PROPOSAL FOR SOFTWARE MANAGEMENT SOLUTION TO PREVENT POTENTIAL ISSUES

Mirona Ana Maria ICHIMOV[1], Mihai Valeriu POPESCU[2,], Olivia Doina NEGOITA[3,], Iustina-Cristina COSTEA-MARCU[4,], Georgiana MOICEANU[5,*]

Computer sciences have become a part of integrated in any field of activity to facilitate processes and improve the efficiency of different activities. By using designated or custom-made solutions, institutions can track easily documents and essential data. By adopting software systems and educating employees about possible security breaches, some of them being due to human errors, the benefits of protecting personal and confidential data in a secured digitalized application are the future in any public or private institution. The authors realize a systematic review of scientific papers to present the main aspects of security issues of applications and the digital environment. As a solution, computer science and engineering are in an integrated fashion, to address critical issues related to the protection of important information.

Keywords: Computer Software Solution, Data Management, Digital Data Protection, Reliability of Data

1. Introduction

Global industries, in the past 30 years, have faced technological changes that increased flexibility, reactivity, and faster product delivery, but also, faced severe challenges given to technological change and increased complexity [1].

Digitalization is a term that in recent years has become widely used in public discourse, although on many occasions it was not completely understood. Digitalization aims to take full advantage of information and communication technology in society and systems. In other words, from paper to computer data via digitization, the concept of digitalization targets automated processes to better take

[1] Lect., Dept. of Entrepreneurship and Management, National University of Science and Technology POLITEHNICA Bucharest, Romania, Academy of Romanian Scientists, Bucharest, Romania, e-mail: mirona.popescu@upb.ro

[2] Ph.D. Eng., Dept. of Entrepreneurship and Management, National University of Science and Technology POLITEHNICA Bucharest, Romania, e-mail: mihai.popescu0409@icloud.com

[3] Associate Prof., Dept. of Entrepreneurship and Management, National University of Science and Technology POLITEHNICA Bucharest, Romania, e-mail: olivia.negoita@upb.ro

[4] Lect., Dept. of Entrepreneurship and Management, National University of Science and Technology POLITEHNICA Bucharest, Romania, e-mail: iustina.costea@upb.ro

[5]* Associate Prof., Dept. of Entrepreneurship and Management, National University of Science and Technology POLITEHNICA Bucharest, Romania, *corresponding author, e-mail: georgiana.moiceanu@upb.ro

advantage of computer data. A common definition says digitization is the material process of converting individual analog streams of information into digital bits. The emergence of digitalization has a continuous effect on society and is a subject of constant discussion. Through digitalization, we will soon have for the first time a single-connected infrastructure for all relevant activities of society [2]. These innovations could lead to new forms of cooperation between companies or the modification of relationships with customers and employees [3]. As a result of this new embedded usage of digital technologies, companies can achieve success in terms of experiencing optimized resource utilization, reduced costs, increased employee productivity and work efficiency, optimized supply chains and increased customer loyalty and satisfaction [4].

However, the increasing number of opportunities driven by digitalization also put pressure on companies to escape their familiar point and to continuously search for new opportunities, requiring managers to significantly adapt to new successful business models. Digitalization, through the appearance of new software solutions that increase flexibility and response time, is easily adopted by emerging companies in all industries. But this is not the case for giant corporations which face more difficulty in implementing these new software systems [5].

A set of concepts that aims to fully take advantage of this new software and hardware innovations, called Industry 4.0, is currently in the phases of adoption. Industry 4.0 is a strategic German initiative to introduce the “smart factory” concept into the industry domain, where computer systems monitor the production processes of a factory and make decentralized decisions. All industries have benefited greatly from technologies like artificial intelligence (AI), cloud computing (CC), ontology, blockchain (BC), data analytics (DA), Internet of Things (IoT), laser scanning (LS), and machine learning (ML), all based on software [6].

While some software solutions aim to fully integrate and connect all relevant people from an organization, from all disciplines to work and collaborate on product lifecycle management system platforms, other software solutions derived from digitalization aim to a more niche approach, offering different software solutions that target specific processes. The increasing volume of data that is being generated within enterprises, the need for stricter data governance. Also, complex hardware requirements, including public cloud, data centers and numerous connected devices, from IoT sensors to robots and remote servers create complex challenges for companies.

Document management systems are automated software solutions that improve workflows and competitiveness and were developed to answer the challenges presented above. Despite the importance of this type of solution to improve workflow and business processes that has made many governments and organizations invest heavily in it, some organizations or individuals still don't utilize this technology, making them vulnerable in the face of competition.

The sheer volume of data that businesses create, manipulate and store is growing and driving a greater need for data governance. In addition, computing environments are more complex, typically spanning the public cloud, the enterprise data center and numerous edge devices, from Internet of Things (IoT) sensors to robots and remote servers. This complexity creates an extended attack surface that is more difficult to monitor and secure.

Consumer awareness of the importance of data privacy is growing. Fueled by increased public demand for data protection initiatives, many new privacy regulations have recently been adopted, including the General Data Protection Regulation (GDPR). Following the COVID pandemic, there is a trend for increasing flexibility through the use of remote connections, thus reducing the need of physical presence. Contracts are a vital part of every company and address the challenges of flexibility and remote use for online contract management.

Few studies have looked at the adoption of information systems that support innovation processes, despite the rising prominence of innovation [7]. Organizational, technological and environmental context refers to descriptive measurements of companies such as traits, IT expertise, existing technologies, and external environment that can influence any decision for adopting a potential software solution management [8, 9].

Since the proposed paper proposes a new web-based contract management application with integrated digital signatures, assuring transparency and flexibility from generation to the signed agreement, it is necessary to say that the adoption and use of IT applications have drawn significant interest from the information system research community over the past three decades. Thus, many theories helped explain some of the aspects related to the use and adoption of IT applications [10]. It can be interesting to think about how an IT application spreads among a company's employees or how IT applications spread among different businesses, especially when using it is not required, maybe the need for the application is not even identified at the moment of appearance but its characteristics and benefits makes it later indispensable [11, 12, 13].

The main issues now move from identifying requirements and interface design to managing the inevitable change that the implementation of IT enterprise apps will bring about in an era, where there are numerous ready-to-use IT enterprise applications [10] and not just that but also security issues brought along with it, mainly because digitalization implies cybersecurity aspects too [14]. Since IT is so important to modern businesses, being able to introduce new IT respectively software management solution applications into organizations successfully are essential for the growth of company capabilities [12, 15, 16].

The primary objective of this paper is to propose a software management solution that can prevent potential issues, ensuring different characteristics such as credibility, financial and information safety, contract management safety, and diminishing the risk of client interception, etc. Major contributions include elements from early concept to end product (software design). Images with the software are presented to be able to understand better the interface. Also, an important aspect is related to the private character and the security aspects that are incorporated.

2. Material and methods

Data security is the practice of protecting digital information against unauthorized access, corruption, or theft throughout its lifecycle. It is a concept that encompasses every aspect of information security, from the physical security of hardware and storage devices to administrative and access controls and the logical security of software applications. It also includes organizational policies and procedures.

When properly implemented, sound data security strategies will protect an organization's information assets from cyber activities but will also protect against insider threats and human error, which remain among the leading causes of data breaches today. Data security involves implementing tools and technologies that increase an organization's visibility into where its critical data resides and how it is used. Ideally, these tools should be able to enforce protections such as encryption, data masking and redaction of sensitive files, and should automate reporting to simplify audits and comply with regulatory requirements. Thus, for companies that have contracts with other third parties, one way to organize and store data for enhanced protection is also in the digital environment through dedicated applications.

Web-based applications offer a much greater ability to integrate with other systems than desktop applications. Localized software is isolated compared to web-based applications, which are significantly more interoperable. This is because web-based applications can be linked together more easily than two separate systems. Access is granted once the software is installed on the host server. Whenever there is an update, it can be applied through the host server, without having to update every computer. This means that new software or upgrades are deployed more easily, and maintenance can be performed through a central point. The time needed to make changes is reduced and the system is consistent.

As more processes need to take place simultaneously, web software can facilitate this. In addition, where problems occur, servers can be completely replaced without affecting the entire operating system.

This, therefore, reduces any downtime. Thus, a software product has been developed to allow organizations to organize and secure their contracts that are private from potential malicious people, unauthorized access, or possibly human error. Fig. 1 shows the architecture of the application. The system consists in several specialized servers which collaborate to ensure the functionality and security of the infrastructure. The main server acts like a communication node between users and components and manages the authentication/authorization, redirecting the requirements to the corresponding modules and ensuring an efficient distribution of resources. All external requirements are filtered by the Firewall server, who blocks the unauthorized tentative of access, including DDoS attacks. Only verified requests are redirected to the main server, providing a high level of security. User data and files are managed by the database server, which communicates frequently with the main server to stock and recover data, guaranteeing accessibility and integrity. For documents that require digital validation, the system includes a server dedicated to signatures, that is responsible for applying digital signatures to PDF files. Once a document is signed, it can be stored on the server dedicated to documents, as here it will be a secured archive for the management and distribution of files. By linking all these servers, the infrastructure allows a secure and efficient flow of data, offering the users a robust system to deposit and process information.

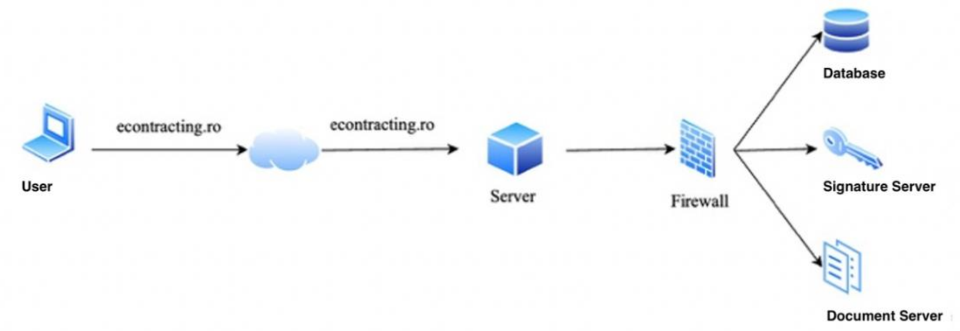

Fig. 1. Proposed architecture of software solution

Fig. 2 shows the architecture of the application. In this case, the Firewall server aims to protect applications against cyber-attacks, for example DDOS attacks. The code snippet in Supplementary material describes the process of loading and reading PDF documents into memory. To digitally sign the document, the first step is to read the document. All documents in the application are in PDF format so that they cannot be modified in text, as they are legislative documents.

Once the document has been uploaded using the method exemplified above, the digital signature process follows. If the document is not uploaded, an error message is displayed to the user trying to operate. If this step is properly completed there are two situations:

Case 1. The document has no digital signature
Case 2. The document has a digital signature

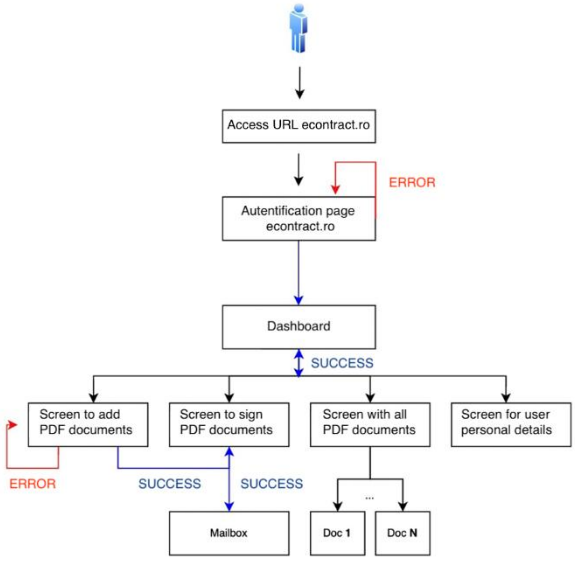
Access URL econtract.ro
ERROR
Autentification page econtract.ro
Dashboard
SUCCESS
Screen to add PDF documents
Screen to sign PDF documents
Screen with all PDF documents
Screen for user personal details
ERROR
SUCCESS
SUCCESS
Mailbox
...
Doc 1
Doc N

Fig. 2. Main activities and screens of econtracting.ro

A different method is used for each case. In the first case of the unsigned document, the method used consists of parsing the document and identifying the area allocated for entering the digital signature. As the document has no digital signature, the section designated for signing (acroform) must be created. The certificate is extracted from the digital signature and the PDF document is signed with it.

In the second case, the PDF document already contains a digital signature. This looks for the end of the acroform section specified above and at its end adds another digital signature.

Supplementary material shows the middleware service, the purpose of which is to intercept every request executed by a user on the web application. If the URL accessed needs authentication, the service checks if the JWT token is valid. This step ensures that private URLs cannot be accessed by unauthenticated users. Each user has their own rights according to their assigned role in the web platform. Once the authentication (JWT token) has been validated, the user permission verification process follows. This step limits the users' right to access URLs, i.e. pages in the application, that are not intended for them. The method in the Supplementary material is used when a PDF document is accessed by the user. The application sends the document ID and the backend then gets the file/folder. Note the use of the authentication middleware service to ensure that the user is authenticated. If the user is authenticated the getFolder() method is called to return the PDF file. The method checks if the user has permission for the desired file.

3. Results

The web application developed allows institutions to organize, handle and digitally sign their contracts. The use of the application facilitates the process of transmitting and handling different types of contracts in the digital environment, providing secure measures for the protection of private data. This process has been designed to be easy, both in terms of the flow of actions required and the user interface, maintaining high transparency by constantly informing users of the status of a contract.

By entering the address econtract.ro a user reaches the first screen of the web application software solution, the login page, Fig. 3. It presents two options: "Create account" and "Log in". If the user is new and does not have a username and password, he or she can access the "Create account" option by clicking on the button that will redirect him or her to a page intended for this purpose. The password must be changed once the platform is accessed for the first time from security reasons.

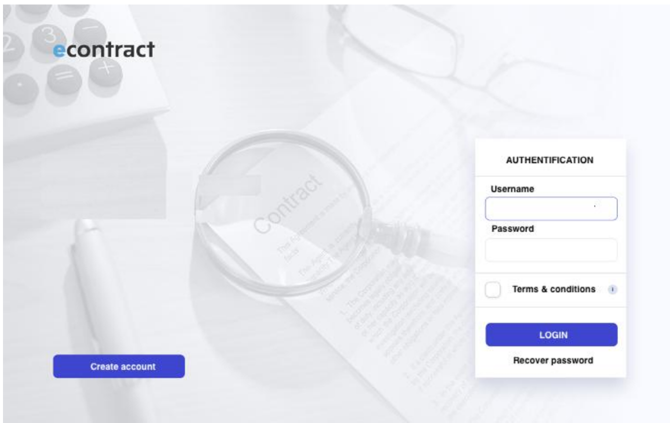

Fig. 3. Screen for authentication and to create a new account

To create a new account, a user must fill in a form, Fig. 3. In this form, there are several fields such as name, surname, and email address. These fields appear in plain text, unlike the password fields. To avoid possible human errors, the password must be repeated. If the user is a legal entity, they must tick the field for this option. Once the terms and conditions are accepted, the account will be successfully created. If one of the fields is not filled in with data appropriate for the purpose for which it was designed, an error message will be displayed, and you will not be able to proceed with this step. The same result is identified if the “Terms and conditions" box is not checked.

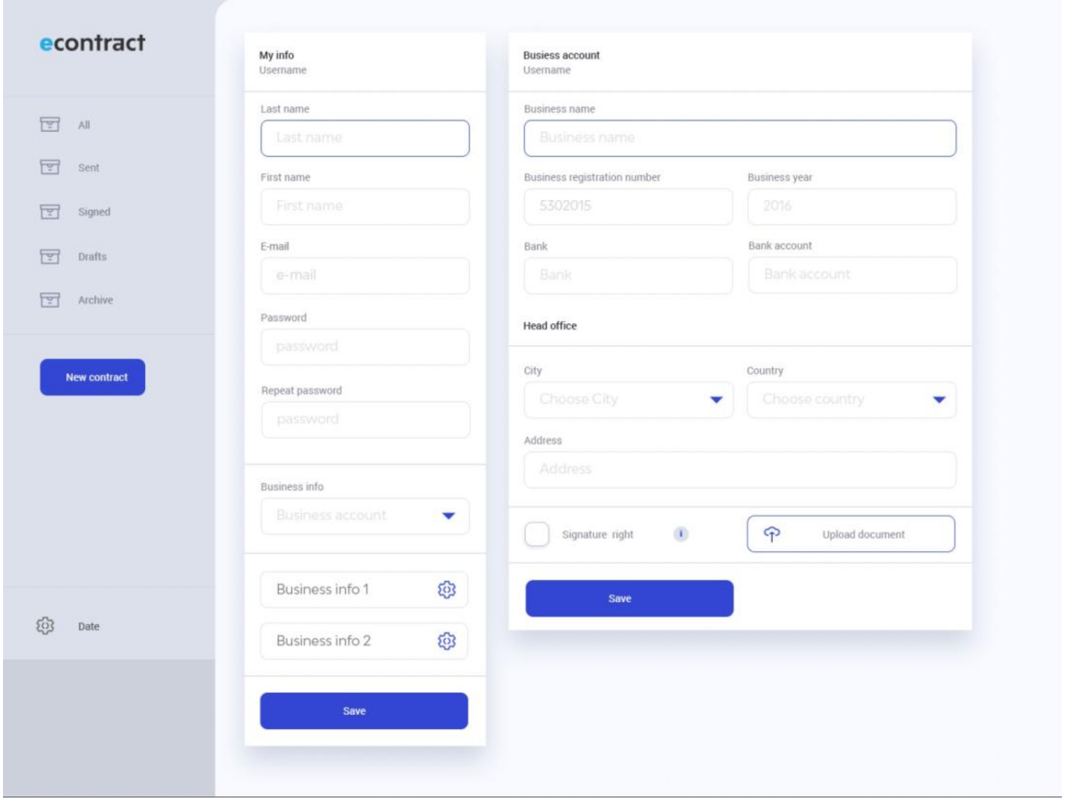

Fig. 4. Form to create an account for legal entity

If the user is a legal entity, he/she will have to fill in additional data, Fig. 4a. This screen appears once the box, "Check if you are a legal entity" is checked. This data refers to the name of the company, i.e. the name under which it is registered, the unique registration code, the trade register number, the bank where the company has an account, as well as the account held and details of its registered office: town, county, address. The "Right to sign" box represents the user's agreement that he/she is authorized by the company to sign on its behalf. To save the completed data, click on the "Save" button. The menu on the left of the screen shows the actions that a user can perform from the web application, namely:

- All (all documents, and files to which the authenticated user has access in the platform)
- Sent (documents that have been sent by the user to other users or third parties)
- Signed (PDF documents that have already been signed by the user)
- Drafts (draft documents that have not yet been finalized)
- Archived (documents already signed, which have been electronically filed)
- New folder (option to create a new folder for organizing files)
- Data (user's personal data)

Once the user successfully logs into the web application, they are redirected to the home page. If he is a new user this page does not contain documents, but only the menu with the options (actions) he can perform (Fig. 4b).

To quickly identify a particular contract, there is a search box that sorts by letter or number characters received as input from the user. When you want to draw up a contract, you can use the "Choose model" option, which returns names of contract types in response. By selecting a specific type, the user opts for a predefined template, where he/she fills in specific data, without having to draft a contract from scratch. Each contract must have a unique name, a contract type, and the persons or third parties who will have the right to view and sign the document must be added. The field named “Invited e-mail" is for persons who only have the right to view the contract. The field “Contract party" is the name of the provider/beneficiary who will be party to the contract in question. To continue the process, the user must give his/her consent to the processing of personal data by ticking the box representing this purpose. After the step of drawing up a new contract, a PDF document that exists in the local memory of the electronic device from which the web application is accessed can be uploaded to be shared and signed with a digital signature. The success message can be found when a document has been successfully digitally signed, account data has been validly filled in, etc. A server error message appears when one of the above actions has not been successfully executed.

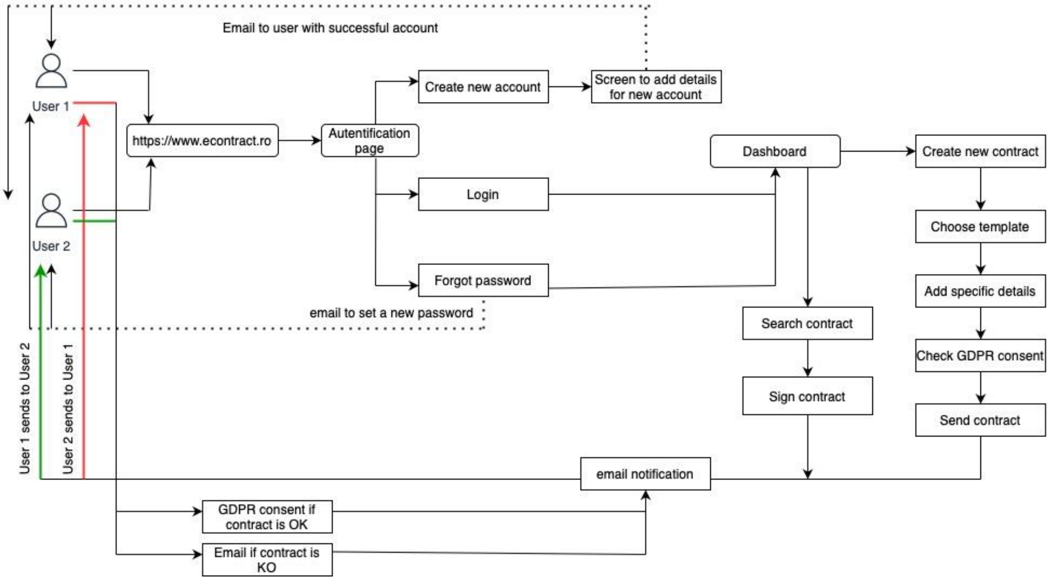

Fig. 5. Flow between two entities to create and sign a contract

Within a contract, there is a predefined flow of steps. Their purpose is to render the status of the contract at every important point in time for users. Fig. 5

presents all the steps between 2 entities that want to sign a digital contract with digital signature.

From a usability point of view, the process is easy, being supported by different types of messages, to notify the user. Also, the interface was designed to provide a flowless environment, having only the important elements, not to overwhelm the user.

Once a new contract is created the CEO of company X gives his consent to the processing of private data. Then, the contract is sent to the CEO of company Y.

The CEO of company X is notified that the CEO of company Y has received the contract. If the CEO of company Y agrees with the data passed, he also gives his consent to the processing of private data. Then, the CEO of company X receives notification with the acceptance of the CEO of company Y.

The CEO of company X signs the contract with a digital signature. As a result, he CEO of Company Y is notified that the contract has been signed by the CEO of Company X, therefore he also signs the contract.

The CEO of Company X receives a notification informing him that the CEO of Company Y has successfully signed the contract. The contract is signed by both participating parties and visible without the right to modify within the platform interface of the CEO of Company X and the CEO of Company Y.

4. Discussions

To build trust with the user of any software solution 3 pillars have been identified: Confidentiality, Reliability, and Integrity. Trust (noun), as defined in Mirriam Webster (Mirriam Webster Dictionary), is an assured reliance on the character, ability, strength, or truth of someone or something. Fundamentally this can be applied directly to software. Any software product should abide by the three pillars to be able to have an impact in the software market, especially if it deals in legally binding actions. To correctly measure these principles scientific studies were analyzed to summarize the core concept behind each pillar, be it a successful example or even study the effects of a poorly managed solution that can have deep ramifications to the well-being of the user.

1. *To start, the Confidentiality metric was analyzed through different papers, each tackling different issues found in the modern software space.*

A study [17] conducted on the matter of cloud computing was pursued to find the current problems the user base is facing. The main security concerns which were discovered revolved around the concept of data breaches and overall managed security. A particular segment of the cloud environment is the health sector's implementation of it. This particular branch of the cloud-based services pertaining to the health sector is analyzed in the paper [18] and a design model is created that is conscious of the security and confidentiality needs of the data that it will contain. Threat models are also discussed with the intent of finding the most glaring issues that a solution of this type can face. Regarding mobile applications in the ever-growing market, a study [19] has been made on static code analysis to evaluate the ongoing problem of data breaches regarding the mHealth application variant. The issues found were identified from a large pool of selected entries and concluded that a machine-based approach of evaluation is a good tool used when paired with human analysis to assess confidentiality violations of this particular type of software. In the banking sector where highly sensitive data is prevalent and tackles an enormous stream of data daily confidentiality is a must. The paper [20] analyzes existing strategies and elaborates upon them to create a safer and confidentiality-oriented data model. It offers concepts regarding data obfuscation, data reduction to bolster the security of sensitive personal data and personally identifiable information. The software solution presented through this research aligns with this metric by assuring the security of sensitive e data and the integrity of documents, allowing controlled access only to the involved actors. Using standardized templates, the system reduces the risk of unauthorized exposure of information, according to the principles identified in recent studies.

2. The second metric analyzed was the Reliability metric considering some of the results of others such as:

A study [21] pertaining to the evaluation of reliability was conducted to assess various approaches to quantify the reliability metric. Four models were defined to compute the software trust value. Regarding the current status and future perspectives of the Internet of Things, concept was reviewed in the article [22]. The main concern of the IOT revolutionary transition implementation stands in its reliability. The fourtier reliability model is determined, and a thorough analysis is done of this technology. The overall conclusion is that it being an infant technology certain issues arose regarding current complexity, lack of exhaustive analysis on this subject, and the plethora of new features that appear daily. Using data from development processes and statistical techniques, the paper [23] studies the reliability metric prediction methods. This study offers a helping hand to software engineers by providing a method of anticipating product reliability and reducing risk-inducing actions. The widespread market of mobile applications is full of error-prone and data-breaching products, as the study [24] determined. As the computational power of handheld devices has risen to levels that can enable users to use resource-heavy applications, that were exclusive to personal computers, data safety concerns are rising. The authors concluded with the notion of data sharing being of utmost importance in the mobile environment. The software solution described in this study improves the reliability by ensuring a stabile process, having reduced errors and downtime. Through the provided templates and automated notifications along with real-time tracking of documents status, the system reduces the risk of data loss or corruption. Therefore, it aligns with the conclusions of other studies that highlights the importance of redundancy, automated checks and of recovery mechanisms to increase reliability.

3. The last metric that has a valued importance is Integrality which was studied considering:

The paper [25] introduces Correctness by Construction, which is a method of software development that reduces the number of errors that can appear during the product lifecycle. Plagiarism is an issue that stains the academic environment. The Arab program [26] paper intends to create plagiarism software suited to discover similarities between two or more papers designed specifically for the syntax and semantics of the Arabian languages. Code signing, the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted is re-viewed in the bulletin [27]. Issues regarding this process is discussed and a general workflow is suggested to mitigate any problem that can appear. Biopharmaceuticals are intrinsically tied with Industry 4.0 and Big Data concepts, as the paper [28] elaborates upon. The study dissects potential mitigation techniques and approaches to guarantee data integrity. The software solution detailed in this paper ensures data integrity through robust mechanisms for validation and protection against unauthorized access. Using digital signatures, automated checks and the history of versions, the systems is designed to keep the contracts intact throughout the entire signing flow. These characteristics aligns with previous research that underline the need for security and auditability protocols to maintain the integrity of data when handling documents.

6. Conclusions

The emerging digitalization and unprevented situations like COVID-19 have a strong impact on institutions' activity. To continue their activity and keep up with market requirements or government decisions, more and more of their processes shifted in the online environment. This paper presents an overview of the most important characteristics related to adopted applications inside the organization: statistics over EU enterprises that have encountered security issues, confidentiality, accessibility, and integrity of data. The authors implement a software product - a web-responsive application that allows the storage and manipulation of institution documents such as contracts and allows them to be signed with a digital signature based on user role and permissions. From a practical point of view, the responsive web application developed and presented in this paper comes as a tool dedicated to Romanian institutions to facilitate the process of signing documents. According to Romanian Legislation institution contracts and official documents must be signed and stored in a physical format. Therefore, in case of unprevented negative incidents, many of them can be lost and the data unable to be recovered. As a solution, this secure implemented platform comes as an online backup. Shortly, it can be the approved digital environment for official documents in Romanian institutions. The software product restricts access to important contracts and organizes/filter them in an easy manner. Its features allow an authorized user to create, modify and delete any contract, to divide them by folders, and present a multitude of authorized legal templates that may help when a new contract is created. One of the main benefits is represented by the digital signature which is better encrypted and guarantees a higher level of security and false identity. Besides these, entities that are in the process of elaborating and signing a contract may see the process status in the platform for a more transparent perspective and are also notified via email. By assuring this level of transparency it reduces the possibility of human threats.

REFERENCES

[1]. Lerch, C. and Gotsch, M., Digitalized product-service systems in manufacturing firms: A case study analysis. Research-technology management, 58(5), pp.45-52., 2015

[2]. Gorensek, T. and Kohont, A., Conceptualization Of Digitalization: Opportunities And Challenges For Organizations In The Eu-ro-Mediterranean Area, Conceptualization of the Digitalization: Opportunities and Challenges, Vol. 11, No. 2, pp. 93 – 111, 2019

[3]. Kiel, D., Arnold, C., Collisi, M. and Voigt, K.I., The impact of the industrial internet of things on established business models. In Proceedings of the 25th international association for management of technology (IAMOT) conference (pp. 673-695), 2016

[4]. Coupette, J., Digitalisierung zwischen Erwartung und Implementierung. IM+ io Fachzeitschrift für Innovation, Organisation und Management, 1, pp.69-75, 2015.

[5]. Wirtz, B.W., Schilke, O. and Ullrich, S., Strategic development of business models: implications of the Web 2.0 for creating value on the internet. Long range planning, 43(2-3), pp.272-290, 2010

[6]. Khudhair, A., Li, H., Ren, G. and Liu, S., Towards future BIM technology innovations: A bibliometric analysis of the literature. Applied Sciences, 11(3), p.1232, 2021

[7]. Troshani, I., Rampersad, G. and Plewa, C., Adopting innovation management software in university innovation commercialization. Journal of Computer Information Systems, 52(2), pp.83-92., 2011

[8]. Awa, H.O., Ojiabo, O.U. and Emecheta, B.C., Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs. Journal of Science & Technology Policy Management, 6(1), pp.76-94, 2015

[9]. Awa, H.O., Ukoha, O. and Emecheta, B.C., Using TOE theoretical framework to study the adoption of ERP solution. Cogent Business & Management, 3(1), p.1196571, 2016

[10]. Varajão, J., Carvalho, J.Á., Silva, T. and Pereira, J., Lack of awareness of IT adoption and use theories by IT/IS project managers: poor relevance, unfocused research or deficient education?. Information, 13(2), p.48, 2022

[11]. Rogers, E.M. Diffusion of Innovations, 5th ed.; Free Press: New York, NY, USA, 2003

[12]. Kääriäinen, J., Pussinen, P., Saari, L. and Kuusisto, O., Applying the positioning phase of the digital transformation model in practice for SMEs: toward systematic development of digitalization. International journal of information systems and project management, 8(4), pp.24-43, 2020

[13]. Janssens, G., Kusters, R. and Martin, H., 2020. Expecting the unexpected during ERP implementations: a complexity view. International Journal of Information Systems and Project Management, 8(4), pp.68-82, 2020

[14]. Moşteanu, N.R., Challenges for organizational structure and design as a result of digitalization and cybersecurity. The Business & Management Review, 11(1), pp.278-286, 2020

[15]. Patnayakuni, R. and Ruppel, C.P., A socio-technical approach to improving the systems development process. Information Systems Frontiers, 12, pp.219-234, 2010

[16]. Varajão, J. and Trigo, A., December. Evaluation of IS project success in InfSysMakers: an exploratory case study. In ICIS, 2016

[17]. Gupta, M., Ahuja, L. and Seth, A., A Study on Cloud Environment: Confidentiality Problems, Security Threats, and Challenges. In Soft Computing for Security Applications: Proceedings of ICSCS 2021 (pp. 679-698). Springer Singapore, 2022

[18]. Thillaiarasu, N., Shanmugam, R., Thirunavukkarasu, K. and Khan, S., Design Schema to Offer Security and Confidentiality to Healthcare Data in Cloud Environment. In Global Healthcare Disasters (pp. 179-195). Apple Academic Press, 2022

[19]. Brüggemann, T., Dehling, T. and Sunyaev, A., No risk, more fun! Automating breach of confidentiality risk assessment for Android mobile health applications. In Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2019), Forthcoming, 2018

[20]. Agufa, S.N., A Mechanism for Enhanced Confidentiality of Personal Data in Mobile-Money Transactions (Doctoral dissertation, United States International University-Africa), 2020

[21]. Raju, M.V., Kumar, A., Phonsa, G. and Tiwary, S., Estimation of Reliability in Software Applications. Think India Journal, 22(30), pp.1474-1480, 2019

[22]. Xing, L., Reliability in Internet of Things: Current status and future perspectives. IEEE Internet of Things Journal, 7(8), pp.6704-6721, 2020

[23]. Sahu, K. and Srivastava, R.K., Revisiting software reliability. Data Management, Analytics and Innovation: Proceedings of ICDMAI 2018, Volume 1, pp.221-235, 2019

[24]. Makar, K., Goel, S., Kaur, P., Singh, M., Jain, P. and Aggarwal, P.K., Reliability of Mobile Applications: A Review and Some Perspectives. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-4). IEEE, 2021

[25]. Chapman, R., Correctness by construction: a manifesto for high integrity software. In ACM International Conference Proceeding Series, Vol. 162, pp. 43-46, 2006

[26]. Saleh, A.A.H.H., Science integrity software in intellectual production with planning to develop an Arab program. Arab International Journal for Information Technology & Data, 1(1), pp.15-38, 2021

[27]. Cooper, D., Feldman, L. and Witte, G., Protecting Software Integrity Through Code Signing (No. ITL Bulletin). National Institute of Standards and Technology, 2018

[28]. Alosert, H., Savery, J., Rheaume, J., Cheeks, M., Turner, R., Spencer, C., S. Farid, S. and Gol-drick, S., Data integrity within the biopharmaceutical sector in the era of Industry 4.0. Biotechnology Journal, p.2100609, 2022