TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 66, Issue IV, November, 2023

DIGITAL SECURITY SYSTEM WITH ARTIFICIAL INTELLIGENCE MODULE FOR DATA COMMUNICATIONS INTO MANUFACTURING COMPANY

Adrian VÎLCU, Dumitrel TODIRICĂ, Ionuț-Viorel HERGHILIGIU, Ion VERZEA

Abstract: *Security systems in the real economy have been adapted for online communication activities, addressing their specificities: remote connections, electronic signatures, data encryption, database security, and customer confidentiality. This research encompasses the design and implementation of an online security system for data communication related to quality and production indicators within a textile company, along with the functional optimization of this system through an analysis of satisfaction levels for its primary functions. The process of reimagining this service is presented through an incremental innovation analysis based on the value engineering method. The methodological research proposes solutions for the functional optimization of the data transfer security system by redefining its functions and, ultimately, applying and implementing these solutions in an enhanced security system with added value.*
Key words*: digital security system, AI module, functional optimization, value engineering method*

1. INTRODUCTION

The rapid evolution of information and communication technology in recent years has led to a significant increase in the volume of transactions carried out through online platforms, which is the main reason why it is necessary to analyze the implementation of security mechanisms in this domain. This evolution has brought significant benefits to consumers and businesses in various industries, offering convenient, accessible, and fast buying and selling opportunities for most products and services used in everyday life and beyond or in safe data transfer within the computer environment. However, the number of threats, fraud attempts, and cyber attacks has continued to rise, highlighting the need to research and develop new methods to protect both businesses and personal transfer data.

Furthermore, in the context of the COVID-19 pandemic, data transfer has exponentially increased [1] as users have been compelled, to a greater or lesser extent, to resort to this method for efficient communication, especially in the business environment [2]. This growth puts even more pressure on the development of new means or, at the very least, the implementation of the most efficient security mechanisms for data transfer between the production systems of directly productive economic units and the systems for analyzing proper functioning, which are often located outside the industrial unit. These production process data are confidential and must be secured through special encryption mechanisms.

An efficiently designed cyber security system for data transfer may be structured based on the following modules (Figure 1).

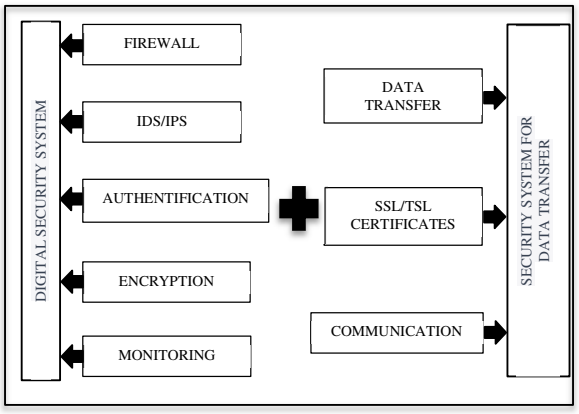

Fig. 1. Modules of a digital security service for data transfer.

Received: 16.08.23; **Similarities**: 04.08.23: **Reviewed**: 24.10./20.10.23: **Accepted**:27.11.23.

The basic modules of a digital security system are:

- Firewall [3]: A software, hardware, and network service that monitors and filters traffic within the internal network and external access to the protected system. It analyzes data packets passing through the protected network and, based on security policies, allows or blocks their transit. Filtering can be based on IP addresses, ports, or security protocols, which include access restrictions and authentication policies. The firewall can detect and block cyber attacks such as Denial-of-Service (DoS) attacks or intrusion attempts.
- Intrusion Detection and Prevention Systems (IDS/IPS) [4]: These services monitor network activity and block malicious activities. The IDS detects suspicious activity, while the IPS intervenes to block attacks in real time. IDS/IPS modules search for patterns (known attack signatures) indicating unauthorized activities or suspicious behaviour (unusual traffic patterns).
- Authentication and [5]: Authentication is the process of verifying the identity of a user attempting to access a system or resource. This process relies on authentication factors such as username and password and multi-factor authentication (MFA): MFA involves using at least two different authentication factors, such as a password, verification codes via SMS or authentication apps, fingerprints, facial recognition, or hardware tokens. This increases the security level by requiring an attacker to obtain access to more than one authentication method. Two-factor authentication (2FA): 2FA is a common form of MFA that involves using two authentication factors, usually a password and a unique verification code sent via SMS, authentication apps, or other means. Authorization is when an authenticated user is granted specific permissions and rights to access and use system resources and functionalities. It is based on defined security policies and rules determining which actions and resources are allowed or restricted for each user or user group. Authorization is usually performed based on assigned roles and privileges to the authenticated user.
- Encryption [6]: Encryption is an essential component of cybersecurity and aims to protect information by transforming it into an unreadable format for unauthorized individuals. The encryption system uses mathematical algorithms and cryptographic keys to convert data into an encrypted form, also known as ciphertext. This provides confidentiality and ensures that only the legitimate recipient can read and interpret the information.
- Monitoring and Logging [7]: Monitoring refers to the continuous surveillance of system, network, and application activities to identify any suspicious activity, unusual behaviour, or violations of security policies. The purpose of monitoring is to detect and respond rapidly to cyber threats such as attacks, intrusions, or abnormal user behaviour. Logging refers to recording and documenting system and network events and activities in a log or log database. Logs contain information about events such as authentication, resource access, configuration changes, errors, alarms, and other significant activities.
- Backup and Data Recovery Systems [8]: These systems ensure the creation of backup copies of data and systems, as well as the ability to restore them in the event of a security incident or catastrophic event.

In addition to the aforementioned cybersecurity services, data communication servers also include the modules:

- Secure data transfer protocols [9] [10]: The use of secure protocols such as HTTPS (HTTP Secure) ensures data encryption during transmission between the client's system and the data server. This prevents unauthorized interception and modification of information.
- SSL/TLS Certificates [11]: Using an SSL/TLS certificate authenticates the server's identity and encrypts communication between the client and server, ensuring the confidentiality and integrity of transferred data.

- Communication with customers [12][13] Maintains secure communication with customers regarding security policies.

This research focuses on assessing the level of protection of a database for a textile manufacturing company and its security mechanisms in the data transfer for production indicator analysis, using a sample of 127 customers and suppliers, with the primary goal of identifying vulnerabilities and potential improvements that can be made to the data communication system. The study's methodology includes an incremental innovation method based on value engineering, which results in redesigning the security system based on customer satisfaction with the digital service (Figure 2).

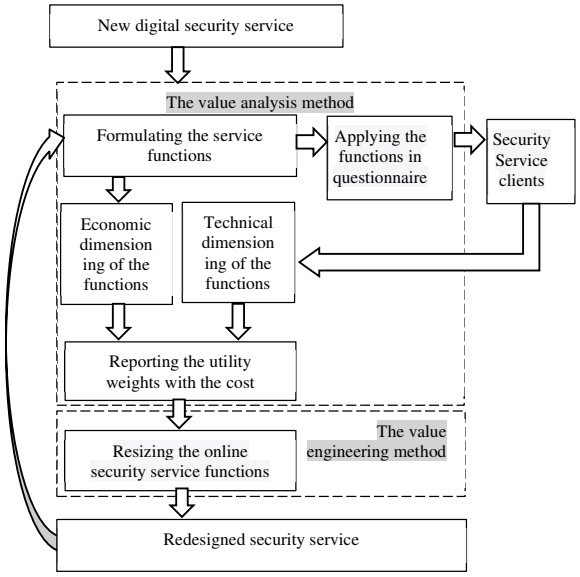

Fig. 2. Iterative algorithm based on value engineering

The principle of the performance incrementation method for the digital security system in data communications is to balance the ratio between the weights of functions in the overall utility of the system and the weights in costs for each function in the total service cost. Suppose the cost per unit of utility is greater than one. In this case, the function is oversized, meaning that more is being paid for the function than an average security system user would pay. Suppose the ratio between a function's cost per unit and the utility per unit is less than one. In this case, the function needs to be more organized, indicating that the customer's need for that function is greater than what is being paid for it. Suppose the ratio of cost weight to utility weight for a function is equal to one. In this case, the function is considered appropriately sized, with the user's projected need for the function aligning with the cost of the function in the total service cost.

2. REDESIGNING THE SECURITY SYSTEM

2.1. Data transfer security system - Design Features

During the development of security system for data communication from production indicators (figure 3), several security methods have been implemented to protect the platform and its users.

Our security system provides a tool specifically designed for collectors called the Library Boosting Tool, which utilizes the client's profile to filter through thousands of data in just a few seconds.

Furthermore, for client interested in other categories of products, there is a section called Packages, where multiple data packages have been created to filter specific types of indicators.

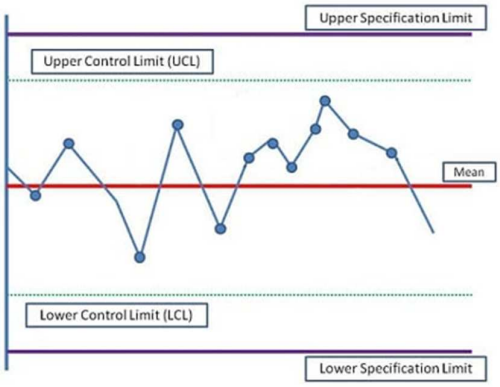

Fig. 3. Quality indicator and its limits

In developing the system, the Laravel framework based on PHP was used. jQuery, a JavaScript library that simplifies the manipulation of elements and functions provided by JavaScript, was also utilized.

MariaDB, a database management system based on MySQL, was used for database management. Several methods were employed to integrate security within the security system. These include using the Cloudflare service, user authentication through two-factor authentication, monitoring user activity through an administrative dashboard and autonomous functionalities, implementing a server firewall, rigorous testing of existing systems, and other methods.

We have implemented data encryption using the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocol to protect data in transit between users and our server. This protocol encrypts communication between the client and server, ensuring that information is protected against unauthorized interception and modification.

We perform periodic backups of data to ensure that we can recover information in the event of unexpected incidents, such as hardware failures or cyber-attacks. Additionally, we constantly monitor and analyze the activity of our systems to quickly detect and respond to any incidents or suspicious behaviour.

After conducting a check using the Google application to verify the status and transparency of the communication, it was found that the current status reported by Google is "No unsafe content found" (Figure 4).

Fig. 4. Google report.

2.2. Designing the functions of the security system

We have designed the main features of the security service into seven functions (Table 1), the satisfaction level of which will be evaluated by users of this service.

Table 1

Functions of the security system.

No	Function Name	Explanation
F1	Service availability	This function is necessary to ensure users with constant availability of the security system and that it is not affected by attacks or technical malfunctions.
F2	Communication	This function is mandatory in the electronic buying-selling process.
F3	Data confidentiality	This function guarantees that user data is protected against unauthorized disclosure. This can be achieved through the use of encryption, authentication, and access control.
F4	Data encryption	Data encryption is essential, safeguarding passwords, credit card numbers, and other personal information. This can be achieved by utilizing encryption algorithms.
F5	Data protection	This function ensures protection against unauthorized modifications, data loss, or theft from users. This is possible through backups, version control, and data integrity checks.
F6	Monitoring user activity	This function is essential for detecting suspicious activities, such as unauthorized access attempts or fraudulent transactions.
F7	User identification and authentication	This function is necessary to ensure that only authorized individuals can access sensitive information and accounts.

The sample of respondents consists of 177 clients of the this security system,

The respondents were asked to rate each function on a scale of 1 to 100 based on their level of satisfaction. The response series are analyzed in terms of normality since, in the subsequent quantitative analysis, the parameter value "mean" is used in the technical sizing of the functions (Table 2).

Table 2

K-S Test for Normality of Response Series

Function	Statistic	df	Sig.
F1	0,051	177	0,074
F2	0,052	177	0,067
F3	0,051	177	0,082
F4	0,052	177	0,067
F5	0,053	177	0,062
F6	0,050	177	0,096

F7	0,052	177	0,064

All response series are normally distributed according to the p-values (p-value > 0,05). Therefore, the mean values for each series of values are representative of the level of satisfaction of the respondents regarding the security service (Table 3).

Table 3

Technical Dimensioning.

	F1	F2	F3	F4	F5	F6	F7
sum_j	21376	17838	23536	16771	20151	22112	22879
$mean_j$	77,17	64,40	84,97	60,55	72,75	79,83	82,60
u_w_j[%]	14,8	12,3	16,3	11,6	13,9	15,3	15,8
utility	0,46	0,48	0,53	0,51	0,63	0,53	0,52

- $sum_j = \sum_{i=1}^{177} n_{ij}$, $with\ j = \overline{1,7}$ - the sum of the values for each function separately
- $n_{ij}\ with\ i = \overline{1,177}$, $j = \overline{1,7}$ - the satisfaction level of respondent i for function j
- $mean_j = \frac{\sum_{i=1}^{177} n_{ij}}{177}\ with\ j = \overline{1,7}$ - mean of j function
- $u\_w_j = \frac{\sum_{i=1}^{177} n_{ij}}{\sum_{j=1}^{7}\sum_{i=1}^{177} n_{ij}}\ with\ j = \overline{1,7}$ - the weight of utility j in the total utility of the product
- $utility_j = \frac{(mean_j - \min_i(n_{ji})}{(\max_i(n_{ji}) - \min_i(n_{ji}))}\ with\ j = 1 \dots 7$ - utility of j function

The satisfaction level of respondents regarding the designed security service is 74.61%, a value that is intended to be increased (especially considering that a cybersecurity service is being evaluated).

The software modules of the digital security system are:

- M1: User Identification and Authentication Mechanism
- M2: Data Encryption Mechanisms
- M3: Access Control Mechanisms
- M4: Activity Monitoring
- M5: Service Availability Assurance Mechanisms
- M6: Data Protection Mechanisms
- M7: Data Privacy Modules

Table 4

Cost allocation by functions as a percentage (%) of the total cost.

	Allocation of security services by functions as a percentage of the total cost						
	F1	**F2**	**F3**	**F4**	**F5**	**F6**	**F7**
M1	10	10	10	10	10	10	40
M2	10	10	10	40	20	10	0
M3	10	10	5	0	10	25	40
M4	10	10	10	0	10	50	10
M5	15	15	15	10	15	15	15
M6	10	10	10	10	40	10	10
M7	10	10	40	10	10	10	10

The values in Table 4, which represent the weights in the total cost of the security service for each function, are determined by the project manager for the development of the security service and the economist responsible for the financial analysis of this service.

The costs associated with implementing these functions in security system can vary depending on several factors, including the size of the system, the desired level of security, available resources, and the capabilities of the developers of these systems.

However, the following cost estimates can be provided, which can be applied to all digital security systems (Table 5).

Table 5

Share in the costs of service functions and security modules.

No.	**Module /Service**	**Service Cost (Euro)**	**Maintenance Cost (Euro/year)**	**Total Cost (Euro/service) in the first year**	**F1**	**F2**	**F3**	**F4**	**F5**	**F6**	**F7**
1	M1	1200	200	1400	140	140	140	140	140	140	560
2	M2	1500	300	1800	180	180	180	720	360	180	0
3	M3	800	250	1050	105	105	53	0	105	263	420

4	M4	1500	400	1900	190	190	190	0	190	950	190
5	M5	1000	350	1350	203	203	203	135	203	203	203
6	M6	1300	200	1500	75	75	75	75	900	150	150
7	M7	500	100	600	60	60	240	60	60	60	60
Total Cost		7800	1800	9600	952	952	1080	1130	1957	1945	1582
Cost weight [c_w][%]		81,3	18,7	100	9,92	9,92	11,25	11,77	20,39	20,26	16,48

2.3. Systemic Analysis of Functions

This analysis compares the ratio of the utility weights of functions to the total utility of the product with the ratio of the cost weights of functions to the total cost of the security system. Ideally (in a perfect digital security system), this ratio is 1.

Graphically, in the coordinate system (u_w, c_w), the functions of the product, in the optimal case (when the functions are optimally sized), are placed on a line inclined at a 45-degree angle. Over-sized functions (c_w > u_w) are located above the 45-degree line, under-sized functions (c_w < u_w) are located below this line, and correctly sized functions (c_w = u_w) are appropriately sized.

Table 5 contains the utility weight parameters (Table 3) and cost weight parameters of the functions, as well as the mathematical calculation for determining the total deviation value (equation 1).

$$S = \sum_{i=1}^{7}(c\_w_i - a * u\_w_i)^2 \qquad (1)$$

Where $a = arctg\left(\frac{\sum_{i=1}^{7} u\_w_i * c\_w_i}{\sum_{i=1}^{7}(u\_w_i)^2}\right)$

In this case (table 6), the value of the sum of squared deviations S=0.0122 exceeds the threshold of 0,01, leading to the conclusion that the system contains functions that are not well-sized in terms of the utility/cost ratio. The slope angle of the regression line is 44.91 degrees.

The graph of the service functions in the orthogonal frame [u_w, c_w] is presented in Figure 4.

Table 6

Systemic analysis of functions.

	u_w	c_w	$(u\_w)^2$	u_w*c_w	$(c\_w - a*u\_w)^2$
F4	0,1159	0,12	0,0134	0,0136	0,0000
F2	0,1233	0,10	0,0152	0,0122	0,0006
F6	0,1529	0,20	0,0234	0,0310	0,0025
F3	0,1627	0,11	0,0265	0,0183	0,0025
F1	0,1478	0,10	0,0218	0,0147	0,0023
F5	0,1393	0,20	0,0194	0,0284	0,0042
F7	0,1582	0,16	0,0250	0,0261	0,0001
TOTAL	1,00	1,00	0,1447	0,1443	0,0122

The value $a = arctg\left(\frac{0,1443}{0,1447}\right) = 0,997$.

The graph in Figure 4 shows the oversizing of functions F4 – data encryption, F5 – data protection, F6 – user activity monitoring and F7 – user authentication. Functions F4 and F5 contain "unseen" mechanisms behind data transfer, which may not be understood in terms of their role and utility.

However, these security modules are necessary for any security system. Two methods can resize these functions: correctly informing clients about the usefulness of these data security mechanisms or "transferring" some encryption and data protection modules to other security service functions (changing the cost weights matrix on the service functions).

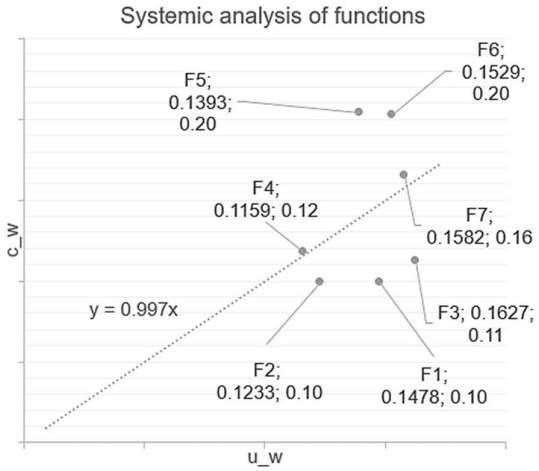

Fig. 4. Representation of function dimensions.

For the resizing of this function, it is possible to use the efficiency of the activity monitoring modules from an economic point of view, by decreasing the cost for their implementation or

by increasing the weight of the utility of this function in the total weight of the service.

For the F2 function (communication with users), an increase in utility is decided by introducing a chat-type communication system with an artificial intelligence module (chatbot).

Another form of synthetic representation of the utility weights of the functions in the total utility and the cost weight in the total cost of the security service is shown in Table 7.

Table 7

Utility and cost weights of security service functions

Indicator	F1	F2	F3	F4	F5	F6	F7
Cost weight [c_w] [%]	9,92	9,92	11,25	11,77	20,39	20,26	16,48
Utility weight [u_w] [%]	14,78	12,33	16,27	11,59	13,93	15,29	15,82
c_w-u_w	-4,85	-2,41	-5,02	0,18	6,46	4,98	0,67

The graph in Figure 5 shows that the only well-sized function from the point of view of the utility weight/cost weight ratio is F4 (data encryption). This highlights that these mechanisms for this function are equally important in utility (clients) and cost (security system designer).

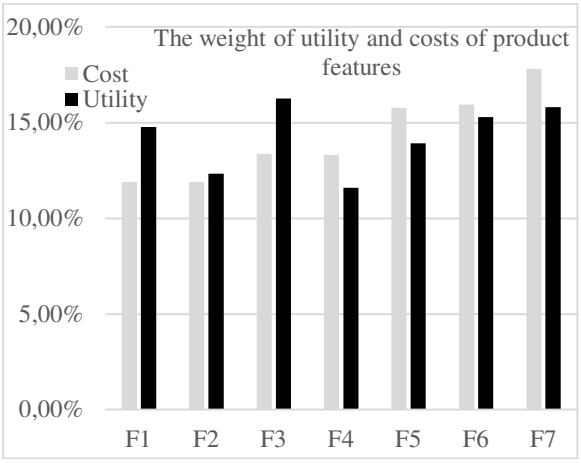

Fig. 5. The utility and cost share of product functions.

2.3. Security service redesigns through functional scaling

Three types of mechanisms are applied for the functional optimization of the digital security system:

- changing the weight of costs on oversized functions (resizing functions F5 - data protection and F6 - monitoring user activity) (table 8);

Table 8

Distribution of cost percentages to functions.

	Allocation of security services to functions as % of the total cost						
	F1	F2	F3	F4	F5	F6	F7
M1	10	10	10	10	10	10	40
M2	10	10	10	40	20	10	0
M3	10	10	5	0	10	25	40
M4	15	15	15	10	10	25	10
M5	15	15	15	10	15	15	15
M6	10	10	10	10	40	10	10
M7	10	10	40	10	10	10	10

- lowering the price of encryption and data protection mechanisms by using basic algorithms (table 9).
- increasing the utility of the communication function (F2) without introducing additional costs by introducing a chatbot with an AI module based on neural networks that contain open-source modules (implementation of a framework using AI development libraries - TensorFlow, PyTorch or Keras).

The percentages from Table 8 represent the distribution of costs for each function within the total cost of the security services.

Table 9

Distribution of costs by functions for the redesigned service.

No.	Module /Service	Service Cost (Euro)	Maintenance Cost (Euro/year)	Total Cost (Euro/service) in the first year	F1	F2	F3	F4	F5	F6	F7
1	M1	1200	200	1400	140	140	140	140	140	140	560
2	M2	1000	300	1300	130	130	130	520	260	130	0
3	M3	800	250	1050	105	105	53	0	105	263	420
4	M4	1500	400	1900	285	285	285	190	190	475	190
5	M5	1000	350	1350	203	203	203	135	203	203	203

6	M6	800	200	1000	100	100	100	100	400	100	100
7	M7	500	100	600	60	60	240	60	60	60	60
Total Cost		6800	1800	8600	1022	1022	1150	1145	1357	1370	1532
Cost weight [c_w][%]		79,07	20,93	100	11,8	11,8	13,37	13,31	15,78	15,93	17,82

The result of the application of the methods of functional optimization of the security service is highlighted in the graph in Figure 6 and Table 10.

Table 10

Systemic analysis of the functions for the redesigned digital security system.

	u_w	c_w	$(u\_w)^2$	u_w*c_w	$(c\_w-a*u\_w)^2$
F4	0,1159	0,13	0,0134	0,0154	0,0003
F2	0,1233	0,12	0,0152	0,0147	0,0000
F6	0,1529	0,16	0,0234	0,0243	0,0001
F3	0,1627	0,13	0,0265	0,0218	0,0008
F1	0,1478	0,118	0,0218	0,0176	0,0008
F5	0,1393	0,16	0,0194	0,0220	0,0004
F7	0,1582	0,18	0,0250	0,0282	0,0004
	1,00	1,00	0,1447	0,1439	0,0028

In this case, the sum of the squares of the deviations is S=0,0028 below the 0,01 threshold, which leads to the conclusion that the system is functionally well-dimensioned from the point of view of the utility/cost ratio.

The regression slope angle is 44.84 degrees, $a = arctg\left(\frac{\sum_{i=1}^{7} u\_w_i * c\_w_i}{\sum_{i=1}^{7} (u\_w_i)^2}\right) = arctg\left(\frac{0,1439}{0,1447}\right) = 0,9946$.

Table 11 compares the initially designed cybersecurity service (S1) and the redesigned service after applying functional analysis (S2). The redesigned service demonstrates improvements in functionality, cost reduction, enhanced data protection, comprehensive user monitoring, enhanced access control, and improved communication capabilities.

Table 11

Comparative analysis of the initially designed and redesigned cybersecurity services.

	F1	F2	F3	F4	F5	F6	F7
S1[%]	-4,85	-2,41	-5,02	0,18	6,46	4,98	0,67
S2[%]	-2,89	-0,44	-2,90	1,72	1,86	0,65	2,00

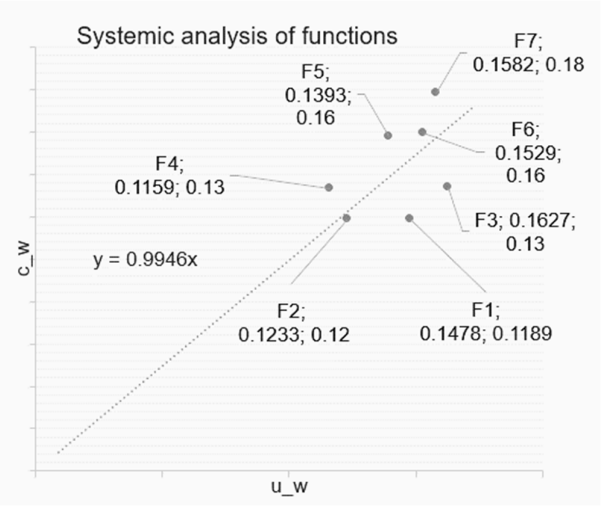

Fig. 6. Representation of the dimensions of the functions of the redesigned system

In Table 11, negative values represent under-dimensioned functions (c_w<u_w), positive values (c_w>u_w) represent over-dimensioned functions, and values very close to 0 indicate well-balanced functions in terms of technical and financial dimensions. Version S2 of the digital security service is balanced across all analyzed functions regarding the utility/cost ratio.

3. CONCLUSION

Through the value engineering analysis, the digital security service underwent a redesign from S1 to S2 and optimization using the incremental innovation method based on value engineering. Focusing on core functions and customer needs decreased the absolute value of function deviation squares in the orthogonal reference [c_w, k_w] for S2 compared to service S1.

Comparing the absolute values of the functions between services S1 and S2, an overall improvement in the absolute value is observed in most functions for service S2.

In service S1, functions F1, F3, and F2 have negative values, while functions F5 and F6 have positive values, indicating strong over-

dimensioning. The optimization mechanism consisting of three solutions was applied, including cost reduction, modification of weights on function design in security modules, and implementation of an autonomous chat system using open-source libraries.

For the redesigned service S2, a significant change in the cost/utility ratio values is observed across all functions. Functions F1, F2, and F3 still remain slightly under-dimensioned (indicating that the cost weight in the total service cost is slightly lower than the utility weight in the service's utility).

The main objective of this work was to apply an incremental innovation methodology based on the value engineering method to a proprietary cybersecurity system. The research addresses the current need for protection in digital transfer data.

4. ACKNOWLEDGEMENTS

This paper was realized with the support of "Institutional development through increasing the innovation, development and research performance of TUIASI – COMPETE 2.0", project - 1183 - funded by contract no. 27PFE /2021, financed by the Romanian government.

This research was also supported by "Gheorghe Asachi" Technical University from Iaşi (TUIASI), through the Project "Performance and excellence in postdoctoral research 2022".

5. REFERENCES

[1] Chevalier, S., *Global retail e-commerce sales 2014-2026. 2022* [Online] Available at: *https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/*[Accessed 01.07.2023].

[2] trade.gov, *Impact of COVID Pandemic on eCommerce. 2022* [Online] Available at: https://www.trade.gov/impact-covid-pandemic-ecommerce [Accessed 1 07 2023].

[3] Anwar, R. W., *Firewall Best Practices for Securing Smart Healthcare*, Applied Sciences, 11(9183), pp. 1-20, 2021.

[4] Krishna, A. et al., *Intrusion Detection and Prevention System Using*, Proceedings of the International Conference on Electronics and Sustainable Communication Systems, pp. 273-278, 2020.

[5] Trnka, M. et al., *Systematic Review of Authentication and Authorization Advancements for the Internet of Things*, Sensors, 22(1361), pp. 1-24, 2022.

[6] Alenezi, M. N., Alabdulrazzaq, H. & Mohammad, N. Q., *Symmetric Encryption Algorithms: Review*, International Journal of Communication Networks and Information Security, 12(2), pp. 256-272, 2020.

[7] Kumar, A. M. et al., *Solar Operated IoT-based Smart System to Monitor*, Proceedings of the Seventh International Conference on Communication and Electronics Systems, pp. 455-461, 2022.

[8] Ramesh, G., Logeshwaran2, J. & Aravindarajan, V., *A Secured Database Monitoring Method to Improve Data Backup*, BOHR International Journal of Computer Science, 2(1), pp. 1-7, 2023.

[9] Hrischev, R., *ERP systems and data security,* IOP Conf. Series: Materials Science and Engineering 8, pp. 1-8, 2020.

[10] Tawalbeh, L., Muheidat, F., Tawalbeh, M. & Quwaider, M., *IoT Privacy and Security: Challenges and Solutions*, Applied Sciences, 10(4102), pp. 1-17, 2020.

[11] Manolache, F. B. & Rusu, O., *Automated SSL/TLS Certificate Distribution System,* 20th RoEduNet Conference: Networking in Education and Research (RoEduNet), pp. 1-6, 2021.

[12] Cui, H. et al., *Pay as You Decrypt: Decryption Outsourcing,* IEEE Transactions On Information Forensics And Security, Volume 15, pp. 3227-3238, 2020.

[13] Knight, R. & Nurse, J., *A Framework for Effective Corporate Communication*, Computers & Security Journal, pp. 1-35, 2020.

Sistem de securitate digital cu modul de inteligență artificială pentru comunicații de date în cadrul unei companii de producție

Sistemele de securitate în economia reală au fost adaptate pentru activitățile de comuniacare online, satisfăcând specificitățile acestora : conexiuni si comunicare la distanță, semnături electronice, criptarea informatiei, securitatea bazelor de date, confidentializtatea clientilor. Această cercetare include etapa de concepție și implementarea unui sistem de securitate pentru comunicarea datelor proveniți de la indicatorii de calitate și productie dintr-o firmă textilă și optimizarea funcțională a acestui sistem prin analiza nivelurilor de satisfacție ale clienților (beneficiari și furnizori) pentru funcțiile sale principale. Se prezintă procesul de reconcepere a acestui serviciu printr-o analiză de inovare incrementală bazată pe metoda ingineriei valorii. Cercetarea metodologică propune soluții pentru procesul de optimizare funcțională a sistemului de securitate pentru transferul de date prin reconceperea funcțiilor și, în final, aplicarea și implementarea acestor soluții într-un sistem de securitate îmbunătățit, cu valoare adăugată.

Adrian VILCU, Eng. PhD., Lecturer, Department of Engineering and management, Faculty of Industrial Design and Business Management, "Gheorghe Asachi" Technical University of Iasi, 29 Dimitrie Mangeron Blvd., Iasi, 700050, Romania, Email: adrian.vilcu@academic.tuiasi.ro.

Dumitrel TODIRICĂ, Eng., "Gheorghe Asachi" Technical University of Iasi-Romania, Faculty of Electrical Engineering, No. 21-23, 700050, Iasi, Romania, Email: dumitrel.todirica@student.tuiasi.ro.

Ionuț Viorel HERGHILIGIU, PhD. habil., Associate professor, Department of Engineering and management, Faculty of Industrial Design and Business Management, "Gheorghe Asachi" Technical University of Iasi, 29 Dimitrie Mangeron Blvd., Iasi, 700050, Romania, Email: ionut-viorel.herghiligiu@academic.tuiasi.ro.

Ion VERZEA, PhD. habil., Professor, Department of Engineering and management, Faculty of Industrial Design and Business Management, "Gheorghe Asachi" Technical University of Iasi, 29 Dimitrie Mangeron Blvd., Iasi, 700050, Romania, Email: ion.verzea@academic.tuiasi.ro.