CUREX: seCUre and pRivate hEalth data eXchange

Farnaz Mohammadi
Department of Digital System
University of Piraeus, Greece,
farnaz@unipi.gr

Angeliki Panou
Department of Digital System
University of Piraeus, Greece,
apanou@unipi.gr

Christoforos Ntantogian
Department of Digital System
University of Piraeus, Greece,
dadoyan@unipi.gr

Eirini Karapistoli
Cyberlens B.V.
The Netherlands,
irene.karapistoli@cyberlens.eu

Emmanouil Panaousis
Department of Computer Science
University of Surrey, UK,
e.panaousis@surrey.ac.uk

Christos Xenakis
Department of Digital System
University of Piraeus, Greece,
xenakis@unipi.gr

ABSTRACT

The Health sector's increasing dependence on digital information and communication infrastructures renders it vulnerable to privacy and cybersecurity threats, especially as the theft of health data has become lucrative for cyber criminals. CUREX comprehensively addresses the protection of the confidentiality and integrity of health data by producing a novel, flexible and scalable situational awareness-oriented platform. It allows a healthcare provider to assess cybersecurity and privacy risks that are exposed to and suggest optimal strategies for addressing these risks with safeguards tailored to each business case and application. CUREX is fully GDPR compliant by design. At its core, a decentralised architecture enhanced by a private blockchain infrastructure ensures the integrity of the data and – most importantly- the patient safety. Crucially, CUREX expands beyond technical measures and improves cyber hygiene through training and awareness activities for healthcare personnel. Its validation focuses on highly challenging cases of health data exchange, spanning patient cross-border mobility, remote healthcare, and data exchange for research.

CCS CONCEPTS

· Social and professional topics~Health information exchanges

KEYWORDS

eHealth, Cybersecurity, Risk assessment, Blockchain, Cyber hygiene

1 Introduction

The digital asset that is regarded to be of the highest importance in the healthcare domain and a priority target for cyber-criminals is data. As a result, the number of cyber-attacks targeting the acquisition of data having recorded a major rise during the last years [1]. Cyber-attacks also cause severe disruptions in health organisations' business processes and their operation. This calls for the effective preparation of organisations in an ever-evolving cyber-attack landscape.

Indicatively, both cyber-attackers and cyber-defenders are currently racing to utilise the power of machine learning. A report by Intel reveals [2] that a large portion of healthcare organisations and service providers have fallen behind in the process of performing a complete analysis and assessment of their cybersecurity and privacy risks, even though there has been an extensive classification effort from ENISA on assets, vulnerabilities and threats that affect modern healthcare organisations and service providers. As stated by the ENISA report [3], currently a significant number of EU member states present a low level of maturity and they lack a structured approach regarding the identification of critical information infrastructure in healthcare service provision. This can pose severe risks regarding the increasing dependency of the vital functions of the society to these organisations.

Healthcare services are moving towards novel models that are highly dependent on massive exchange of data, increased connectivity between platforms, devices, and organisations. It is also important that data exchange needs to cover cross-border situations in order to provide better service variety in healthcare. This creates more challenges regarding the preservation of data security and patient privacy. At the same time, the new EU GDPR framework significantly reshapes the relationship of data controllers and processors (i.e. hospitals and healthcare service providers) with data owners, by giving greater control to the latter over their data. Full compliance with GDPR directives will need to be constantly ensured as any violation leads to serious penalties.

Healthcare officers need ways to stay ahead of impacts incurred, both financial and social, resulting from data security and privacy violations. Medical professionals need to be able to provide their services as effectively as possible. It is crucial for them to be able to exchange data seamlessly even when this exchange has a cross-border nature. On the other hand, IT administrators need efficient solutions that help them to remain aware, at all times, of their systems' cybersecurity and privacy levels. In the same vein, it is apparent that an organisation needs to be aware of all human factors (psychological, personality, technological background) that may have an impact in the security and privacy of health data and systems. Such awareness can be achieved primarily by making information about

potential vulnerabilities and threats easily accessible. To mitigate associated risks [4], the proposition of countermeasures offers the capability of preventing healthcare organisations from facing GDPR fines.

CUREX aims to create a cybersecurity and privacy risk assessment toolkit tailored to different types of healthcare infrastructures and services. This can be accompanied by end-user (patient and healthcare personnel) applications interfaced with a Private Blockchain (PrB) consensus business network. CUREX PrB is a business level distributed immutable ledger, where all transactions (data exchange requests/approvals, risk reporting, user consent) are stored using consensus validation, and where each transaction are governed by the implementation of specialised smart contracts. This toolkit employs ontological models to successfully map data to resources (technical and human) and leverage state-of-the-art methods of vulnerability discovery and threat intelligence. As previously identified need, CUREX also includes decision support mechanisms that devise optimal safeguards that healthcare organisations can implement to effectively mitigate the identified risks.

2 Related Work

Modern societies have become increasingly dependent upon critical (cyber) infrastructures, and this dependency is only becoming stronger as ICT progresses. Healthcare ICT infrastructures are more evidently considered as critical information infrastructures, since healthcare service provision organisations, which depend upon such infrastructures, comprise one of the backbones of economic growth and wellbeing. As compliance with the upcoming GDPR becomes one of the biggest challenges for organisations, maintaining the privacy of this information to the required level is undoubtedly a critical factor [5].

2.1 Health Data Modeling

Ontologies have been widely used to represent knowledge of different domains (including biomedical). The aim of the ontologies created in the biomedical domain includes filling the interoperability gaps between information systems and providing common ways of representing knowledge. Examples of their application are OBO-Foundry terminologies [6] for biomedical information or more clinical oriented vocabularies such as well-known vocabularies, which have ontology-based versions includes, e.g. SNOMED-CT, MeSH and ICD among others. In terms of security, ontologies have been widely used to represent information regarding information systems and knowledge in the domain of security [7].

2.2 Risk and Vulnerability Assessment

The current state-of-practice for the assessment and analysis of data-related vulnerabilities in the healthcare sector includes mostly custom and proprietary solutions that are typically employed on demand, e.g. when new systems or components are installed, or when new policies are enforced. The main goal of risk management is to protect assets and minimise costs in case of failures. The outcome of risk analysis is in most cases a list of risks or threats to a system, together with the probabilities of occurrence. International standards in the field of risk management are used to support the identification of risks or threats as well as to assess their respective probabilities such as [8], [9]. Most of these standards specify framework conditions for the risk management process but rarely go into detail on specific methods for the risk analysis or risk assessment. In principle, choosing the right method and the right tool for risk analysis and risk evaluation proves to be complicated. In recent years, a number of concepts, algorithms, and tools have evolved from research, specially designed to protect the IT infrastructure and related systems. Since their historical background is settled in a business context, in these methods a quantitative risk assessment is usually performed based on monetary costs [10] and the EBIOS method and the aforementioned ISO/IEC standard [9]. In this context, most of the methods and tools (see [11] for a comprehensive list) just use the commonly known rule of thumb Risk = Probability x Potential Damage [12]. Depending on the applied method, the terms and scales for the assessment of the probabilities as well as the potential damage are predefined (e.g. [13], [14]).

2.3 Decision Support for Proposing Optimal Safeguards

There is a number of approaches proposed to identify which safeguards should be selected for implementation within an available budget. Most approaches apply management tools and financial analysis based on measures like annual loss expectancy, return on investment, internal rate of return, net present value [15]. Other approaches use real options analysis where dynamic aspects of investments are considered and the flexibility of decision making is utilized [16]. An optimisation driven approach to select security safeguards is proposed by [17] which produce optimal safeguard portfolios. The authors in [18] proposed a model that minimises the total loss caused by security incidents. By employing a what-if analysis, the decision maker can then decide which solution should be implemented. Another option to treat uncertainty is fuzzy set theory used in [19] to develop a decision support system addressing uncertain threat rates, impacts on assets, and counter-measure costs. To achieve this all approaches, require extensive input data like threat probabilities, incident costs, countermeasure costs, countermeasure success probabilities, etc. which makes them very to apply in practice. [20] lower input data requirements by using discrete scales for probability and impact values. It is, however, still problematic since finding a trade-off between costs and risk requires both to be measured accurately.

2.4 Cyber Hygiene

The preparedness of healthcare organisations has not been studied thoroughly yet. However, [21] notes that alongside awareness efforts, organisations need to try to discover the descriptive norms in their organisations. This supports the argument for monitoring of behaviour, to provide direct

evidence of existing security-related habits in system data and from other sources. [22] explores the potential for understanding employee behaviour to be a foundation for encouraging secure working practices, where encouraging employees to be proactive can increase their organisation's security. Moreover, the authors in [22] advocate consideration of psychological factors in user-facing security, but also appropriate delivery of messages, and provision of reporting structures for two-way involvement. These human aspects (psychology, personality etc.) have been also identified by ENISA in their Cybersecurity culture report [3], as a major factor that may affect the security of data and systems.

2.5 Blockchain Technologies

During the last years, the popularity of the blockchain has been increasing and has reached important notoriety not only in scientific and IT journals but also in general public media. Since Blockchains (through Bitcoin [23] mostly) began attracting the attention of the financial, security and IT communities, several other blockchain implementations have been appearing. As an alternative to Bitcoin and Ethereum, the Linux Foundation has proposed a new blockchain project called Hyperledger. This project is a blockchain framework to develop new services and applications based on a permissioned ledger.

3 CUREX Architecture

The CUREX platform is composed of a number of components (tools, applications, blockchain). These components, as well as their interdependencies, are shown in Figure 1. The integrated CUREX Platform relies on a flexible and agile architecture comprising of four discrete layers:

(i) The Asset Discovery layer, which involves the tools and methodologies which consider the mapping of data, technical and human resources into ontological models.

(ii) The Threat Intelligence layer, which includes the discovery of vulnerabilities and the analysis of various resources that identifies potential threats.

(iii) The Risk Management layer, which involves the analysis and the generation of quantifiable risks that consider both cybersecurity and privacy, and the proposition of optimal safeguards and cyber hygiene enhancing techniques based on decision support systems.

(iv) The Trust Enhancing layer, which includes the deployment of a business consensus-based blockchain that stores compiled risks reports from the previous layers and integrates the CUREX tools and end-user applications into a fully GDPR compliant platform.

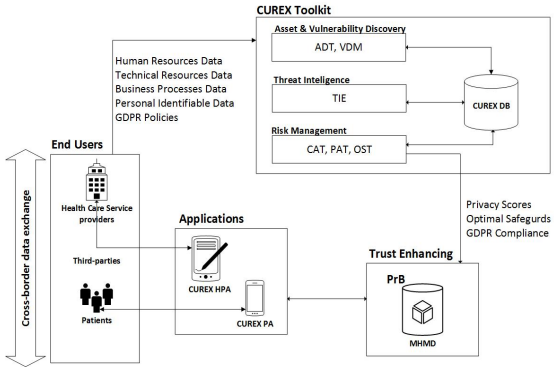

Figure 1: CUREX Architecture

From a technical perspective, this approach enables interoperability and resilience between the different components and guarantees an easy adoption and an effective platform operation. This architecture has been designed to fulfil the necessities of hospitals; healthcare centres along with their service providers and employees; and patients. Besides the architecture, in the following, we describe the aim and functionalities of each CUREX functional component.

3.1 Asset Discovery Tool and Vulnerability Discovery Manager

The first stage of the CUREX risk assessment process concerns the planning and data governance of the healthcare organisation and includes the discovery of assets during which, all information systems that collect, transform and analyse health data are taken into account. The Asset Discovery Tool (ADT) incorporates automated mapping of resources, hierarchical grouping as well as ontological representation of data and policies. The use of ontologies empowers the framework so that assets and policies about information security issues and biomedical information, which can be affected by vulnerabilities, can be grouped together. Part of the CUREX risk assessment process includes the analysis of assets and data modelling in order to identify cybersecurity and privacy vulnerabilities. These vulnerabilities are being complemented by zero-day online databases and libraries provided from standards (e.g. [9],[25]). The Vulnerability Discovery Manager (VDM) covers both health data and its structure as well as all information systems and appliances. VDM is a domain-specific tool for identifying, analysing and reporting vulnerabilities detected in a target system. Additionally, VDM uses as input information provided ADT for analysing the system and compiling the vulnerabilities. The result of VDM is provided to the Threat Intelligence Engine (described next), which will perform further and in-depth analysis of the system.

3.2 Threat Intelligence Engine

Incident discovery, which is an integral part of threat intelligence is achieved through conducting sophisticated data analysis. The Threat Intelligence Engine (TIE) incorporates

advanced machine learning (by supervised and unsupervised learning techniques) and data analytics algorithms to support its functionality and address different kinds of challenges for each business case. Several different unsupervised anomaly detection algorithms have been evaluated on the CUREX use cases as different datasets to reveal the strengths and weaknesses of particular patterns are used. TIE addresses threats that emerge from malicious external actors, but also insider threats due to either malicious intent or to lack of the proper security and privacy awareness.

3.3 Cybersecurity and Privacy Risk Assessment Tools

CUREX undertakes the activity of implementing a cybersecurity and privacy assessment toolkit incorporating state-of-the-art approaches for each individual stage of the assessment. This toolkit concludes by calculating a risk score that covers both cybersecurity and privacy readiness of the organisations. The outcome of the CUREX cybersecurity risk assessment is in the form of a measurable score or risk that accounts of all aspects of the organisations' assets, vulnerabilities, and threats. As health data exchange rises multiple privacy concerns, CUREX privacy risk assessment provides meaningful interview-based surveys to the organisations officers, in order to determine the level by which the healthcare organisation complies with the GDPR Framework. All risk analysis performed by the assessment tools are compiled into risk reports which in turn are stored in the PrB. The Cybersecurity Assessment Tool (CAT) is the CUREX Platform's implementation of cybersecurity risk assessment. CAT employs an incident detection functionality which provides the capabilities of a Security Information and Event Management solution with the additional characteristic of being able to handle large volumes of data. Additionally, CAT focuses on collecting and analysing, in real-time, cybersecurity events and consolidate a correlation of them for a risk assessment. It is specialised in preparing the information for reports in order to improve cybersecurity awareness. Moreover, CAT can obtain the information of cybersecurity events by means of agents that are deployed in different components and sub-systems. The information of the analysis of incidents is provided in CUREX to the safeguard and cyber hygiene component, which compiles and prepares all the information of cybersecurity and privacy assessment together with the business needs and information of systems. Additionally, the information processed can be accessed directly in a multilevel web-based visualisation framework for monitoring and response and allows for definition of alarms and specific reports. Finally, the goal of CAT is to employ state-of-the-art algorithms and technologies and combine them into an automated solution for hospitals and care centres to understand inherent risks that emerge from exchanging health data and drive the decisions towards successfully addressing and mitigation of these risks. The tool allows a real-time evaluation by executing specific module rules: qualitative and quantitative models. This tool allows for having a business interpretation of the cyber risks, providing expectations of costs and impact in the business for the threats. That way, the tool supports decision-making by suggesting mitigation measures.

As privacy readiness is one the of pillars of CUREX being the principle of protecting clinical data and Personal Identifiable Information (PII), as mandated by the GDPR, the Privacy Assessment Tool (PAT) assesses hospitals and care centres towards alignment with the GDPR directives. PAT addresses these privacy threats, identifies and quantifies the associated risks, and provides the analysis. As health data are typically linked to various human and technical assets inside the healthcare organisation with a specific relationship, PAT relies significantly on the modelling products of the ADT (asset ontologies and formal representations of the assets and their relationships). PAT makes extra use of the VDM in order to associate the modelled assets with existing vulnerabilities, which may have a direct effect on the privacy of the related/linked clinical data. Ultimately, to assess the privacy risk levels, PAT calculates the overall impact to all data assets of the healthcare organisation, based on the perceived privacy vulnerabilities and their likelihood to be exploited by any identified threat. Integrating NIST's guide for security risk assessment [26] with the GDPR Framework, PAT calculates the risk with a formula that quantifies the impact of the associated threats and the vulnerability-level for this asset.

3.4 Optimal Safeguards Tool (OST)

The CUREX Platform complements its cybersecurity and privacy risk assessment functionality by offering a decision support tool to propose optimal safeguards to mitigate the identified as well as future risks emerge in any health data exchange. The tool is based on previous work undertaken in [27], [28], [29].These safeguards are tailored to the specific business procedures of the hospital and targeted towards the preservation of the data security and privacy, as well as towards security and privacy aware health data exchange. As the safeguards are uniquely proposed based on each individual healthcare organisation profile, the latter is created prior to the recommendation in order to understand: i) the functional and non-functional requirements of the organisation; ii) its risk appetite; and iii) the available budget for investing in protection. The recommendation takes into account the outcomes of the previous CUREX phases (vulnerability analysis, threat intelligence, cybersecurity and privacy risk assessment) and it uses advanced mathematical models to come up with optimal decisions. These are implemented by the Optimal Safeguards Tool (OST) which drive the decisions regarding cybersecurity and privacy countermeasures within the healthcare organisation with the end goal the organisation to comply with the GDPR Framework. Regarding privacy, the CUREX OST aids hospitals and care centres to ensure that every data process that is executed within the organization the privacy of patients' information by proposing various types of Privacy Enhancing Technologies (PETs).

3.5 Cyber Hygiene

In conjunction with optimal recommended safeguards, CUREX delivers targeted measures for raising the cyber hygiene of healthcare organisations through training and raising awareness activities, targeted towards healthcare employees on cybersecurity and privacy risks incurred during data exchange. Training involves the development of cybersecurity defending skills, e.g. empowering social engineering defences. CUREX identifies the communication and delivery channels that better suit the diverse employee groups in a healthcare organisation including newsletters, email notifications, etc. CUREX examines and assesses the existing awareness processes and material in the organisation (through its risk assessment toolkit) in order to derive best-fit training strategies that meet the learning needs of individual healthcare professional groups and match their role in the organisation.

3.6 Patient Application and Health Professional Applications

The Patient Application (PA) provides data owners the necessary control to their data, according to GDPR. The PA complements health data exchange through the CUREX Platform and its components and enables data owners (patients) to review and define the way their data is handled. The users will have the ability to intervene on the whole process when they find that their data is misused. On top of that, users will be able through the PA to review the complete transaction history regarding the exchange and the processing of their data. The Health Professional Application (HPA) is the main point for health professionals to create and validate data transactions between stakeholders and/or services, which then is stored to the PrB. When the transaction is validated by peer HPA instances across the CUREX, the relevant request is posted in the HPA instance of the hospital. Transactions initiated by HPA instances are sealed by a Smart Contract that are executed through the PrB.

3.7 Private Blockchain (PrB)

The PrB provides a decentralised database to store auditable information such as: activity into the system, risk assessment report, and the data sharing process. As an integral part of the cybersecurity and privacy toolkit, CUREX PrB is used to record: i) the cybersecurity and privacy risk scores derived by the relevant assessment methodologies, and ii) all transactions that occur between all stakeholders. Each data exchange request recorded into the blockchain includes a privacy and security risk score. This provides the essential functionality to audit the process and feed the recalculation process of the risk assessment scores. Also, as the CUREX aims at exploiting the results of relevant H2020 initiatives in the healthcare domain, the CUREX PrB is integrated to the MyHealthMyData (MHMD) project[1]. The PrB is integrated to the MHMD blockchain as a parallel channel. This gives the independency of the services in order to maintain separately the data related with the risk assessment and the data sharing process. The blockchain replication process is done by using a consensus algorithm which provides the security of the decentralized system. The CUREX-MHMD smart contracts notifies the events in both ledgers in order to allow systems to query the blockchains between each other.

[1] http://www.myhealthmydata.eu/

4 CUREX Use Cases' Overview

Three target scenarios have been identified during the proposal preparation as promising fields for the applicability of CUREX concepts. The CUREX Platform covers a variety of business cases and needs in the healthcare domain and it shapes its solutions accordingly in different cases of health data exchange. Every CUREX use case states a hypothetical sequence of actions and interactions between users (i.e. medical staff, patient, IT staff, and Administrative staff) and the system, within an environment, and related to a specific goal. A short description of each CUREX uses case can be found below:

4.1 Use Case 1: Emergency in a Foreign Country

In this use case, a patient travelling abroad visits a clinic the patient's Electronic Health Record (HER) is not available in the local country. In order to assist the physician and help provide a proper diagnosis of the patient's illness, she/he must access the CUREX Platform via HPA and get the proper authorization to retrieve the patient's EHR from her/his country of origin. The objective of this use case is the secure and private transfer of the patient's EHR to a foreign country.

4.2 Use Case 2: Data Exchange in Remote Healthcare Services

This use case tests and evaluates the CUREX platform potential impact on data exchange in remote healthcare services. The objectives of this use case are to formulate the decision mechanisms to further safeguard a given institution's infrastructure and remote devices. The use case also monitors of IoT devices and the private transfer of the patient's data, which are remote, outbounds of the health centre. The aim of this use case is split into two subcases: i) Risk Assessment for an IoT Healthcare Platform, where the patient's device shares data with the health care centre from outside of the hospital/clinic; ii) Risk Assessment for a POC System, where the patient's device shares data within the hospital/clinic.

4.3 Use case 3: Data Exchange for Healthcare Research

Use case 3, evaluates the operation of the CUREX Platform in parallel with the MHMD Platform. The Data sources selection is carried out exactly as use case 2. The MHMD platform uses blockchain technologies to rule Data exchanges between hospitals, research centres and other types of institutions, thanks to dedicated smart contracts. CUREX platform is used in each MHMD node to assess the privacy level of the data packages before to be shared (at Data Controller facilities) and once the

data has been received (at data requestor facilities) in order to evaluate if the data package is compliance with the data management policies defined by each institution. The main purpose of MHMD is to provide access to data with the consent of the data owners.

5 Conclusion

In the CUREX, protection from cyber-attacks is assisted by rigorous cybersecurity and privacy risk assessment tools and best practises to implement countermeasures and cyber hygiene. CUREX comes to deliver a novel, flexible and scalable situational awareness-oriented platform, addressing advanced cybersecurity threats, targeted at critical healthcare information infrastructures, safeguarding the privacy of patients, leveraging secure, authorised and fully auditable exchange of sensitive health data, and facilitating cyber threat situational awareness uplifting, optimal defence strategy design and cyber-risk management and mitigation through recommendation of optimal security safeguards. More precisely, CUREX delivers a cybersecurity and privacy assessment toolkit (CAT, and PAT) which performs vulnerability assessment and identify attack surfaces on data and infrastructure assets, as well as on business processes, and thus facilitates the identification of threats against healthcare services, data, and infrastructures. In conclusion, the CUREX platform provides a holistic approach for cybersecurity and privacy aware health data exchange based on three strategic impacts: i) improved security of healthcare services, data and infrastructures; ii) less risk of data privacy breaches caused by cyberattacks; iii) increased patient trust and safety.

ACKNOWLEDGMENTS

This research has been funded from the EU as part of the CUREX project (H2020-SC1-FA-DTS-2018-1 under grant agreement No 826404).

REFERENCES

[1] [Online]. Available: http://www.information-age.com/rise-cyber-attacks-financial-services-firms-123470588/ .
[2] Intel, "Healthcare Security Readiness – Global Industry Highlights," 2017.
[3] ENISA, "Cyber Security Culture in organisations," 2017.
[4] A.Panou, C.Ntantogian, C.Xenakis, "RiSKi: A Framework for Modeling Cyber Threats to Estimate Risk for Data Breach Insurance," in [illegible] Greece, 2017.
[5] N.Vavoulas, C.Xenakis, "A Quantitative Risk Analysis Approach for Deliberate Threats," in [illegible] Greece, 2010.
[6] C.Panos, C.Xenakis, P.Kotzias, I.Stavrakakis, "A specification-based intrusion detection engine for infrastructure-less networks," [illegible] vol. 54, pp. 67-83, 2014.
[7] B. Smith, M. Ashburner, et.al, "The OBO Foundry: coordinated evolution of ontologies to support biomedical data integration," [illegible] no. 25, pp. 1251-1255, 2007.
[8] B. Blobel, "Ontology driven health information systems architectures enable pHealth for empowered patients," [illegible] vol. 80, no. 2, pp. 17-25, 2011.
[9] International Standardization Organization, "ISO 31010: Risk management -- Risk assessment techniques," Geneva, Switcherland, 2009.
[10] International Standardization Organization, "ISO 31000: Risk Management – Principles and Guidelines," Geneva, Switcherland, 2009.
[11] International Standardization Organization, "ISO 27005: Information security risk management," Geneva, Switcherland, 2011.
[12] S.E.Schechter, M.D.Smith, Computer security strength and risk: A quantitative approach, Harvard University, 2004.
[13] European Network and Information Security Agency, "Inventory of Risk Management / Risk Assessment Methods," 2010.
[14] CCRA Working Group, "Common Criteria for Information Technology Security Evaluation," 2006.
[15] "Special Publication 800-30: Risk Management Guide for Information Technology Systems," National Institute of Standards and Technology, 2002.
[16] Clusif Methods Commission, "MEHARI V3 Risk Analysis Guide," 2004.
[17] R. Bojanc, B. Jerman-Blazi c, "Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System," vol. 45, p. 276–288, 2012.
[18] C. Ullrich, "Valuation of IT Investments Using Real Options Theory," [illegible] no. 5, p. 331–341, 2013.
[19] T. Sawik, "Selection of optimal countermeasure portfolio in IT security planning," [illegible] no. 55, p. 156–164, 2013.
[20] T. R. Rakes, J. K. Deane, L. Paul Rees, "IT security planning under uncertainty for high-impact events," Omega, 2012, p. 79–88.
[21] L. P. Rees, J. K. Deane, T. R. Rakes, W. H. Baker, "Decision support for Cybersecurity risk planning," [illegible] no. 51, p. 493–505, 2011.
[22] V. Viduto, C. Maple, W. Huang, D. Lopez-Perez, "A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem," [illegible] no. 53, p. 599–610, 2012.
[23] K. Renaud, W. Goucher, "Health service employees and information security policies: an uneasy partnership?," [illegible] vol. 20, no. 4, pp. 296-311, 2012.
[24] S. L. Pfleeger, M. A. Sasse, A. Furnham, "From weakest link to security hero: Transforming staff security behavior," [illegible] vol. 11, no. 4, pp. 489-510, 2014.
[25] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[26] International Standardization Organization, "ISO 27001: Information Security Management," 2013.
[27] National Institute for Standards and Technology, "NIST Cybersecurity Framework," 2014.
[28] National Institute of Standards and Technology, "Risk Management Framework for Information Systems and Organizations," 2017.
[29] A.Fieldera, E.Panaousis, P.Malacaria, C.Hankina, F.Smeraldic, "Decision support approaches for cyber security investment," [illegible] vol. 86, pp. 13-23, 2016.
[30] E.Panaousis, A.Fielder, P. Malacaria, C.Hankin, F. Smeraldi, "Cybersecurity games and investments: A decision support approach. In International Conference on Decision and Game Theory for Security," [illegible] pp. 266-286, 2014.
[31] A.Fielder, E.Panaousis, P.Malacaria, C.Hankin, F.Smeraldi, "Game theory meets information security management.," in [illegible], Berlin, Heidelberg., 2014.