UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

DIPARTIMENTO DI INFORMATICA

PhD Program in Computer Science and Mathematics
XXXIII cycle

Research Project

PhD Student: Vita Santa Barletta

Supervisor: Prof. Danilo Caivano

Coordinator: Prof. Maria F. Costabile

PhD student signature _____

Supervisor signature _____

1. Research title

Secure Project Management

2. Research area

Software Engineering: Project Management

3. Research motivation and objectives

Project Management is becoming more and more complex, especially in contexts, such as smart cities that transversely invest many technological fields and sectors of intervention. The growth in size and complexity of projects increases the criticality of the information and data processed and managed. This imposes, see for example the provisions on the subject dictated by the GDPR, "*General Data Protection Regulation*"[1], the adoption of organizational structures, processes and tools to mitigate the risks related to security and data privacy.

The problem is further exacerbated in highly computerized contexts and with reference to software development projects.

Therefore, it becomes necessary to identify the threats, vulnerabilities and risks associated with the management of projects that could directly or indirectly damage (e.g. economic, political, social, reputation) an organization or individual and, in general, project stakeholders.

According to the Project Management Institute (www.pmi.org), project management is organized along the organizational dimension - or rather knowledge areas – of processes, tools and techniques to support processes. Each of these elements must therefore be analyzed, evaluated and, if necessary, appropriately integrated and extended, conceptually and operationally, in order to assure secure project management. As so, it will be necessary to evaluate the impact of the security factor on the aforementioned dimensions:

- **Organizational**: it concerns the various organizational models and structures and, as such, acting on the operating procedures, the system of rules, technological assets, company roles, decision-making power, as well as organizational responsibility and, finally, individual responsibility, contributes to the creation of a "*secure system*".

- **Project Management Processes and Knowledge Areas**: the project life cycle is managed through the execution of various activities known as Project Management Processes and common to all industrial sectors. A series of processes, associated with a specific topic, define a knowledge area. The need of managing secure projects may require additional processes or knowledge areas.

- **Tools and techniques**: they define tools and tecniques for secure project management together with a set of guidelines and best practices (or even the bad practices that should be avoided) for addessing security in software design, development and service delivery.

The objective of this research project is the proposition and experimentation of a framework, i.e. a set of models and organizational structures, processes, tools and techniques, for secure project management.

In order to achieve this result, the following three research goals will be addressed during the PhD course:

- **Goal 1**: Analyze models and organizational structures with the purpose of evaluating/adapting them to "security" factor from PM's point of view in the context of (software) project management.

- **Goal 2**: Analyze Project Management Processes and knowledge Areas with the purpose of evaluating/adapting them to "security" factor from the PM's point of view in the context of (software) project management.

- **Goal 3**: Analyze tools and tecniques with the purpose of evaluating/adapting them to "security" factor from the PM's point of view o in the context of (software) project management.

4. State of the art

According to Project Management Institute (PMI) a project is a temporary endeavor undertaken to create a unique product, service, or result [2]:

- a unique product that can be either a component of another item, an enhancement or correction to an item, or a new end item in itself;
- a unique service or a capability to perform a service;
- a unique result, such as an outcome or document;
- a unique combination of one or more products, services, or results.

Projects are undertaken at all organizational levels. A project can involve a single individual or a group, a single organitazional unit or multiple organizational units from multiple organizations.

Effective project management helps individuals, groups, and public and private organizations to meet business objectives; satisfy stakeholder expectations; be more predictable; increase chances of success; deliver the right products at the right time; resolve problems and issues; respond to risks in a timely manner; optimize the use of organizational resources; identify, recover, or terminate failing projects; manage constraints (e.g., scope, quality, schedule, costs, resources); balance the influence of constraints on the project (e.g., increased scope may increase cost or schedule); manage change in a better manner.

Within the software context, projects drive change in organizations, and usually impact on a huge amont of data and information. Thus for a succesful project management, it is particularly important, independently from the size of the organization, to stress concepts such as data and information security in project activities which deal with or target integrity, availability, and confidentiality [1].

From an ***organizational point of view***, an organization can either incorporate security guidance into its general project management processes or react offhand to security failure. Moreover it is increasingly difficult to respond to new threats by simply adding new security controls to the already existing ones. There are many non-technical components that are just as essential to an integrated and effective secure environment as the latest firewall or anti-virus application, such as employee training, data breach insurance, policies and procedures, and more. The technical and non-technical components should be included in the organization and managed as integrated projects.

Saleh [3] narrows the gap between theory and practice for information security management by following the process of a security maturity model and by identifying the benefits of implementing a standard for security needs of an organization. This approach, if developed without an understanding of the organizational culture, will impact the effectiveness of the implementation as well as human reaction to the adoption of new technologies. Organizational culture often hinders the success of this approach and the delivery of the intended benefits concerning the implemented security model or standard.

Furthermore, the success factors in addressing security in software project management it is not simply a technological matter. The adoption of the latest and most costly technology is often less effective than a good organization.

By balancing investments from less rewarding technologies into these breakthrough innovation areas, organizations could improve the effectiveness of their security project. For example two enabling security technology areas identified as “Extensive use of cyber analytics and User Behavior Analytics” and “Automation, orchestration and machine learning” [4] were the lowest ranked technologies for enterprise-wide deployment, 32% and 28% respectively, and yet they provided the third and fourth highest cost savings for security technologies.

Security can be considered part of the larger Cost of Quality of a project [5]. Since security vulnerabilities are continuously evolving, it is difficult to quantify rates of occurrence. It is also difficult to estimate the damage to asset value that would be done in a single loss occurrence.

For organizations moving to make security a higher priority, project managers need to address how that change affects the following [6]: requirements and scope the technical plan; project life cycle (deliverables and sequencing of deliverables); activities required to complete deliverables resources; skills needed, duration of resource requirements; other related estimates such as size and defects project and product risks.

According to ISO 27001[7], information security can be integrated into project management activities in several ways:

- Include information security objectives in project objectives.
- Perform a risk assessment in an early stage of the project.
- Carry out treatment of the identified risks and implement security measures.
- Make the information security policy an indispensable part of all stages of the project.

Therefore “security” affects many things during project life cicle.

Technically speaking [2], Project Management can be decomposed along two different dimensions: ***Project Management Process Groups and Knowledge Areas***.

Project management processes are organized in "Groups" by grouping all the processess logically linked by the outputs they produce, where the output of one process generally results in either an input to another process, or a deliverable of the project or project phase. The processes are also categorized by Knowledge Areas where a knowledge area is an identified area of project management defined by its knowledge requirements and described in terms of its component processes, practices, inputs, outputs, tools, and techniques. This result in the so called PMBOK MATRIX where PMBOK stand for Project Management Body Of Knowledge [2].

Knowledge Areas	Project Management Process Groups				
	Initiating Process Group	Planning Process Group	Executing Process Group	Monitoring and Controlling Process Group	Closing Process Group
Project Integration Management	4.1 Develop Project Charter	4.2 Develop Project Management Plan	4.3 Direct and Manage Project Work 4.4 Manage Project Knowledge	4.5 Monitor and Control Project Work 4.6 Perform Integrated Change Control	4.7 Close Project or Phase
Project Scope Management		5.1 Plan Scope Management 5.2 Collect Requirements 5.3 Define Scope 5.4 Create WBS		5.5 Validate Scope 5.6 Control Scope	
Project Schedule Management		6.1 Plan Schedule Management 6.2 Define Activities 6.3 Sequence Activities 6.4 Estimate Activity Durations 6.5 Develop Schedule		6.6 Control Schedule	
Project Cost Management		7.1 Plan Cost Management 7.2 Estimate Costs 7.3 Determine Budget		7.4 Control Costs	
Project Quality Management		8.1 Plan Quality Management	8.2 Manage Quality	8.3 Control Quality	
Project Resource Management		9.1 Plan Resource Management 9.2 Estimate Activity Resources	9.3 Acquire Resources 9.4 Develop Team 9.5 Manage Team	9.6 Control Resources	
Project Communications Management		10.1 Plan Communications Management	10.2 Manage Communications	10.3 Monitor Communications	
Project Risk Management		11.1 Plan Risk Management 11.2 Identify Risks 11.3 Perform Qualitative Risk Analysis 11.4 Perform Quantitative Risk Analysis 11.5 Plan Risk Responses	11.6 Implement Risk Responses	11.7 Monitor Risks	
Project Procurement Management		12.1 Plan Procurement Management	12.2 Conduct Procurements	12.3 Control Procurements	
Project Stakeholder Management	13.1 Identify Stakeholders	13.2 Plan Stakeholder Engagement	13.3 Manage Stakeholder Engagement	13.4 Monitor Stakeholder Engagement	

Fig. 1: Project Management Process Group and Knowledge Area Mapping

According to [6] the following knowledge areas are strongly influenced by security: scope, resource, communication, risk, procurement, quality, and integration. Thus they need to evolve

toward a secure management. For example, security's impact on scope has several dimensions: the scope is influenced by the type and number of threats, by the sophistication and resources available to the attacker, by the desired response to an attack, and by the level of assurance required that the system meets its security requirements.

Another critical issue is "Data Breach" in software intensive companies where software projects are numerous and frequent [8]. A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data Breach is a complex affair often involving some combination of human factors, hardware devices, exploited configurations or malicious software. As it can be expected, data breach response activities (investigation, containment, eradication, notification, and recovery) are proportionately complex. These response activities, and the lingering post-breach aftereffects, are not just an IT security problem. They are an enterprise problem involving legal counsel, human resources, corporate communications and other incident response stakeholders. Each of these stakeholders brings a slightly different perspective to the breach response effort. By ingraining security practices in every phase of a project, project managers have the opportunity to deliver more secure systems in a more secure and deterministic manner [9].

Software projects require special attention for what concerns confidentiality, especially if it pursues strategic business goals [10]. In general IT projects imply that the documentation produced frequently includes intimate details of network and system architectures that presents an attractive target for industrial espionage and hackers. Failed changes to IT systems can also impact availability and integrity.

For what concerns ***the use of tools and techniques*** for a more secure project management, several strategies can be followed. The use of backups and back-out plans togheter with security risks assessment early in the project is one of them. It has a strong impact on project success instead of reacting offhand to an unexpected risk occurrence that may cause systems to go down, or cause data loss, corruption or breach [11].

According to Gartner [12] 75% of the attacks are directed directly to applications as they provide an easy path to compromise systems or launch further malware attacks. Thus considerable attention has been paid to incorporating security best practices into the software development life-cycle, i.e. security "baked-in" to code by various means, also if a large number of IT projects are not only software development projects [13].

The software architecture describes the system structure in terms of components and specified interactions. Currently several types of software architectures are avalilable, ranging from client-server to mobile applicatons passing through the web ones, each characterized by different security levels, risk exposure and threats. Only an architectural overall risk assessment can addresses the available solutions and contribute to risks mitigation. Unfortunately, operating system level approaches, network level approaches and machine level approaches are not enough for guaranteeing overall security of a software system. External protective and proactive measures against existing treaths are also needed [14].

Threat modeling is a technique used to model threats into software systems [15,16]. By applying threat modeling during the early stages of the software development life cycle, several threats can be identified and mitigated resulting in a more secure software system. Another strategy is to use

agile processes in order to realize a continuous risk analysis and security check, or to adopt agile practices such as Pair Programming. Indeed, for very sensitive code segments, security governance may require that changes always be made by two developers to limit the chance that an individual inserts malicious code [17].

Data Privacy in a software system can be compromised due to an architectural flaw or mismatch. Privacy by Design has emerged as a proactive, integrative and creative approach to reinforce privacy requirements in the early stages of application design [18]. Gürses [19] identifies three privacy research paradigms: Privacy as Confidentiality (Hiding); Privacy as Control (Informational Self-determination); Privacy as Practice (Identity Construction). Among the challenges associated with the privacy by design is the lack of holistic, systematic and integrative methodologies that address the complexity and variability of privacy and support the translation of its fundamental principles in engineering activities and software architecture. An emerging research direction in this sense is related to the identification and use of Privacy Design Pattern [20]

To addresses Privacy by Design, a discipline named Privacy Engineering has emerged [21]. It aims to apply engineering principles and processes in the development, implementation and maintenance of systems, in a systematic and repeatable way, to reach an acceptable level of privacy protection. Privacy by Design intends to explain "What to do?" to achieve an adequate level of privacy protection, while Privacy Engineering intends to explain "How to do it?" by defining privacy as a quality attribute in systems engineering.

5. Problem approach

The research project implies the resolution of problems ranging from the definition/evolution of appropriate models and paradigms among those proposed by the scientific and industrial communities, up to the research, identification and/or definition of new organizational structures, processes, guidelines and best practices necessary to strengthen such models and paradigms. For these reasons, the project will be organized in major phases (PH) that will cover the entire life cycle of the innovation process as summarized below:

- **PH.1: Context analysis**. Contextualization of the topics of interest with reference to the world of research and the marketplace. It is important to assess the real state of progress of research in such areas, to select useful contributions and, at the same time, to identify the tools and solutions already available to bring research results into the operational field. Some of the research results and tools already available will be directly usable and others will require appropriate extensions, testing and adaptations. Furthermore, there may be aspects which will not be immediately addressed as primary topics in the current methodological/technological offer and will therefore be developed during the later stages of the PhD course. At the end, of this stage we will have the exact perception of the tools and techniques, processes as well as organizational structures to be used in the research project. During this step approaches such as Systemati Mapping Study and Systemati Literature Review will be planned and carried out to point out the current state of art of the literature and point out current research gaps to address during the PhD proposal.

- **PH.2: Innovation Proposition**. Definition, formalization and specialization of the proposed approach. During this step, the extensions and evolutions needed to the organizational, process and knowledge areas and tools and techniques layers will be proposed. In the absence of reference methods and tools to be adapted, we will proceed to the design the new ones. Therefore, at the end of this phase, based on the research gap outlined at the end of the context analysis, we will formally propose a a theoretical framework to be implemented in the next phases.

- **PH.3: Innovations Development**. Development of demonstrators and prototypes to support the use of the framework in real context, also useful to be used for empirically validating the underlying innovations.

- **PH.4: Experimentation, analysis and interpretation of the experimental data**: in order to qualitatively and quantitatively verify the benefits deriving from the use of the proposed framework, empirical investigations will be designed and executed. For this intent a quality model and the experimental design will be definied across multiple and different experimental sites. The main goal of this phase is to verify the cause-effect relationship between the use of the proposed framewok and the expected benefits in the light of the three main research goals outlined in the previous sections.

- **PH.5: Generalization of the results and innovations.** The obtained results will be generalized and formalized in order to be transferable to the target community and generate relevant spillover effect.

6. Expected results

The research plan aims to achieve the definition of a framework that guarantees secure project management of software projects made of:

- organizational structures;
- project management processes and knowledge area;
- tools and techniques.

Special attention will be paid in order to make the framework usable and flexible with respect to small to medium enterprises and startups that are often targeted for their breakthrough technology.

7. Phases of the project

The research will cover a 3 year plan and will be organized in the following phases (**PH**) and activities:

First year

- **PH.1: Context analysis.**

  The purpose of this WP is to contextualize the project initiative with respect to the research community.

- Activity 1.1: Literature Review.
- Activity 1.2: Analysis of the state of the practice.

  This step involves the analysis of tools and procedures that are of interest both in terms of maturity and stage of evolution for practical use in industrial contexts.
- Activity 1.3: Close examination of the issues related to project management techniques.
- Activity 1.4: Research and study of methodologies for the analysis and secure project management.
- Activity 1.5: Participation in international schools related to the research topic.

Second year

- **PH.2: Innovation Proposition**

The goal of WP is to define a framework for secure project management according to the following three problem dimensions:

- Activity 2.1: Definition of an *organizational model and structure* for secure project management.
- Activity 2.2: Definition of *processes and knowledge areas* for secure project management.
- Activity 2.3: Definition of *tools and tecniques* for secure project management.

- **PH.3: Development of innovations**

In this WP, the framework defined (organizational structure, processes and knowledge areas, tools and techniques) in the WP2 will be automated through demonstrators and prototypes:

- Activity 3.1: Document template and operational guidelines for secure project management.
- Activity 3.2: Prototype of tools and tecniques for the secure project management.

Third year

- **PH.4: Experimentation, analysis and interpretation of data obtained**

In this WP the empirical study for framework validation will be designed and executed.

- Activity 4.1: Experiment design.
- Activity 4.2: Experiment Execution.
- Activity 4.3: Experimental data collection, analysis and improvement .

- **PH.5: Generalization of the result and innovation**
  - Activity 5.1: PhD thesis production.

8. Result evaluation

The research project outlined in this proposal includes three main Research Goals. They will be addressed and validated through various types of empirical investigations. In order to obtain proof of evidence, goals will be validated both *individually*, with focus on either of the three specific dimensions discussed above (organizational structures; project management processes and knowledge area; tools and techniques) as well as altogether to prove their interdependencies and relations

Furthermore, empirical validation will be planned and carried out in experimental sites ranging from laboratory and controlled contexts (in-vitro) to real, field contexts (in-vivo) such as software companies.

In order to collect evidence, we will adopt both qualitative and quantitative analysis techniques.

Qualitative Analysis techniques have the main objective of interpreting evidence to reach new theoretical or conceptual level of understanting. Qualitative techniques are based on re-interpretation and re-analysis of text forms of evidence (eg. collected from surveys, focus groups, interviews either structured or semistructured, questionnaries, published literature). The Fig. 2 below represents the main steps of the synthesis process that will be adopted.

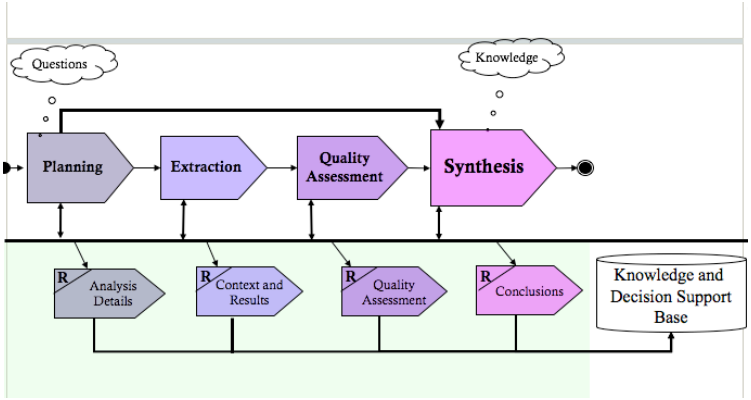

Fig. 2: Synthesis Process adopted

Planned studies will be surveys, focus groups or interviews carried out with the participation of SME project managers. Data will be collected and synthesized. Generally speaking, qualitative synthesis comprises the identification of the main, recurrent or most important theme arising in a body of evidence (eg. survey, focus group, interview or literature). It is a method used for identifying, grouping and summarizing findings from included studies. Morevoer, it will allow to identify, analyze, and report patterns (themes) within data collected (Fig. 3).

Qualitative synthesis will be structured according to the following steps: (i) Extract data: Essential text and data from the primary studies are obtained in an explicit and consistent way according to a defined extraction strategy: (ii) Identify Codes: Codes are descriptive labels that are applied to segments of text in each study. It is necessary to examinate and organize the data contained in each source of the synthesis. (iii) Extract Themes: A theme describes and organizes possible observations into a category or “meaningful whole”. (iv) Model making: define the model from the previously extracted themes.

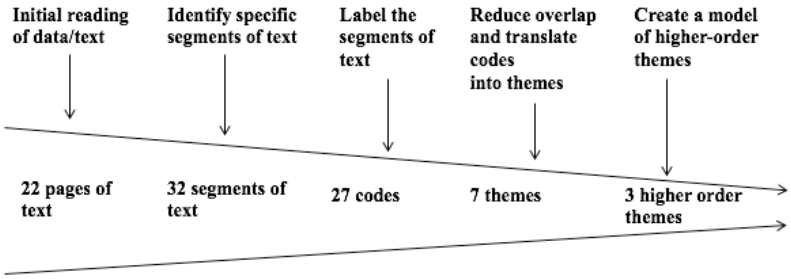

Fig. 3 - Themes extraction in qualitative synthesis

Quantitative Analysis techniques, mainly focuse on aggregating evidence to reach statistical conclusions. The Fig. 4 summarizes the types of quantitative empirical research that will be involved.

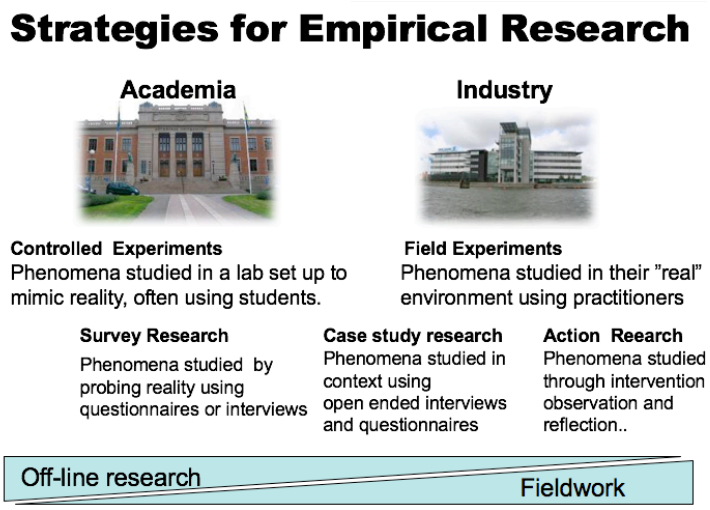

Fig. 4 - Quantitative Empirical Research

In general, various types of strategies will be used depending on the context. First, studies will range from more controlled ones, carried out in a laboratory (in-vivo) where all variables can be set, modified and monitored. Here subjects such as students can also be involved. Second, case study and field experiments, as well as action research will be carried out in a real environment (in-vivo). These studies will involve industrial partners that will provide real projects, data, and subjects such as practitioners, project managers, developers, etc. Moreover, they are important as they will provide a proof environment for the innovations developed during the PhD proposal.

9. Possible reference persons external to the department

According to goal research, reference external to the department are:

- Dr. Domenico Raguseo, IBM Security - Manager of Europe Security Technical Sales and Solutions
- Dr. Paola Mosca, President of Project Management Institute Southern Italy Chapter

- Dr. Roberto Mignemi, OmnitechIT - Strategic Consulting, including business plan & sales strategy development
- Dr. Gennaro Del Campo, Ser&Practices S.r.l. - Infrastructure and Service Delivery Manager
- Prof. Mario Piattini, University Castilla-La Mancha, Spain
- Prof. Corrado Aaron Visaggio, University of Sannio

10. References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
2. Project Management Institute: A Guide to the Project Management Body of Knowledge. 6nd Edition, (2017)
3. Malik F. Saleh, Information Security: Maturity Model. International Journal of Computer Science and Security (IJCSS), Volume (5): 2011
4. Accenture: Cost of Cyber Crime Study. Insights on the security investments that make a difference. (2017)
5. Xie, N., & Mead, N. SQUARE: Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies (CMU/SEI-2004-TN- 045). Retrieved May 28, 2013, from the Software Engineering Institute, Carnegie Mellon. (2004)
6. Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead: Software Security Engineering: A Guide for Project Managers, 1st Edition. (2008)
7. Alan Calder: The Case For ISO 27100:2013 2nd Edition, IT Governance Publishing
8. Verizon: 2017 Data Breach Investigations Report (2017)
9. Agenzia per l'Italia Digitale: Linee guida per l'adozione di un ciclo di sviluppo di software sicuro (2017)
10. Agenzia per l'Italia Digitale: Linee guida per lo sviluppo di software sicuro. (2017)
11. Agenzia per l'Italia Digitale: Linee guida per la configurazione per adeguare la sicurezza del software sicuro (2017)
12. Gartner: www.gartner.com, Last access on January 10, 2018
13. Agenzia per l'Italia Digitale: Linee guida per la modellazione delle minacce ed inividuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by design (2017)
14. Singh, A.A. & Singh, K.S.: Network ThreatRatings in Conventional DREAD Model Using Fuzzy Logic. International Journal of Computer Issues, 9(1), pp.1694–0814. (2012)

15. Hussain, S., H. Erwin and P. Dunne: Threat modeling using formal methods: A new approach to develop secure web applications. Proceeding of 7th International Conference on Emerging Technologies (ICET), pp: 1-5. (2011)
16. Sodiya, A.S., Onashoga, S.A. &Oladunjoye, B.A.: Threat modeling using fuzzy logic paradigm. Informing Science: International Journal of an Emerging Transdiscipline, 4(1), pp.53–61. (2007)
17. Singhal, A.: Development of Agile Security Framework Using a Hybrid Technique for Requirements Elicitation. Advances in Computing, Communication and Control, pp.178–188. (2011)
18. Cavoukian, A., "Privacy by Design: The 7 Foundational Principles," (2010)
19. Fahriye Seda Gürses. Multilateral privacy requirements analysis in online social network services. PhD thesis, Department of Computer Science, KU Leuven, 2010.
20. Theeraporn Suphakul, Twittie Senivongse: Development of Privacy Design Patterns Based on Privacy Principles and UML, 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD) (2017)
21. National Institute of Standards and Technology. NIST:https://www.nist.gov, Last access on January 13, 2018