chemotherapy the stored value of $chemotherapySessions^e$ is to be updated. To do so we propose the following *update*() process implementation:

1. Gather patients identification data *patientID*.
2. Obtain *path* value using (17).
3. Encrypt 1 using patient's public key:

$$encryptedOne = g \ \cdot r^n \bmod n^2. \tag{18}$$

4. Retrieve stored value of $chemotherapySessions^e$.
5. Using homomorphic transformation add encrypted 1 to the value of $chemotherapySessions^e$.

$$chemotherapySessions^e = chemotherapySessions^e \ \cdot encryptedOne \bmod n^2. \tag{19}$$

6. Store new value of $chemotherapySessions^e$.

It should be noted, that we used Paillier's method for the homomorhpic encryption, but the method with a small adjustment can be adapted for other homomorphic encryption method usage.

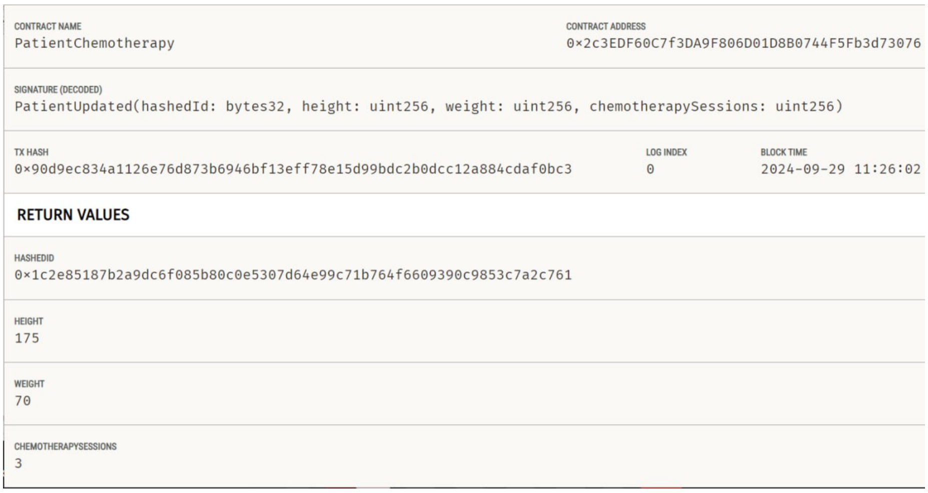
6. Developed Software Tool

Whether during the visiting doctor occurs the situation when the patient does not remember the necessary data for calculating the dose of chemotherapy drug and the number of received chemotherapy sessions, the doctor performs *receive()* process and gains the necessary data for treatment prescribing.

The smart contract was developed that allows to structure the information needed during the process of prescribing further treatment.

PatientChemotherapy smart contract, is designed to manage patient data related to chemotherapy treatments, including tracking a patient's height, weight, and number of chemotherapy sessions. *Patients* mapping – this is a mapping that associates a hashed *patientID* (using keccak256) to a patient's details stored in the *Patient* struct. The *hashedID* ensures that the actual *patientID* is not stored in a plain form, providing confidentiality.

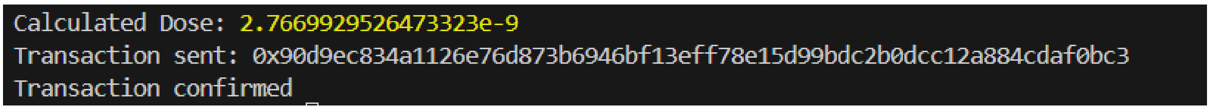
An Ethereum-like blockchain [20] and Ganache [21] test environment, which is free and convenient for testing, were chosen to interact with the smart contract. The results of the successful recording by calling *PatientUpdated()* function of the some arbitrary patient's personal data and the dose of chemotherapy drug encrypted using the Paillier scheme are shown in the Figure 1.



```
CONTRACT NAME                                   CONTRACT ADDRESS
PatientChemotherapy                             0×2c3EDF60C7f3DA9F806D01D8B0744F5Fb3d73076

SIGNATURE (DECODED)
PatientUpdated(hashedId: bytes32, height: uint256, weight: uint256, chemotherapySessions: uint256)

TX HASH                                                              LOG INDEX   BLOCK TIME
0×90d9ec834a1126e76d873b6946bf13eff78e15d99bdc2b0dcc12a884cdaf0bc3   0           2024-09-29 11:26:02

RETURN VALUES

HASHEDID
0×1c2e85187b2a9dc6f085b80c0e5307d64e99c71b764f6609390c9853c7a2c761

HEIGHT
175

WEIGHT
70

CHEMOTHERAPYSESSIONS
3
```

Figure 1: The example of the successful recording of the patient's personal data.

As it can be seen from the Figure 1 the initial data (height, weight, chemotherapy sessions number) for the patient was successfully recorded by the smart contract stored in blockchain. The next step is to calculate the dose of the chemotherapy, using the data retrieved from the smart contract according to the respective methodology (see subsection 2.3). The result of the successful calculating the dose of the chemotherapy drug is shown in the Figure 2.



```
Calculated Dose: 2.7669929526473323e-9
Transaction sent: 0x90d9ec834a1126e76d873b6946bf13eff78e15d99bdc2b0dcc12a884cdaf0bc3
Transaction confirmed
```

Figure 2: The example of the successful calculating the dose of chemotherapy drug.

After the chemotherapy session the chemotherapy sessions number must be updated, i. e. incremented. In order to perform so due to utilization of homomorphic encryption scheme there is no need in decrypting the current number of sessions. Instead the software encrypt the value "1" and adds it to the encrypted value of currently stored number of sessions (3 for the instance). Thus without decryption and even without disclosing to the nurse or IT department staff the current value of chemotherapy sessions their value had been updated. The other parameters can be updated in the similar way.

Thus the method is implemented. The feature of programmable smart contract of the Ethereum-like blockchains allowed to develop along side of the data structures algorithms of processing the data on the side of blockchain such as data updating in the homomorphically encrypted form.

7. Discussion

Patients' data protection has the strict regulation from the governments and increased attention from the society [1, 2, 3]. This is explained by both criticality of the medical infrastructure and huge amount of personal data being processed at this area. While the need of data privacy protection in this area is obvious, needs of its integrity, availability and traceability are important as well. The latter parameters are important due to lethal consequences of improper data processing and the data can be used at the legal area such as court proceedings. The research is performed for the instance of cancer patients' data who are internal refugees in Ukraine at the warfare circumstances, when documents along with a server running database containing patients' data might be destroyed causing data loss, which is crucial for the treatment process. The latter proves the need of patients' data protection improvement.

Known works on the topic of the homomorphic encryption usage for the medical data protection utilize it for the large data arrays [14, 17], that impact productivity due to computationally demanding transformations used by the encryption process. This negatively impact data availability and capacity of servers used for the data storing to handle simultaneously several user requests. Moreover data presented in encrypted form for such algorithms are several times larger than the original before the encryption one.

These homomorphic encryption properties create constrains for its application at the healthcare field, which are not properly addressed. Firstly, only data that is supposed to be used at computations should be protected by this type of encryption. Secondly, designated storage medium should possess enhanced availability properties in order to compensate the above-mentioned drawback. To meet the former constraint the implementation area is to be analyzed and the data is to be determined. The latter constraint leads to the utilization of the distributed storage such as clouds and blockchains. Due to security compliance considerations clouds seem to be less desirable due to the cloud provider trust legal regulations. Therefore a blockchain was chosen as a data storage medium that allowed to meet the requirement and additionally provide increased integrity and traceability protection comparatively with known approaches based on the server file storages, databases or clouds [15, 16, 18, 19].

Performed analysis of the Ewing's sarcoma treatment methodology allowed us to determine, that partially homomorphic encryption, which is computationally less demanding and have less impact on data size increasing after the encryption, is enough for the case, because data updating needs can be satisfied only be the additive operations. That's why Paillier scheme, which provides fully homomorphic addition, but partially homomorphic multiplication, was chosen for the research.

Presented task formalization allowed us to identify the task parameters and restrictions, in particular the data set, that is to be protected by the homomorphic encryption. The latter allowed to develop a method on the basis of them. Mathematical description of the task can be used in the further research in the area of medical data protection.

We proposed a method for data protection on the basis of homomorphic encryption and distributed storage, namely Ethereum-like blockchain. Due to homomorphism property of the encryption the data can be processed and updated in the encrypted form, which allowed to negate the drawback of blockchain's openness and a lack of mechanisms for data privacy protection. The very blockchain's openness and data distribution via multiple nodes provides increased protection of integrity, availability and traceability to the method. Proposed method and its processed were formalized. In order to reach proof-of-concept we presented results of software, which implements the method, those allowed to prove its efficiency. However due to the utilization of partially homomorphic encryption scheme proposed method have limitations for the possible data processing operations, those can be performed in encrypted form without compromising patients' personal data.

That's why in order to scale the method for other patients data protection instances it should be prior adapted to new case's data processing requirements. The latter may lead to the necessity of encryption method substitution by other partially homomorphic or by fully homomorphic ones.

However, several tasks are yet to be solved before the method could be integrated to the medical practice. In particular the task of key sharing, their certification and distribution. We anticipate utilizing of electronic systems of healthcare such as eHealth system in Ukraine [22] and integration of key sharing protocols to the system. The task is to be addressed in our future research. Nevertheless, proposed method reaches its goals and meets restrictions of the task.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Law of Ukraine "Law on the protection of personal data" of 01.06.2010 no. 2297-VI : as of 27 April 2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

[2] Hjerppe, K., Ruohonen, J., & Leppanen, V. The General Data Protection Regulation: Requirements, architectures, and constraints. In Proceedings of the 2019 IEEE 27th International Requirements Engineering Conference (RE). (2019). doi: 10.1109/re.2019.00036.

[3] U.S. Department of Health and Human Services. (1996). Health Insurance Portability and Accountability Act (HIPAA). URL: https://www.hhs.gov/hipaa/index.html.

[4] M. Ogburn, C. Turner, P. Dahal. Homomorphic Encryption. Procedia Computer Science. 2013. Vol. 20. pp. 502–509. doi: 10.1016/j.procs.2013.09.310.

[5] Ç. K. Koç, F. Özdemir, Özger Z. Ödemiş. Paillier Algorithm. Partially Homomorphic Encryption. Cham, 2021. pp. 95–105. doi: 10.1007/978-3-030-87629-69.

[6] P. Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. Advances in Cryptology – EUROCRYPT '99. Berlin, Heidelberg. pp. 223–238. doi: 10.1007/3-540-48910-x_16.

[7] F. Wibawa. BFV-Based Homomorphic Encryption for Privacy-Preserving CNN Models. Cryptography. 2022. Vol. 6, no. 3. P. 34. doi: 10.3390/cryptography6030034.

[8] J. H. Cheon. Homomorphic Encryption for Arithmetic of Approximate Numbers. Advances in Cryptology – ASIACRYPT 2017. Cham, 2017. pp. 409–437. doi: 10.1007/978-3-319-70694-8_15.

[9] R. Geelen, F. Vercauteren. Fully Homomorphic Encryption for Cyclotomic Prime Moduli. 2024. 32 p. URL: https://eprint.iacr.org/2024/1587.

[10] Body Surface Area. URL: https://www.ncbi.nlm.nih.gov/books/NBK559005/.

[11] T. Kouno. Standardization of the Body Surface Area (BSA) Formula to Calculate the Dose of Anticancer Agents in Japan. Japanese Journal of Clinical Oncology. 2003. Vol. 33, no. 6. pp. 309–313. doi:10.1093/jjco/hyg062.

[12] R. Mosteller. Simplified Calculation of Body-Surface Area. N Engl J Med. 1987;317(17):1098. doi:10.1056/NEJM198710223171717.

[13] MedCo | Collective protection of medical data. URL: https://medco-ch.github.io/index.html.

[14] Homomorphic encryption in healthcare. URL: https://www.inno-boost.com/blog/homomorphic-encryption-in-healthcare/.

[15] S. Adhikary, S. Dutta, A. D. Dwivedi. Secret Learning for Lung Cancer Diagnosis - A Study with Homomorphic Encryption, Texture Analysis and Deep Learning. Biomedical Physics & Engineering Express. 2023. doi: 10.1088/2057-1976/ad0b4b.

[16] A. Malik. Confidential and Protected Disease Classifier using Fully Homomorphic Encryption. 2024 IEEE Conference on Artificial Intelligence (CAI), Singapore, Singapore, 25–27 June 2024. 2024. doi: 10.1109/cai59869.2024.00074.

[17] K. Munjal, R. Bhatia. A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex & Intelligent Systems. 2022. Doi: 10.1007/s40747-022-00756-z.

[18] J. W. Bos, K. Lauter, M. Naehrig. Private predictive analysis on encrypted medical data. Journal of Biomedical Informatics. 2014. Vol. 50. pp. 234–243. doi: 10.1016/j.jbi.2014.04.003.

[19] A. M. Vengadapurvaja. An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security. Procedia Computer Science. 2017. Vol. 115. pp. 643–650. doi: 10.1016/j.procs.2017.09.150.

[20] Ethereum. URL: https://ethereum.github.io/yellowpaper/paper.pdf.

[21] Ganache. URL: https://archive.trufflesuite.com/ganache/.

[22] eHealth. URL: https://ehealth.gov.ua/.