Ensuring Confidentiality of Information When Processing Operational Production Plans in Cloud Services

Radda A. Iureva[1], Sergey V. Taranov[1,2], Alexander V. Penskoi[1] and Artem S. Kremlev[1]
[1] *ITMO University, Saint Petersburg, Russian Federation*
[2] *SPbETU "LETI", Saint Petersburg, Russian Federation*

Keywords: Confidentiality, Cloud Services, Operational Plans, Data Anonymization, Homomorphic Encryption.

Abstract: This paper proposes two methods for ensuring the confidentiality of information transmitted to cloud services when processing the operational production schedule. The first method consists of the consistent classification of critical information and the depersonalization of symbolic parameters, which may be personal or commercial secret, concerning the type of anonymized data. The second method, as an additional gain, involves homomorphic encryption of numerical parameters.For each of the proposed methods, the disadvantages and advantages of its use and implementation are described.

1 INTRODUCTION

According to a study by the InfoWatch Analytical Center, in 2018, there were 70 confidential data leaks through cloud servers and other insecure information storages with Internet access. 28.2% of incidents in the area of sensitive data leakage occurred in the cloud, with more than 40% of them from storage facilities owned by high-tech companies (Figure 1). For example, in August 2019, the personal data of almost 90 thousand customers of the Mastercard payment system in Germany was discovered on the Web. Such kind of information can be used for phishing mailings.

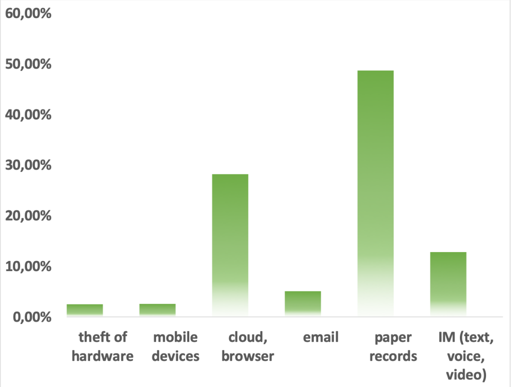

Figure 1: Distribution of fraudulent data incidents by channel.

The use of cloud computing extends the scope of information security tasks (Park and Tran, 2015) to protect resources, trade secrets, personal data, and other user data (Figure 2).

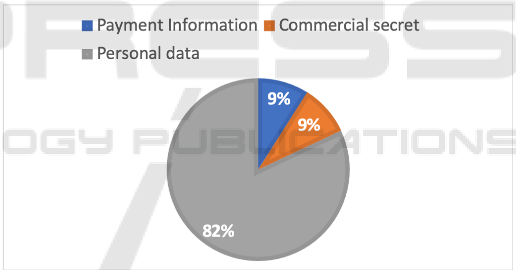

Figure 2: Distribution of leaks from cloud servers by data type.

When using cloud computing to generate an operational production schedule, the know-how of the enterprise, building plans, logistics flow charts, as well as personal data of employees are used. These data are sensitive, as its loss may result in material and reputational damage. As part of this study, anonymization and data encryption procedures are considered to protect the confidentiality of this information. The security of using a cloud service is described as follows:

$$CS = (C_{imp}), (I_{imp}), (A_{imp}), \qquad (1)$$

Where index $impact = \{low, moderate, high\}$., C means Confidentiality, I means integrity and A is for availability.

The Security of Cloud Computing based on fully Homomorphic Encryption is a rather new concept of information security, so there are not so many re-

Iureva, R., Taranov, S., Penskoi, A. and Kremlev, A.
Ensuring Confidentiality of Information When Processing Operational Production Plans in Cloud Services.
DOI: 10.5220/0009873201670173
In *Proceedings of the 17th International Conference on Informatics in Control, Automation and Robotics (ICINCO 2020)*, pages 167-173
ISBN: 978-989-758-442-8

searchers on ot. In (Singh et al., 2019) is made a review on this field of science and described common advantages of using homomorphic encryption, as it is enable to provide the results of calculations on encrypted data without knowing the raw entries on which the calculation was carried out respecting the commercial secrets. In (Kavitha and Harsoor, 2018), (Murthy and Kavitha, 2019) is made a review and an analysis of The Security of Cloud Computing based on fully Homomorphic Encryption to exhibit various applications of in the real world. It is stressed also that the system must work efficiently without compromising the required cloud security services. The paper (Priya and Sumitha, 2018) provides another analysis with comparison of performance on encryption algorithms. The authors made a conclusion that Paillier and Elgamal algorithms are considered to be the most efficient when it comes in terms of security

The purpose of this study is to increase privacy security.

2 FORMATION OF REQUIREMENTS FOR METHODS OF ENSURING CONFIDENTIALITY WHEN PROCESSING PRODUCTION SCHEDULE IN CLOUD SERVICES

Consider the types of interaction, possible threats, distribution of powers, and data flows between entities (information owner and cloud service) to formulate requirements for methods of ensuring confidentiality. Figure 3 shows the permissions for the cloud user and information owner.

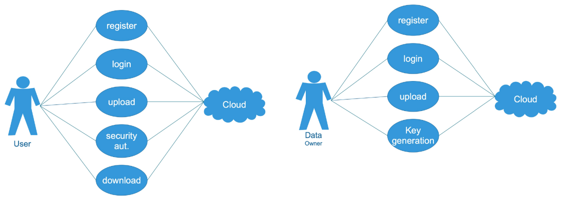

Figure 3: Powers of the owner of the information and user of the service.

It is considered to be non-disclosure to third parties in the process of cloud computing when planning the assembly process of linear drives. To conduct a vulnerability analysis of the system under study, a use case diagram of the service user is constructed (Figure 4).

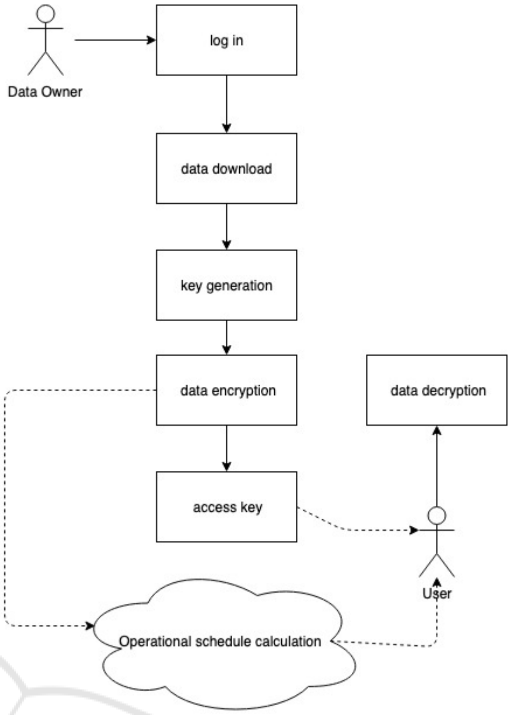

Figure 4: Use Case diagram for service user.

When using a cloud service and ensuring the confidentiality of data processed in the cloud, it must be borne in mind that the cloud client must be able to synchronize files in blocks and be able to quickly access any data on the cloud to update or decrypt it without the need to transfer large amounts of "left" data. The Figure 5 shows the data flow when they are uploaded to the cloud for computing the operational production plan. There are two types of cloud service usage:

1. The information owner independently encrypts the data (Figure 5), the key is stored in the information owner's database, sensitive data is transmitted in encrypted form to the cloud. **Advantages:** Confidential information is not transmitted to the cloud in an open or even anonymous form. **Disadvantages:** When synchronizing and updating information, it is necessary to re-encrypt huge data sets on the side of the information owner. Moreover, when encrypting with non-homomorphic cryptographic algorithms, operations on numerical parameters will be completely impossible.
2. The owner of the information fully trusts the owner of the cloud service and transfers the data to the representatives of the service for calculating the operational plan in the clear. **Advantages:** Cloud services process open information most ef-

ficiently without the need for pre-processing. Information can be quickly updated by the owner of the information **Disadvantages:** There is no protection against malicious exposure from the cloud service

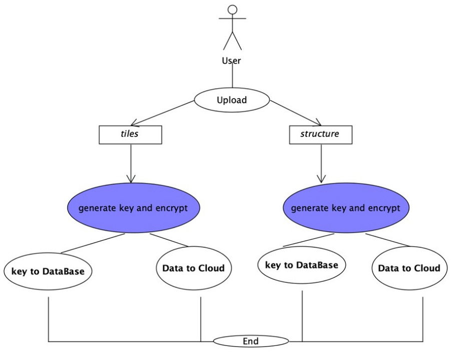

Figure 5: Data flow in the process of download data on Cloud.

The main problem of encryption in data centers is that suppliers store keys to user data so that the cloud service administrator can see all the data related to personal information and commercial secrets at any time. Thus, customers of the cloud service have to overpower themselves and show trust because their data is not fully protected. The methods proposed in this paper are going to solve this problem.

When creating distributed applications, it is advisable to visualize the network infrastructure of the software system. The use of cloud computing power determines the need to address issues related to the security and stability of access to information of corporate clients. Thus, the general configuration and topology of the software system, containing the image of the placement of components on individual nodes of the network, are presented in the Figure 6. It also offers information transfer routes between devices that are involved in calculating the operational production plan of a distributed enterprise.

Based on the above requirements for the organization of flows and interaction of entities, it is recommended to follow the next sequence of operations, presented in Figure 7, to ensure the confidentiality of information transmitted by the information owner to the cloud for the implementation of the production plan generation process.

The main structural element of the interaction scheme between the information owner and the cloud service shown in Figure 7 is the projective transformation, which for the most part, rests with the task of ensuring the confidentiality of information. The methods underlying this protective conversion are described in the next section of the paper.

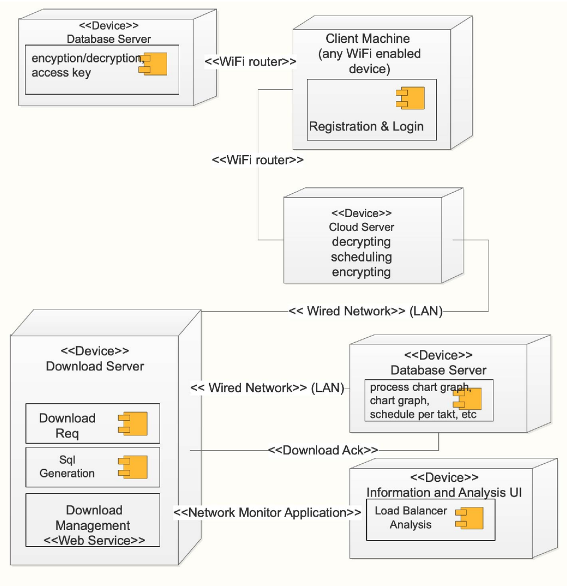

Figure 6: Deployment Diagram of Operating Scheduling.

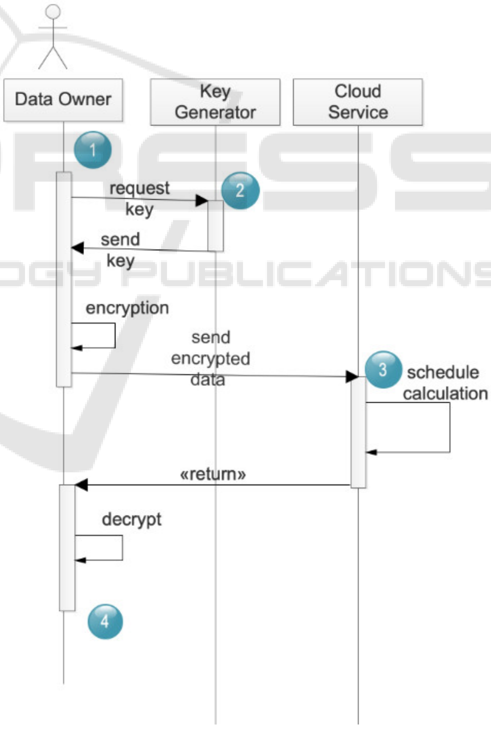

Figure 7: The sequence diagram of operations when calculating the operational production schedule using encryption.

3 METHODS FOR ENSURING CONFIDENTIALITY OF INFORMATION FROM TECHNOLOGICAL MAPS DURING PROCESSING IN EXTERNAL CLOUD SERVICES

Before describing the security conversion proposed in the paper, it is worthwhile to clarify the relationship between the described privacy methods and the existing secure connection protocols (SSL/TLS, IPsec, HTTPS). The purposes of ensuring confidentiality proposed in the paper relating to the protocol interaction of the information owner's node and the cloud service at the application level, therefore, the task of providing a secure connection between the cloud and the owner is not considered and it is believed that it is solved at lower levels (network and transport).

To describe the proposed protection method, we consider the simplest example of a technological map, an accompanying enterprise database, and the process of downloading information from an enterprise database to an external cloud to optimize critical parameters of an operational production plan. The table 1 presents the simplest example of a flow chart for manufacturing a metal part.

Table 1: Example of operational plan.

Number	Sequence
1	Select a workpiece for processing
2	Mark the workpiece in length
3	Cut the workpiece along the marking lines
4	...
...	...

Based on technological maps, enterprises form technological processes that involve the necessary personnel, equipment, and additional tools to create the materials indicated in the technological maps. The most straightforward database accompanying the flow chart may can consist of attributes with following clarifying information:

1. number of specialists in the enterprise;
2. required number of workpieces;
3. labor costs;
4. number of workbenches.

In the corporate database, information from technological maps is concertized, the necessary capacities for creating the product are compared with the current resources of the enterprise. An urgent task for an enterprise with continually changing external (interaction with suppliers, equipment and materials, prices, logistics, production calendar) and internal (availability of certain personnel and specialists) conditions is the selection of the optimal ratio of critical parameters (labor costs, time of employment of personnel and equipment consumed resources, etc.) in order to improve the quality or quantity of products. When assessing volumetric flow charts and taking into account a wide range of critical parameters, the task of selecting the optimal ratio becomes computationally complex and, accordingly, intractable within a particular enterprise. In this regard, a frequent practice at present is the transfer of the procedure for selecting the optimal ratio of critical parameters to external public cloud services (Margun et al., 2017). Despite the fact that the protection of confidentiality from external intruders and third parties is solved at the TLS/SSL protocol level, the actual threat of confidentiality violation is the threat of access by unscrupulous administrators and cloud owners to customer data stored and processed in the cloud. The obvious and primary problem when transferring information on limited-access outside the enterprise is the preservation of its confidentiality.

Consider the approach to finding the optimal key parameters by solving the system of inequalities. This approach is used, in particular, in the preparation of information for generating a production plan. For example, in a routing, there are two consecutive steps A and B, in each of which two different specialists are involved, the labor of which is required to complete the corresponding steps as d_A and d_B. Specialists cannot replace each other, and parallelization of A and B operations cannot be performed. Under such conditions, the task of optimizing labor costs for the enterprise will be the solution to the following inequality systems:

$$\begin{cases} A_2 = A_1 + d_A; \\ B_2 = B_1 + d_B; \\ A_2 <= B_1. \end{cases} \tag{2}$$

The last inequality is necessary to accurately determine the sequence of operations. This paper assumes that the cloud assumes the function of finding the optimal parameters by solving systems of inequalities similar to 2.

For the methods of ensuring confidentiality proposed in this paper, preliminary data processing is required, which ranks the information to the one that will participate in the calculations (structure or numerical data), and the one that does not directly participate in the estimates (tiles or character data). Character data includes not only explicitly defined confidential information but also, for example, variables for optimizing production plan parameters.

The first method proposed in this paper to ensure the confidentiality of information downloaded from technological maps is to depersonalize key parameters when transferring data to an external cloud service. The following approach is proposed when processing information before moving it to the cloud, which consists of two successive stages: depersonalizing parameters (the depersonalization method must be utterly reversible for the information owner and preserving the data structure) and marking the data types necessary for performing operations by the cloud service. The most simple way of depersonalizing data is the method of introducing identifiers. This approach provides for the replacement of critical information from a security point of view with a random set of generated identifiers.

In the enterprise database, replacement tables are additionally generated, the purpose of which is to depersonalize the data transmitted to the cloud. For example, to solve the system of inequalities 2, the following additional attributes can be entered in the enterprise database - Tables 2 and 3.

Table 2: Example of the substitutional table to character parameters.

Number	Sequence	Notion	Forwarded data
1	Select a workpiece for processing	A_1	5DCBD2
2	Mark the workpiece in length	A_2	6EB3BE
3	Cut the workpiece along the marking lines	B_1	1A0623
4	Finish making workpiece	B_2	2645B2

Table 3: Example of the substitutional table to numeric data.

Position	Notion	labor costs	unit	type identification
Locksmith	d_A	20	man hours	557C86
Turner	d_B	10	man hours	5F0228

In the event that replacement tables are formed on the client-side, as shown in Figure 2, only the last attribute from the substitution table 2 and the second and previous attribute from the substitution table 3 are transferred to the external cloud service. As a result, the cloud service receives the following inequality to solve:

$$\begin{cases} 6EB3BE = 5DCBD2 + 20; \\ 2645B2 = 1A0623 + 10; \\ 6EB3BE <= 1A0623. \end{cases} \tag{3}$$

That is, the information transmitted to the cloud server contains exclusively anonymized data (anon function) and marking for data types, as shown in Table 4.

Table 4: Example of data format forwarded to cloud service.

Formulation of the problem	Description of data types
anon(Sequence of manufactoring steps)	Invariable
anon(Specialists and labor)	Invariable
Only numerical data with the number of needed workpieces	integer allowed range
Number of specialists with specific qualification	Integer exact value

It is worth noting that to increase the resistance to correlation attacks, the method of anonymization based on identifiers can be complicated and modified, in particular, using other methods of anonymization, for example, the technique of mixing data. In some cases, the depersonalization method can be replaced by the full encryption of individual variable blocks (encryption must be performed in electronic codebook mode so that the same variables in the cloud have the same ciphertext values). Encryption can be indispensable if, in the corporate network of the enterprise for sending tasks and processing the results received from the cloud, individual network nodes, for example, located in different branches of the enterprise, are responsible.

Even though most of the data is encrypted/anonymized, cloud services have all the necessary information to solve the system of inequalities. The last attribute of the substitution Table 3 allows you to determine whether absolute numerical values (20 and 10 in our specific example) have the same units of measurement and whether operations are allowed on them. Since when depersonalizing/encrypting the same values with restrictions in the proposed method, the same ciphertexts are obtained, the cloud service can perform ranking and ordering of variables based on inequalities additionally introduced into the system.

The obvious **advantages** of the first method is the simplicity of its implementation, we need to modify the data structure used in the enterprise by adding replacement tables and identifier arrays to mark variables and units of measure. Another advantage is that in a cloud service, based on the ranges of values defined by the client, parallelization can be performed on computing stations. When transmitting information to the cloud, the owner of the information converts the blocks of data independently of each other, so each block can be changed on the owner's side and re-sent to the cloud. **Disadvantage** of the proposed method is that we transmit in an open form (for the cloud owner) numerical values to an external cloud service. Numeric values can be used by cybercriminals (dishonest cloud server administrators) to recover partial or complete information about the internal business processes of an enterprise. Also, the owner of the cloud will know the sequence of operations, the allowed ranges of values for the processed parameters, which, in turn, can provide indirect information about confidential client data.

Confidentiality of numerical data can be ensured, provided that partially or fully homomorphic cryptographic algorithms are used for their transmission (Gentry, 2009a; Gentry, 2009b; Rohloff and Cousins, 2014). Thus, the second method of ensuring confidentiality is the use of fully homomorphic encryption for numeric data transmitted to external services. The following modification of the first proposed method is proposed. Each numerical value x from the second attribute of the Replacement Table 3 is assigned a $Enc(x)$ cost encrypted using a fully homomorphic cryptosystem, which is subsequently transferred to the cloud. As an encryption algorithm, this method proposes to use the fully homomorphic cryptosystem L. Jian and D. Song (Li et al., 2012), which is a cryptosystem adapted to ensure confidentiality in the clouds. Let us briefly describe the main stages of encryption of the cryptosystem under consideration:

1. The key k is generated as a random odd number of length l -bit
2. The process of encrypting one bit of the message
$$x_1 \in 0,1$$
is carried out according to the following formula
$$c_n = x_n + k + r * k * q, \tag{4}$$
where r is a random value of D-bit length, q is a constant representing a large integer, n is the serial number of the message bit and ciphertext.
3. To decrypt information on the client side, it is enough to perform the operation:
$$c \ mod \ k \tag{5}$$

The paper (Li et al., 2012) proves the homomorphism of the presented cryptosystem. An additional significant advantage of the presented method is the ability to verify the integrity of data sent to the cloud without decrypting it. In particular, when using the proposed method, the information owner can send encrypted messages to the cloud at some intervals to verify the integrity of numerical data:

$$c_{client} = x_{client} + k + r * k * q \tag{6}$$

The server, in turn, is able, using only the general synchronization parameter q, to verify that the selected clear text bits do match:

$$Integrity = (c_{server} - c_{client}) \ mod \ q \tag{7}$$

If the integrity parameter $integrity$ is equal to zero, then the copy stored on the server matches the sent parameter.

Note that using a homomorphic system, it is proposed to encrypt exclusively numerical data and not information completely transmitted to the server, including the statement of the problem, operating parameters, and identifiers. The encryption process itself, when it is used out of control, will be time-consuming and labour-consuming for the information owner. Therefore, it is proposed to further rank the numerical parameters before sending it to the cloud to determine which disclosure of which carries the greatest risk to the enterprise. And concerning critical numerical parameters, apply the proposed method based on a homomorphic encryption algorithm. **Advantages** As in the first method, the cloud server will be able to perform ordinary actions on numerical data and even, as shown in the paper (Chialva and Doom, 2018), perform comparisons, ranking, dividing parameters into ranges under certain conditions. Using selective encryption, you can achieve an effective balance between the load on the client and the level of information confidentiality. When using the second method, the probability of violating the confidentiality of information is very low. The attacker will only know the sequence of operations, which is almost impossible to correlate with the technological processes of the enterprise.

It is also worth highlighting **drawbacks**, characteristic of the second method, on the client-side, it is necessary to further modify the allowed type and range for numeric and character parameters, because, after encryption, the received value may not satisfy the requirements defined for the initial settings. Modifications may concern, among other things, the statement of the problem as a whole if, as a result of applying the second method, the optimization parameter of the production schedule was encrypted.

4 CONCLUSIONS

The paper raises the urgent problem of ensuring the confidentiality of information when it is processed in cloud services. In this paper, an analysis of information flows between interacting entities was carried out, a model of threats to information privacy violations in solving the problem was constructed.

The paper suggests using a comprehensive method for anonymizing and marking confidential information with the preservation of the data type for subsequent processing as a protective transformation for data transferred to cloud services. As a second method, it is proposed to strengthen the original algorithm for the protective transformation using schemes of homomorphic encryption of numerical data. For each of the proposed methods, the disadvantages and advantages of its use and implementation are described.

ACKNOWLEDGEMENTS

This work was financially supported by Government of Russian Federation (Grant 08-08) and by the Ministry of Science and Higher Education of Russian Federation, passport of goszadanie no. 2019-0898. Section three funding was provided by Russian Science Foundation (RU) (Grant No. 19-19-00566).

REFERENCES

Santosh kumar Singh, Pankaj Manjhi, Dr. V.R Vadi (2019). Homomorphic. Encryption in Cloud Computing Security, Conference

C. R. Kavitha, B. Harsoor A survey on Homomorphic encryption in cloud security, January 2018

Shrujana Murthy, Kavitha C.R. Preserving Data Privacy in Cloud using Homomorphic Encryption, Conference: 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), June 2019 DOI: 10.1109/ICECA.2019.8822127

Changigarh S Manju Priya, J. Sumitha. Comparative Analysis of Homomorphic Encryption in Cloud Computing. Conference: 4th International Conference On Science,Technology And Management, December 2018

Data in the clouds: leaks through unprotected servers increased by 43%, https://www.infowatch.ru/company/presscenter/news/15559, 2019 (accessed 22.10.19)

Future Factory: How Technology Is Transforming Manufacturing:Resource Planning and Sourcing/Operations Technology Monitoring and Machine Data, http://cresprit.com/en/2019/04/05/future-factory-how-technology-is-transforming-manufacturing2resource-planning-sourcing-operations-technology-monitoring-machine-data/, 2019 (accessed 22.10.19)

Hong-Seok Park, N.-H. Tran, Development of a cloud based smart manufacturing system, Journal of Advanced Mechanical Design Systems and Manufacturing 9(3), July 2015

Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019, https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g, 2019 (accessed 22.10.19)

J. Li, D. Song, S. Chen and X. Lu (2012). A simple fully homomorphic encryption scheme available in cloud computing, 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, Hangzhou, pp. 214-217

C. Gentry (2009). A fully homomorphic encryption scheme, PhD thesis, Stanford University, crypto.stanford.edu/craig.

C. Gentry (2019). Fully homomorphic encryption using ideal lattices, Proceedings of the 41st Annual ACM Symposium on Theory of Computing, pp. 169–178

K. Rohloff and D. B. Cousins (2014). A scalable implementation of fully homomorphic encryption built on NTRU, Financial Cryptography and Data Security Workshops, V. 8438 , pp. 221–234

D. Chialva, A. Dooms (2018). Conditionals in Homomorphic Encryption and Machine Learning Applications, The International Association for Cryptologic Research.

A. A. Margun, A. A. Bobtsov, I. B. Furtat (2017). Algorithm to control linear plants with measurable quantized output, Automation and Remote Control, V. 78, N. 5, pp. 826-835