Categorization of Standards, Guidelines and Tools for Secure System Design for Critical Infrastructure IT in the Cloud

Sarita Paudel, Markus Tauber, Christian Wagner, Aleksandar Hudic
Austrian Institute of Technology
Vienna, Austria
{*sarita.paudel, markus.tauber, christian.wagner, aleksandar.hudic*}*@ait.ac.at*

Wee-Keong Ng
Nanyang Technological University
Singapore
awkng@ntu.edu.sg

***Abstract*—With the increasing popularity of cloud computing, security in cloud-based applications is gaining awareness and is regarded as one of the most crucial factors for the long-term success of such applications. Despite all benefits of cloud computing, its fate lies in its success in gaining trust from its users achieved by ensuring cloud services being built in a safe and secure manner. This work evaluates existing security standards and tools for creating Critical Infrastructure (CI) services in cloud environments – often implemented as cyber-physical systems (CPS). We also identify security issues from a literature review and from a show case analysis. Furthermore, we analyse and evaluate how mitigation options for identified open security issues for CI in the cloud point to individual aspects of standards and guidelines to support the creation of secure CPS/CI in the cloud. Additionally, we presented the results in a multidimensional taxonomy based on the mapping of the issues and the standards and tools. We show which areas require the attention as they are currently not covered completely by existing standards, guidelines and tools.**

***Keywords*-security-engineering; secure software development; critical infrastructure; CPS**

I. Introduction

Cyber-physical systems (CPSs) are smart systems that nowadays often form the foundation of critical infrastructure [1]. They promise increased efficiency and interaction between computer networks and the physical world enabling advances that improve the quality of life, including advances such as in personalized health care, utilities and even traffic control and public safety CCTV systems[1]. It will have a revolutionary and pervasive impact on future manufacturing, national security, transportation, energy networks, infrastructure and healthcare.

The increasing flexibility and unpredictable usage patterns of such utilities makes the cloud an attractive solution for implementing them. However, this exposes CI (which historically were built as isolated systems) to cyber-risks. This results in a demand for building such system with protection against cyber-attacks in mind, even more than traditional IT systems as failing CI may have a cascading effect on each other and hence fatal effects[2].

[1]Related issues are investigated in SEcure Cloud computing for CRitical infrastructure IT (SECCRIT) which supports this work. For more information see www.seccrit.eu

Existing secure software development standards and tools are applicable in different context (focusing mainly on traditional IT systems) and help us to address the open security issues. Choosing the appropriate software security standards and tools for a CI/CPS context will help us to overcome the above mentioned problems. Thus, based on previous work [3], and in detail [4] we investigate on *i) identifying security issues in the cloud in the context of CI, ii) mapping of the security issues; to how secure software development and system engineering standards and tools can support mitigation, iii) defining a multidimensional taxonomy of the identified issues pointing to the secure software development means, and iv) evaluating the applicability of the standards and tools to CI (i.e. Cyber Physical Systems)*.

Our research approach can be categorized as a fact-finding empirical study, where we derive the facts based on our literature review. We conduct the research in three phases, Figure 1 is the graphical representation of these phases. i) *Problem Analysis* - We conduct a literature survey and implement an example CI-cloud application. The goal is to get an overview of available standards and tools, and identifying a list of cloud security issues from literature survey. ii) *Generalization and Interpretation* - We study most popular secure software development standards and tools, classify and categorize them, and map them to the identified security issues. Mapping is presented in a multidimensional taxonomy. iii) *Validation of results* - We select an available standard from the taxonomy, evaluate the taxonomy based on the standard and experiment with our show case [4]. Output of our work will help software developers, cloud providers, CI providers and other stakeholders to select the right software security standards and tools to build secure cloud applications in the CI domain.

This paper is structured as follows: in Section II, we discuss the related work, Section III describes security issues in CI and cloud, Section IV describes some existing popular security standards and tools, and their applicability in the context of CI, Section V describes mapping of security issues and security standards and tools, and Section VI describes validation of the mapping. Our conclusions are presented in Section VII.

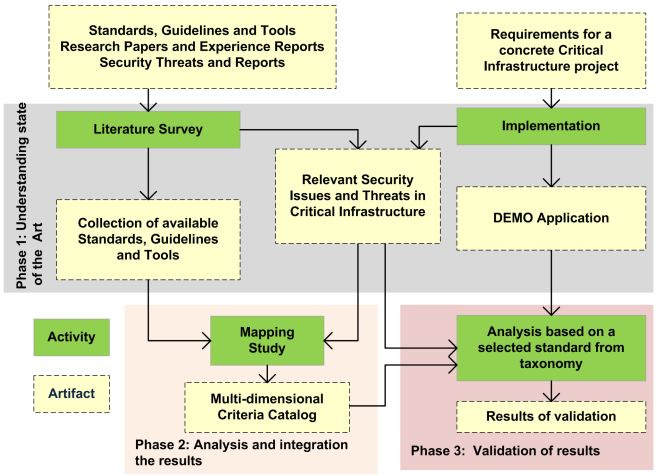

Figure 1. Overview of research approach– depicting the three phases and the activities in the different phases.

II. Related Work

In this Section, we discuss the existing body of research that has been conducted on security issues of the cloud in the context of CI. We found many contributions discussing security requirements, assessing and developing a taxonomy to select appropriate means for secure software development process and implementing standards to build secure software. However, most of the existing approaches do not address issues related to CI and those which do, do not provide any guidelines to select appropriate software security standards, guidelines and tools. We therefore base our work on these existing approaches to select appropriate means for secure software development and systems engineering focusing on Critical Infrastructure IT in the cloud.

A. Security Requirements and Assessment

Youchan Zhu et.al. [5] analyze the research status of security in the cloud and provide the three-layer (application, transport and database) security solution. The authors report that the abuse of cloud computing resources and environment security are the common security problems in the cloud. Our approach also reports some open security issues but focuses in CI and the applicability of security standards and tools. Kui Ren et.al. [6] outline various critical security challenges such as data service outsourcing security, computation outsourcing security, access control, trustworthy service metering, and motivate for further investigation of security solutions by pointing out their importance. Our approach is focused to motivate for further investigation of security standards, guidelines and tools and their applicability in the context of CI.

ENISA generalizes security issues of cloud computing from Critical Information Infrastructure Protection (CIIP) perspective [7]. Additionally, authors discuss the risk assessment and security measures related with CIIP. Although our work is closely related with the work from ENISA, we are more focused on outlining open issues of running CI services in the cloud.

Abbadi et.al. [1] discussed major security challanges and requirements related with untrusted cloud infrastructure towards a more secure and trustworthy Cloud infrastructures, e.g Critical infrastructures. Our work focuses not only on the issues related with CI but also on investigates the applicability of the state of the art security standards and tools in the CI domain.
Similarly, Younis et.al. [8] explore security issues of secure cloud computing for CI Providers and investigate security requirements for the CI providers. At the moment there is no existing work addressing these open issues while developing secure software in the cloud in CI context. Therefore we want to bridge this gap by addressing the issues in the development of secure cloud applications in CI context.

B. Classification of Secure Development Means

Futcher et.al. [9] provide guidelines and best practices for secure software development. Authors discuss and evaluate variety of guidelines and best practices by classifying them as follows: i) security standards and best practices (e.g. ISO/IEC 27002, ISO/IEC 27001), and ii) software development standards and best practices (e.g. Security Development Lifecycle-SDL [10], Common Criteria-CC [11]), and propose a set of guidelines for secure software development. Our state of the art analysis of standards, guidelines and tools secure software development is closely related with the Futcher et.al work, however we are addressing issues more specific to the CI. Therefore, we categorize our work as folllows: i) standards to security and software development standards, and ii) guidelines and tools to security and software development guidelines and iii)tools. We however consider this as subcategories for a) standards and b) guidelines (see later). Reason for this is that in CI specific areas explicitly require standardized approaches where others don't.

Yu et.al. [12] propose a methodology for characterization and classification of workflow management systems. Authors also present a survey of existing workflow systems. It motivates our approach in classification and mapping. Our work will be in the applicability of security standards and tools in the context of CI.
Similarly, Dukaric et.al. [13] propose a unified taxonomy and an Infrastructure as a Service (IaaS) architectural framework. Furthermore, the authors use the proposed taxonomy and framework for evaluating different IaaS architectures.

It motivates us to develop and map a taxonomy, but we however develop a taxonomy based on the identified security issues and security requirements in CI to point out different existing security standards and tools supporting CI.

C. Implementing software development standards

Razzazi et.al. [14] design and implement the Evaluation Process Management Software for security evaluation. To

evaluate IT products using CC, authors describe the roles of developers, evaluators and administrators and their activities in the evaluation process. Additionally, they also present the flow of the evaluation process. However, in our case we address those standards relevant to the CI domain.

Johns et.al. [15] analyze underlying mechanisms of vulnerabilities and propose an approach for secure code generation providing strict separation between data and code. This related work is focusing on general Web applications. However, our approach will be focused more on applications for cloud environments and we will be developing taxonomy for secure code generation and security standards in CI context.

III. Security Issues in CI and Cloud

To comprehend the challenges from the developer's perspective, we address the show case of a Cloud application in the context of critical infrastructures, by identifying the most relevant cloud security issues through the literature research and the show case analysis. In this Section we present the list of identified security issues and relate the list towards the cloud security threats according to their types [16] i) technical, ii) contractual, iii) jurisdictional, and iv) organizational (documented in [4]) and provide an indication of impacted security aspects.

A. Data Security

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to e.g. computers, databases and websites.

1) Data Storage: Data of cloud applications are stored in a cloud storage server where the users can access and update data frequently, so correct dynamic data update is of high importance. Data storage protection methods e.g., redaction, truncation, obfuscation have to be considered in the cloud [17], [18], [19]. Integrity and availability of data must be guaranteed, which influences the quality of service. Data storage security is a technical threat and caused if cloud applications are not able to meet availability and confidentiality of information.

2) Data Breaches or Leakage: Sensitive internal data of an organization can fall into wrong hands while storing, transferring, processing or auditing it. Offline backups of data should reduce the impact of a catastrophic data loss but they also increase the probability data breaches if the backups are not secured properly. Interception of data between the customer and the cloud provider leads to data leakage to a third party [20], [21], [22]. Interception of data between the customer and the cloud provider leads to data leakage to third party, which is a technical threat created due to the violation of confidentiality.

3) Data Loss: In order to prevent major data losses by natural disasters such as fire or earthquake,internal data losses occurred by accident or intentionally cloud providers should take adequate measures to backup data. Also, if a customer uploads encrypted data in the cloud and loses the encryption key then in this case data will be lost [20]. Data loss is a technical threat violating the availability security objective.

4) Data Scavenging: Unfortunately data cannot easily be deleted from the storage devices, and therefore could be recovered from the hardware or using other techniques [21]. Therefore often required to physically destroy the storage device. It is a technical threat and causes the violation of confidentiality.

B. Transmission Security or Network Security

Due to the possibilities of information sniffing, spoofing, hijacking during the transmission phase data encryption and communication over secure channels are important with respect to security [17], [18]. One distinctive aspect from traditional IT systems is that CI IT services are often built on very simple network devices. Therefore, the integration of CI services with the cloud requires the assurance of secure transmission. This is a technical threat that occurs due to the violation of confidentiality.

C. Application Security

Applications can be protected from threats using software, hardware and procedural methods. Security built into applications mitigates the security vulnerabilities and therefore reducing the malicious attacks on the application infrastructure.

Attackers are turning their attention to the common weaknesses created by application developers such as cross site scripting, malicious file execution, injection flaws attacks which are possible in the Internet [18], [19]. Consideration of countermeasures to the possible attacks helps to mitigate the attacks. It is a technical threat which can be caused due to weaknesses of confidentiality or integrity and can result in problems of the availability of the regarding services.

D. Virtual Machine Security

1) Creation Security: An attacker who has a valid account could create a VM containing malicious code such as a trojan horse and store it in the providers repository [21]. When virtual machines run overtime and cannot be managed by administrators this it is called VM Sprawl. Potentially VM Sprawl can overuse the resources resulting the infrastructure costs to increase. This happens when VMs are created without proper procedures or control of the release of these VMs. It is a technical threat that violates multiparty trust security objective.

2) Isolation Security: Typically, several VMs run on a common platform. If VMs on a platform are not strictly isolated, a user of a VM could access other VMs and access sensitive information [1]. VM hopping happens when a VM is able to gain access to another VM (e.g., by exploiting some hypervisor [1] vulnerability) [21]. Failure of separating

storage, memory and routing effectively causes isolation failure [22]. This is also a technical threat and its occurrence exposes confidentiality.

3) Execution Security: The execution environment of each VM must be secured to be able to process sensitive data [1]. Assurance of execution environment should be provided while communicating messages across. It is a technical threat that is violating multiparty trust.

4) Migration Security: Live migration of VMs can potentially expose the content of a VM. Therefore giving the opportunity to an attackers to access the data, transfer the VM to an untrusted host or create and migrate several VMs and therefore causing disruptions and denial of service (DoS) [21]. This technical threat for live migration of VMs exposes a confidentiality issues in the cloud environments.

E. Insiders Security

Insiders are employees that are able maliciously misuse their rights and privileges to gain access inside of theorganisations IT infrastructure [1], [22]. Therefore, also affecting confidentiality, integrity or availability of internal information and processes. For example a cloud system administrator can delete virtual machines, temper data, provide denail of services inside his organization. Cloud hardware supplier are able can copy the sensitve content of VM images and share or sell it to the competitor organization. Lack of transparency related with process, access to virtual assets by employees, and employees roles and responsibilities are the main cause of users being reluctant to migrate towards the cloud due to the potential security issues [8].

F. Interfaces and APIs Security

Interfaces used for management and interaction of cloud services is commonly directly exposed to the outside world. Therefore, these exposed interfaces require high attention in respect security and standardization to mitigate and prevent potential malicious attacks. Availability the services hosted in cloud highly depend on the security these APIs [20]. Cloud service providers depend upon APIs to deliver services to their customers. Thus, APIs have to ensure that mechanisms like secure authentication, encryption, activity monitoring mechanisms and access control are working efficiently [8].

G. Shared Resources Security

Cloud service providers provide scalable services by sharing infrastructure, platforms and applications [20]. Most of the components are not designed for sharing resources in the cloud [8]. These components (e.g., CPU caches, GPU, etc.) of shared infrastructures are not designed to offer strong isolation for IaaS, PaaS, and SaaS. Single failure or misconfiguration can lead across an entire providers cloud [20]. Therefore, a defensive strategy in regard to compute, storage, network, and application is required. It is a technical threat related to the usability of the cloud environment and cloud resources or applications.

H. Cloud Integrity Security

When a user requests a service implementation then the cloud system determines a free-to-use instance of the requested type and address for accessing the new instance and communicate it back to the user. For this identification purpose, it requires metadata on service implementation modules. These metadata should be stored outside the cloud to maintain the correct association of service implementation instances and metadata [18]. The CI metadata is important for billing and provision of basic needs but it also allows identifying the behavioral patterns. It is a technical threat to information integrity.

I. Security related to Third Party

A Trusted Third Party (TTP) [17], [18] establishes secure interaction with two parties (where both of rely trust on the third party) and provides end-to-end security services (based on security standards and tools) within the cloud. All critical transactions between the two parties are reviewed and ensured by the TTP. Data held by the third party is often complex and lacks control and transparency. Therefore, the third party requires assurance of confidentiality being met, client and server authentication, certificate-based authorization and creation of security domain. It is a mutual auditability threat that can potentially create weakness in multiparty trust.

J. Harmonization of Security Policies between Cloud Layers and Cloud Providers

Self-automated services often have dependencies among multiple layers or sub-layers inside the cloud infrastructure. Therefore, agreement of policies that governs interaction of such layer with other layers are to be considered [1]. This is a technical threat and it occurs due to the violation of multiparty trust security in the cloud.

K. Hypervisor Security

A hypervisor [1] is a piece of software or hardware that creates and runs multiple VMs. Clouda dministrator having access to the hypervisor has the ability to access memory and temper data of VMs. The VM privilege escalation threat is designed to exploit the hypervisor in order to take control of the underlying infrastructure [21]. Due to the possibility of such threats hypervisor should be monitored and secured. This technical threat is related directly with the confidentiality and integrity of information in a VM.

L. Account Security

Hijacking an account happens by social engineering or weak credentials [21]. By accessing user's credentials attackers can access and manipulate sensitive data, and redirect any transaction. Attack methods such as phishing, fraud and exploitation of software vulnerabilities are used to get credentials and passwords [20]. After getting credentials attackers eavesdrop real user's activities and transactions, manipulate data, return falsified information and redirects

clients to illegitimate sites. It is a technical threat related to confidentiality of credentials.

M. Cloud Service Security

Due to the ability of an attacker to consume more resources that can result as a DoS or DDoS, users can be prevented to access service or experience system slowdown when Dos or DDos occurs. Attackers that are impersonating users may misuse cloud infrastructure for malicious purposes. For example, it takes years to crack an encryption key using limited hardware but using an array of cloud servers, it might be possible to crack in some minutes. Attackers can potentially stage a DDoS attack by distributing pirated software using an array of cloud servers. Attackers access critical areas of deployed cloud computing services with the stolen credentials and compromise confidentiality, integrity and availability of the services [20]. Service hijacking threat could happen when attackers hack a website hosted in a cloud service provider, install their software and control the cloud provider infrastructure [8]. It is a contractual threat related to information confidentiality, integrity and availability.

IV. SOFTWARE SECURITY STANDARDS AND TOOLS

Many software security standards, guidelines and tools are available to develop secure software. Implementing these software security standards and guidelines helps us to ensure the security of a software. However available secure software development guidelines and standards are often used in different context. Therefore, we have to implement appropriate security standards, guidelines or tools to identify and mitigate security issues related with Critical infrastructures. Therefore we are motivated to evaluate these secure software development gudielines and standards, and classify them as following *i)* Standards and *ii)* Guidelines and Tools and further sub-categorize them to i) Security Engineering and ii) Software Development.

A. Standards

A standard is an established norm in a form of a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that products, processes and services are aligned with theri technical requirements. Standards that provide guidelines and techniques for ensuring security to minimize attacks in an application are called security standards. Security standards that address security techniques for minimizing the number of cyber-security attacks are known as cyber-security standards. Standards are strict and do not change often and certification of these standards helps to get assurance as well. There are different types of international standards available. The popular standards we consider on our study are i) International Organization for Standardization - ISO standards , ii) International Electrotechnical Commission - IEC standards, iii) ISO/IEC standards (e.g.,ISO/IEC - Information technology Security techniques - Information security management systems - Requirements 27001:2005 [23], [24], ISO/IEC 27002:2005 - Information Technology - Security Techniques - Code of practice for information security management [25]), iv) Common Criteria - CC [11], and v) Security Development Lifecycle - SDL [10], [26].

B. Guidelines and Tools

A guideline is a document that provides best practices for addressing or tackling technical or non technical challenges, e.g. help to secure IT products. Furthermore, guidelines also provide the security requirements, specifications that can be used to ensure products. Both guidelines and standards are able to address variety of domains and challenges, however standards in respect to guidelines are less volatile. It is important that cloud providers should take appropriate security measures, because these measures should be based on best-practice standards and guidelines. Due to the continuous and rapid technology evolution security requrements and mechanisms are also constantly changing and therefore have to be continuously improved. Thus, best practices are also changing continuously to entail the security requirements. It is highly important to prevent and mitigate the impact of cyber-attacks by creating logical redundancy. That is, defense attacks using different layers and separating systems with a different logical structure, cross-check transactions and detect attacks. All these activities are best practices considering cyber-security.

Variety of tools available for supporting different phases of software development are considered for building developing secure software in the cloud in CI context. These tools are configured in an application and feed parameters as input. Running the tools after feeding the parameters generate output. From this output we can benefit on developing secure software. These tools are automated tools for verification and validation of formal specifications and design. For instance, Security Development Life Cycle - SDL is providing a threat modeling tool called SDL Threat Modeling Tool. Guidelines and tools we consider in our study are i) SDL Threat Modeling Tool, ii) Computer Emergency Response Team - CERT best practices [27], [28], iii) European Network and Information Security Agency - ENISA guidelines [29], [30], and iv) Cloud Security Alliance -CSA best practices [31], [32].

C. Security Engineering

Security standards facilitate the implementation of security controls in respect with information security policies. Information security policies are high-level statements or rules defined for protecting systems and its services. Security standard is a low-level prescription company that can enforce the given policy. Thus, security standards help to built-in security in an application as well as in operating environment. There are different types of standards supporting to develop

No.	Security Issues	Software Security Standards, Guidelines and Tools						
		SDL/MSDL	ISO/IEC 27001	ISO/IEC 27002	CC	ENISA guidelines	CERT best practices	CSA best practices
1	Data Security							
	a) Data Storage	✓	✓	✓	✓	✓	✓	✓
	b)Data Breaches or leakage	✗	✓	✓	✗	✓	✓	✗
	c) Data Loss	✗	✓	✗	✗	✗	✗	✓
	d) Data Scavenging	✗	✗	✓	✗	✗	✗	✗
2	Transmission and Network Security	✗	✗	✓	✓	✓	✓	✓
3	Application Security	✓	✓	✓	✓	✓	✓	✓
4	Virtual Machine Security							
	a) Creation Security	✗	✗	✗	✗	✗	✗	✗
	b) Isolation Security	✗	✗	✗	✗	✗	✗	✓
	c) Execution Security	✗	✗	✓	✗	✗	✗	✗
	d) Migration Security	✗	✗	✗	✗	✗	✗	✓
5	Insiders Security	✗	✓	✓	✗	✓	✓	✗
6	Interfaces and API Security	✓	✗	✗	✗	✗	✗	✓
7	Shared Resources Security	✗	✗	✗	✗	✗	✗	✗
8	Cloud Integrity Security	✗	✗	✗	✗	✗	✗	✗
9	Security Related to Third Party	✗	✓	✓	✗	✓	✓	✗
10	Harmonization of security policies between Cloud layers and cloud providers	✗	✓	✗	✗	✗	✗	✗
11	Hypervisor Security	✗	✗	✓	✓	✗	✗	✓
12	Account Security	✗	✓	✓	✓	✗	✓	✗
13	Cloud Service Security	✗	✗	✗	✓	✗	✗	✗

Table I
APPLICABILITY OF POPULAR SOFTWARE SECURITY STANDARDS, GUIDELINES AND TOOLS IN THE IDENTIFIED LIST OF SECURITY ISSUES. ✗ MEANING THAT THE INDIVIDUAL SECURITY ISSUES IS NOT DEALT WITH BY THE SPECIFIC TOOL OR STANDARD. MORE DETAILS ARE AVAILABLE IN [4]

secure software. We sub-categorize standards, guidelines and tools and discuss them in the Sections A and B depending on their contribution of producing secure software. If the standards, guidelines or tools help to make software secure by enforcing security policies or help to make more secure against the attacks by other means then we list them in this category. Following is the list of secure development means that falls in this category are i) ISO/IEC 27001, ii) ISO/IEC 27002, iii) CERT best practices, and iv) CSA best practices.

D. Software Development

Software development standards define frameworks for software lifecycle processes, containing a hierarchy of processes, activities and tasks to be applied in software development environment. Thus, software development standards provide best practices and rules applied in different phases of the software development lifecycle (from requirement phase to deployment phase). Activities involved in software development from the provided standards or guidelines are applied to produce secure software. It reduces cost and vulnerabilities. Not only best practices, there are also tools available that help in secure software development. Similar to standards and guidelines, these tools also help in different phases of software development lifecycle. Thus, different tools are to be used for different purposes. The popular secure software development means we have discussed in the Sections A and B fall in this category are i) SDL/MSDL, ii) ENISA guidelines, iii) CC, and iv) SDL threat modeling.

Graphical representation of categorization and sub-categorization of these secure software development means is shown in our multidimensional taxonomy Figure2.

V. MAPPING OF SECURITY ISSUES TO STANDARDS

For each of the identified issues, we find out the applicability of the popular secure software development standards and tools. We investigate on available documents of the secure software development means and find out how these means help us in addressing the security issues. We summarize our result in a table (see Table I), we tick the boxes of the issues and the means for those addressing the issues and cross the boxes for those not addressing the issues. For each of the ticked boxes we give reason how the particular mean helps to address the issue, and for the not addressing issues (crossed boxes) we also give reason in a summary (see [4]). Here, we give some examples of the contribution of the means to address security issues.

Contribution of SDL/MSDL to mitigate Application Security [10]: in Practice 1, under topic *Training Requirements*, it is stated that security training of secure design, threat modeling, secure coding (buffer overflow, cross-site scripting, SQL injection) and security testing need to be given to the software development team before the development of software. In practice 5 (*Design Requirements*), it is mentioned that secure features (well engineered functionality with respect to security) and security features (functionality with security implications like firewall) should be considered in the design phase. In Practice 7, *Threat Modeling* helps to consider security issues in application level and implication of security in a planned operational environment and structured fashion. *Static Analysis* (Practice 10) helps to ensure that secure coding polices are followed. *Dynamic Program*

Analysis (Practice 11) ensures the correct functionality of the programs as they are designed.

Contribution of ISO 27002 to address application security [33]: Issues related to system development and maintenance are addressed in section 12 (*information systems acquisition, development and maintenance*). This section is described in different subsections as: i) *Security requirements of information systems*: Its aim is to ensure that security is built into IT systems. Therefore, an analysis of security requirements should be carried out at the requirement analysis phase of each development process. ii) *Correct processing in applications*: Its aim is to prevent loss, modification or misuse of user data in application systems. Controls like *input data validation*, *control of internal processing*, *message integrity* and *output data validation* should be performed to make sure that applications process information correctly. iii) *Technical vulnerability management*: Its aim is to reduce risk arising from exploitation of public technical vulnerabilities. Technical vulnerability management should be implemented in an effective and systematic way. These measurements should be confirmed to its effectiveness against the vulnerabilities.

Contribution of ENISA guideline to address Insider Security [34]: domain *Human resources security* has guidelines that help to establish and maintain an appropriate process for managing changes in employees, contractors and third-party users, and changes in their roles and responsibilities in a subdomain *personnel changes*. For example, "[from ISO27002 Ch 8.3] Responsibilities should be in place to ensure an employees, contractors or third-party users exit from an organization is managed, and that the return of all equipment and the removal of all access rights are completed." Managing personnel and their roles and responsibilities helps to mitigate insiders security issue.

Mapping of the security issues and the secure software development means is presented in a multidimensional taxonomy (Figure 2). Different color and lines are used for mapping the security issues to different mean to avoid overlapping and confusions.

VI. Evaluation of Taxonomy

We evaluate our taxonomy by adopting a standard prescribed by the taxonomy to implement our show case. Based on the issues identified in the show case, we first translate these issues to associated security issues (in the taxonomy) and select security issues to be evaluated. Selected security issues are *i) Data Storage Security, ii) Application Security, and iii) Interfaces and API Security*. These issues can then be mapped to a standard using the taxonomy. In our case, an analysis of the taxonomy led us to the conclusion, that SDL standard was suitable for implementing our show case. So, we come to know that these issues are addressed by SDL. Secondly, we select a SDL standard (SDL Tool) from the taxonomy and then evaluate the mapping of the security

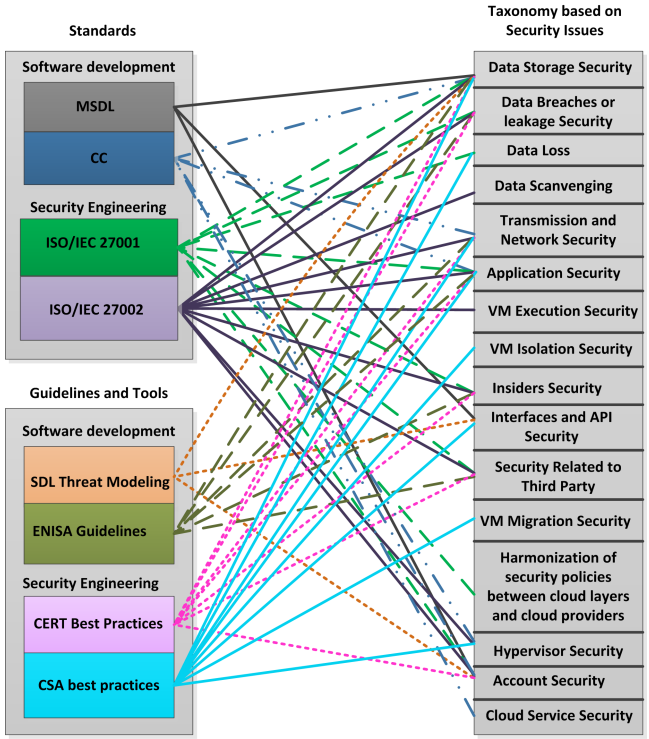

Figure 2. Multidimensional Taxonomy: Mapping the list of identified security issues to the popular secure software developments means based on their applicability. The main focus is to illustrate the dimensioning and ignoring the threat classes.

issues to SDL in the taxonomy, and finally, we examine the contribution of the tool to address the selected security issues.

Our experience showed that SDL Tools are great for developing right secure software and these tools sets are used for different purposes in different phases of software development lifecycle. SDL Threat Modeling Tool uses STRIDE and DREAD principle and helps to identify potential threats and mitigation(s) in design phase which is relatively easy, cost-effective to resolve and reduce the total cost of development. We developed a data flow diagram (DFD) of our show case and apply it in the tool. For all generated potential threats, we defined impacts and mitigation(s). Additionally, we calculated risk level of the threats and prioritized them. This helps us in examining the contribution of this tool on addressing the selected security issues (documented in [4]).

VII. Conclusion

Critical infrastructures are thought of as the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health, safety, commerce, and national security or any combination of those. CI are rapidly being integrated in the cloud to benefit from their characteristics; this is making them cyber-physical systems. This integration implies security issues, which we have analyzed. We have investigated the applicability of various system engineering and software development means to

addressing these security issues. We map each security issue to supporting standards, guidelines and tools and present these mappings in the form of a multidimensional taxonomy. An evaluation of this work is provided by using it for a show case in which an identified tool is applied to support the given security issues. A more general result of our work is that some identified security issues are not being addressed by any of the investigated means sufficiently. So, further investigation on more standards and tools may be required to find out whether they address these security issues. Alternatively to bridge this gap, the security issues can be addressed in updates of existing standards and tools or new means can be provided addressing these issues. In any case, we envisage that our output will help Critical Infrastructure and cloud providers or stakeholders of other CPSs to select the right means to build a secure software for their given context.

REFERENCES

[1] I. Abbadi, "Toward trustworthy clouds internet scale critical infrastructure," in *Information Security Practice and Experience*, ser. Lecture Notes in Computer Science, F. Bao and J. Weng, Eds. Springer Berlin Heidelberg, 2011, vol. 6672.

[2] J. Peerenboom, R. Fisher, and R. Whitfield, "Recovering from disruptions of interdependent critical infrastructures," in *CRIS/DRM/IIIT/NSF Workshop on Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures*, 2001.

[3] S. Paudel, M. Tauber, and I. Brandic, "Security standards taxonomy for cloud applications in critical infrastructure it," in *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for*, Dec 2013.

[4] S. Paudel, "Security Engineering and Software Development for Critical Infrastructure IT in the Cloud," http://www.seccrit.eu/publications/, 2014, [Online; accessed July-2014].

[5] J. Liang and P. Wu, "Challenges of cloud computing evaluation," *Applied Mechanics and Materials*, vol. 198-199, 2012.

[6] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *Internet Computing, IEEE*, vol. 16, no. 1, 2012.

[7] M. Dekker, "Critical cloud computing:ciip perspective on cloud computing," 2013, [Online; accessed 19-July-2013].

[8] M. M. Younis A.Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: A survey," Liverpool John Moores University, UK, Tech. Rep., 2013.

[9] L. Futcher and R. von Solms, "Guidelines for secure software development," in *Proceedings of the 2008 SAICSIT riding the wave of technology*, ser. SAICSIT '08, 2008.

[10] M. Secure Development Lifecycle, "Simplified implementation of the microsoft sdl," 2010, [Online; accessed July-2013].

[11] C. M. Committee, "Common Criteria for Information Technology Security Evaluation," http://www.commoncriteriaportal.org/cc/, 2013, [Online; accessed 16-July-2013].

[12] J. Yu and R. Buyya, "A taxonomy of workflow management systems for grid computing," Tech. Rep., 2005.

[13] R. Dukaric and M. B. Juric, "Towards a unified taxonomy and architecture of cloud frameworks," *Future Generation Comp. Systems*, 2013.

[14] M. Razzazi, A. Tahouri, and K. Fayazbakhsh, "Evaluation process management software for security evaluation," in *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd Int. Conf. on*, 2008.

[15] M. Johns, C. Beyerlein, R. Giesecke, and J. Posegga, "Secure code generation for web applications," in *Engineering Secure Software and Systems*, ser. Lecture Notes in Computer Science, F. Massacci, D. Wallach, and N. Zannone, Eds. Springer Berlin Heidelberg, 2010, vol. 5965, pp. 96–113.

[16] D. Molnar and S. Schechter, "Self hosting vs. cloud hosting: Accounting for the security impact of hosting in the cloud."

[17] H. Tianfield, "Security issues in cloud computing," in *Systems, Man, and Cybernetics, 2012 IEEE Int. Conf. on*, 2012.

[18] M. Z. Meetei and A. Goel, "Security issues in cloud computing," in *Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on*, 2012.

[19] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in *MIPRO, 2010 Proceedings of the 33rd International Convention*, 2010, pp. 344–349.

[20] C. S. ALLIANCE, "The notorious nine: Cloud computing top threats in 2013," [Online; accessed Oct-2013].

[21] "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, 2013.

[22] P. Saripalli and B. Walters, "Quirc: A quantitative impact and risk assessment framework for cloud security," in *Cloud Computing (CLOUD), 2010 IEEE 3rd Int. Conf. on*, 2010.

[23] I. O. for Standardization and I. E. Commission, "Iso/iec 27001:2005 information technology security techniques information security management systems requirements," 2005, [Online; accessed 23-July-2013].

[24] ISO/IEC, "Iso/iec 27001:2005 information technology security techniques information security management systems requirements," 2005, [Online; accessed 23-July-2013].

[25] ISO, "Iso/iec 27002:2005 information technology security techniques code of practice for information security management," 2005, [Online; accessed 23-July-2013].

[26] M. Howard and S. Lipner, *The Security Development Lifecycle*. Redmond, WA, USA: Microsoft Press, 2006.

[27] C. M. Software Engineering Institute, "Computer emergency response team," [Online; accessed 23-July-2013].

[28] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. J. Shimeall, and L. Flynn, "Common sense guide to mitigating insider threats," [Online; accessed 23-July-2013].

[29] P. Balboni, K. Mccorry, and P. W. David Snead, "Benefits, risks and recommendations for information security," 2009.

[30] E. Giles Hogben, Marnix Dekker, "A guide to monitoring of security service levels in cloud contracts," 2012.

[31] C. S. A. Commitee, "Security guidance for critical areas of focus in cloud computing," vol. 3, 2011.

[32] B. Sullivan, S. Tablet, E. Bonver, J. Furlong, S. Orrin, and P. Uhley, "Practices for secure development of cloud applications," 2013, [Online; accessed 8-August-2014].

[33] ISO/IEC, "Information technology security techniques code of practice for information security management-official document provided by international standard," 2005.

[34] M. Dekker, D. Liveri, D. Catteddu, and L. Dupre, "Technical guideline for maximum security measures," 2011, [Online; accessed 7-July-2014].