SECURED CLOUD SUPPORT FOR GLOBAL SOFTWARE REQUIREMENT RISK MANAGEMENT

Shruti Patil[1] and Roshani Ade[2]

[1]Dr.D.Y.Patil School of Engineering and Technology,
Savitribai Phule Pune University, India
[2]Dr.D.Y.Patil School of Engineering and Technology,
Savitribai Phule Pune University, India

ABSTRACT

This paper presents core problem solution to security of Global Software Development Requirement Information. Currently the major issue deals with hacking of sensitive client information which may lead to major financial as well as social loss. To avoid this system provides cloud security by encryption of data as well as deployment of tool over the cloud will provide significant security to whole global content management system. The core findings are presented in terms of how hacker hacks such systems and what counter steps need to follow. Our algorithmic development provide random information storage at various cloud nodes to secure our client requirement data files.

KEYWORDS

Requirement Engineering, Global Software Engineering, Cloud Software Security

1. INTRODUCTION

It is a major issue to provide security to software products and applications. To avoid or catch hacking activities is one of major target of our research. But, looking at graduate level of students without knowledge of security aspects it is big deal for industry professionals to handle hacking risks. We believe, if University provides such software and networking security education at undergraduate level, which will deploy new comers with security loaded brain. As a case study we tested our hypothesis with SQL Injection security project. The education as well as discovering approach in Software Security Engineering (SSE) has been debated in the past decade to consider the present necessity for complicated as well as dimensional systems of software's also software-intensive approximations. Commonly, educators guide beliefs by presenting academic directions, considering exercised conducts in an educational mini security project [1].

Thus, the new generation software engineers encounter an approach where bookish approaches along with courses are not appropriate, and they conduct ad hoc conducts based on their experiences, converging on coding. This may adversely impact the activity of engineering beliefs along with gainful conducts in software development approaches. The educational hub should not acquire all the obligation however expects to formulate the scholars for existing confrontations in SE business [2]. Driven by this factuality, several conducts consisted in constructing citation determines alike as PMBOK [3], as well as the development of numerous undergraduate as well as finishing school approaches around the globe.

DOI : 10.5121/ijsea.2014.5602

Furthermore, all these conducts assist to disperse when given as a apportion of occasional approaches, delivering to a deviated as well as localized approach in software security edification, no evidence-based and no concentrated on application of the better instructional domains. Hence, it is authoritative to determine approaches that allocate the consistency of this evidence, demonstrating it to the hacking security domain [4].

In discipline to assist to hacking threat enlightenment, the benchmarked prototype confounds the accumulation as well as benchmark of confirmation and apotheoses that can be applied to improvise approximate as well as materialize correlations among technologies, conducts, and experiences on SS education as well as information approaches [5]. Hence, benchmarked consequences can construct an assemblage of evidence over time, ascribing a sole to approved as well as well-formed considerations about Software Security Engineering (SSE) learning. These considerations can be emerged by a discovering units and competence narratives archive, where researchers as well as educators can exhibit, appear as executors as well as users of instructional reserves, and also effectuation SSE learning to a accrual developed domain of Computer Science.

In this perceive, this paper heads to evince SSE Research approach, an approach to examine benchmarked analyzes as a mean to acknowledge large scale SSE learning. From coincidentally augmenting a scientific benchmark protocol with SSE community in quartet phases, a comprehensive council of information can be cast, appropriating into account SSE comprehensive conditions as well as national individualities. Additionally, this approach distributes the presence of an active and evidence-based archive of SE discovering challenges as well as competence articles in its further phase.

2. PROJECT MANAGEMENT RISK HOT SPOT

Software project management is an intricate and comprehensively characterized position. Project managers observe and aide the work of planners, designers and analyzes of software while now and again taking part in these exercises themselves. Where developer concentrates on code, construction modeling and execution, managers keep tabs on elevated amount concerns: the course of the project, allotment of assets, the list of capabilities, and the client experience. Supervisors work to synchronously fulfill stipulations imposed by clients, engineers, analyzers, maintainers and management.

2.1. Educational challenges and securing software engineering knowledge systems

An educational challenge is the smallest autonomous constitutional competence that holds an aim, a grasping conduct as well as determination [6]. It circumscribes a caste of applicable and self-contained digital means with an instructional pursuit arranged by trio core constituents: contents, education conducts as well as contextual factors. An education body must have an extrinsic knowledge constitutes that assists its archive, search as well as retrieval [7].

An education material is any digital or non-digital entity that can be applied in the technological benefit to information, guidance or drilling, i.e., texts, images, graphs, tables, presentations, diagrams, videos, games or any digital educational material, used by the professors helping students in teaching a subject [8]. In its focus, an understanding approach is advantageous.

Several kinds of education may be constituted in a pedantry approach and its metadata: common aim communicative information, life cycle, guiding content, glossary of identities, explorations as well as approximations, classifies associations to other channels, and instructional category.

Numerous conducts approximate an approach prototype for education challenge composition [9]. Also, the development of the pedantry challenge archetypes drive the connotation of authoritative differences achievable, like as reuse, endurance, as well as accessibility, highlighted in standards [4].

In SSE pedantry, the application of pedantry challenges head at curtailing the mentioned dilemmas hence it ascribes approaches to assist the instruction and pedantry mechanisms, distant simplifying associations among considerations, activities and outgrowths in software engineering. Numerous pedantry ambiences are conceived to benefit the SE understanding manner additionally approximate frequent concrete activities augmented to software development that encourages and assists academics. This caste of pedantry articles can be simulation game, flowcharts, graphs, and others.

2.2. SQL injection risk in cloud application deployment

From decade industry facing problems of SQL injection hacking and solutions provided as a positive tainting or syntax awareness systems. Although industry provided good security, hacker still hacking systems using newer tricks and techniques. Furthermore to avoid hacking of software systems cloud came in market for secure deployment of projects over cloud. Now the cloud security became latest issues as hackers are hacking cloud security. As a case study present research focusing over data encryption for deployed software files itself to randomize storage location of deployment files. The motivation behind this research is need in market. It is very necessary to train undergraduate students with basic security threats and mitigation techniques. We are developing such system and web tracking application to avoid project failure. We are focusing over mitigation techniques for requirement failure due to breach of security.

2.3. Role of practitioners experience to enhance security engineering education

The enforcement of instructional analysis is acknowledged by analyzes which focuses to determine unknown or benchmark perceived things. They can be assorted into initial and final analyzes. Initial analyzes are controlled by arguments to be acknowledged or accounted. These examines are comported when it is essential to improvise a definite pedantry challenge in application within a distinguishing context. The consequence benchmark of an initial examine can be quantitative, semi-quantitative or qualitative, as well as it can delineate (or is associated to) an competence comment. trident categorizes can be determined [10]: (i) portfolio examine is conducted to conform a action or prodigy discernible by an entity within a bound duration; (ii) quasi-experiment is conducted once a greater direct of the condition is desired, approaching at considering one or more variables and execute the approximate of others; and (iii) examine is conducted to accumulate data from a archetypal of the occupant using a set of queries.

Furthermore initial examines pantomime a individualized pedantry challenge, they are not enough [11]. Thus, further analyzes head to conform effects from numerous co-operational elementary examines. Additional reviews are favourable in disclosing apotheoses as well as developing councils of evidence that can be mapped to existent as well as common instructional aides. These examines ensue through mannerly reviews as well as meta-analysis [7]: the alpha one is a methodology concentrated on a literature comb protocol; and the other one examine addressed following a mannerly review to approximately compensate the quantitative evidence from annotated papers.

Performances of benchmarked examines concept along with accomplishment in SSE pedantry can be determined in the literature, few of them describing impressions of applying asymmetric as well as interesting approaches to have the students' attentiveness. Papers from 2011 to 2014 were inspected, determining numerous instructional confrontations, like as

i. Implementation of Software engineering in computer science and engineering disciplines

ii. Educating domains of information from SWEBOK Security/Risk and SWEBOK contribution in University textbook

iii. Graduate SSE projects

iv. Practitioners Involvement in SSE Educational Support and milestone of SSE in institute as well as business. This benchmark is exhibited in figure-1.

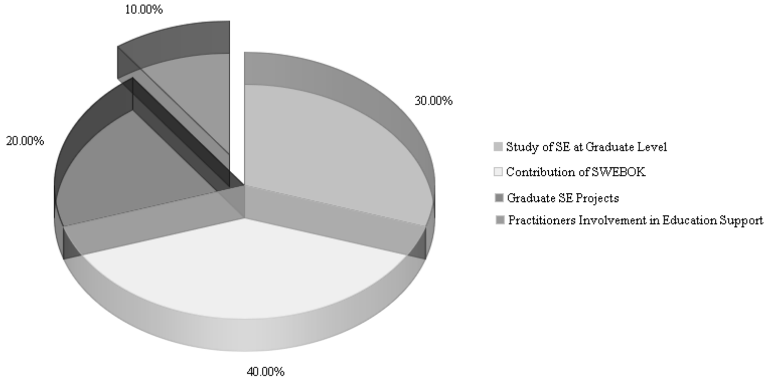

Figure 1. Literature Review 2011-2014

3. THEORY/SWEBOK/PROJECT SECURITY (TSPS) METHODOLOGY

As an outcome of literature survey of articles from 2011 to 2014, our methodology proposes systematic review and survey to establish and integrate software engineering education researches with collaboration of industrial practices and academic approaches. Hence, two communities are highlighted as Industrial stakeholders: who work in software engineering domain and wish to improve the education of their software engineering areas and mentors who train SSE to their students.

Using our TSPS (Theory/ SWEBOK /Project Security) approach, the academic theory can be initial pin points for project goal with reference to SWEBOK and security risk aspects. To evaluate software security engineering education and adaption approach, it is necessary to identify and resolve problems. Hence student needs technical interaction with industrial person to list out practitioner's experiences about execution of specific goal. At the same time it is not enough to identify goal and thereafter approach towards solution, hence student need to grasp necessary findings with reference to SWEBOK, PMBOK to make ground judgement with the help of academic mentor. Thus, it is task of practitioner, mentor and students to resolve problem definition hand in hand. Hence it is clear that our research methodology actors will be from academic as well as industrial background.

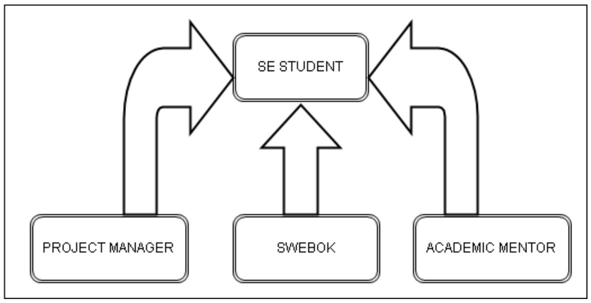

Figure 2: TSPS Methodology Outline

In order to collaborate educating and pedantry perseveres as well as pedantry challenges approximations, software engineering educators can feed convictions as well as explicate activities, characteristics, approaches, and contexts challenged in the course of software engineering classrooms in any software engineering domain or orientation. This evidence is additionally an effectual element and should be archived as well as categorized to be combed as well as accumulated. Software Security engineering researchers can approach them to augment or evolve pedantry challenges as breakthroughs. In this perceive, it is authoritative to aspire pedantry challenges and competence accounts to dilemmas, breakthroughs, confrontations, as well as regional differences lately determined in TSPS research strategy [12].

Based on the above discussed methodology, web application framework to support TSP research strategy was constructed and an infrastructure is under development. Figure 2 shows clear actor involvement in this research. As an illustrative module we focus over requirement risk mitigation domain and hence we collecting more information from industrial software engineering experts as well as from University mentor. This application fuses proclamation; association, synchronism, as well as control approaches to benchmark analyze disciplines, and conducts. Contemporarily TSP project is embodying web application and the related factors. This genotype heads at driving a software engineering education for pedantry challenges along with competence anecdotes conception and control, based on software reuse approaches.

4. CLOUD DATA SECURITY

As a part of global software development data security, we implemented file encryption and splitting methodology to store data files over different cloud nodes. This implementation provides secure storage for requirement documentation as well as design documentation generated in software project life cycle. As we discussed TSPS methodology incorporating with software project development, the cloud storage plays very important role to avoid hacking of crucial documents like defence project documents.

It is common in software industries to share software project documents over the globe but, more or less the issue of document security never focused. We implemented this methodology to avoid hacking risk in early stages of software development. Using cloud framework, global software team can handle all requirement phase in most secured and shared manner. Figure 3 shows the conceptual view of cloud data security system.

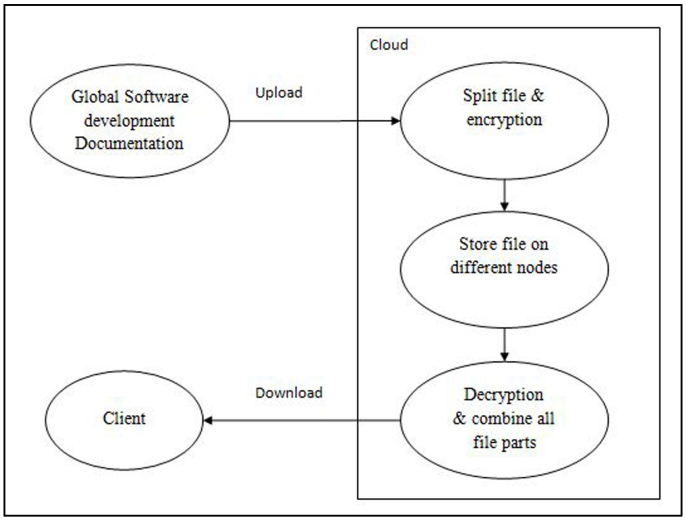
Cloud
Global Software development Documentation
Upload
Split file & encryption
Store file on different nodes
Decryption & combine all file parts
Download
Client

Figure 3: Conceptual view of cloud data security

5. CONCLUSIONS

This educational research in software engineering domain itself implies the reason for research. TSPS approach along with secured cloud approach proves necessity of global teamwork to achieve balanced theoretical as well as implementation improvements and gives benefits to industries. This approach can provide ready to deploy strategies for software industry and there will be less loss for project failures. Such approach will focus to think over security problem mitigation techniques prior to face problems in software engineering domain. Till date in software engineering practices, people undergo through various problems and this may lead to failure risks. Further, this approach can be used for risk mitigation in early stages of cloud service selection to fulfil the client’s requirements.

ACKNOWLEDGEMENTS

The authors would like to thank all colleagues who supported in this research work.

REFERENCES

[1] Kruchten, Philippe. "Experience teaching software project management in both industrial and academic settings." Software Engineering Education and Training (CSEE&T), 2011 24th IEEE-CS Conference on. IEEE, 2011.

[2] Borges, Pedro, Paula Monteiro, and Ricardo J. Machado. "Mapping RUP roles to small software development teams." Software Quality. Process Automation in Software Development. Springer Berlin Heidelberg, 2012. 59-70.

[3] Verner, June M., et al. "Systematic literature reviews in global software development: A tertiary study." (2012): 2-11.

[4] González-Morales, Daniel, Luz Marina Moreno de Antonio, and José Luis Roda García. "Teaching “Soft” skills in software engineering." Global Engineering Education Conference (EDUCON), 2011 IEEE. IEEE, 2011.

[5] Savi, Rafael, Christiane Gresse von Wangenheim, and Adriano Ferreti Borgatto. "A Model for the Evaluation of Educational Games for Teaching Software Engineering." Software Engineering (SBES), 2011 25th Brazilian Symposium on. IEEE, 2011.

[6] Ardis, Mark, et al. "Recent Trends in Graduate Software Engineering." Software Engineering Education and Training (CSEE&T), 2013 IEEE 26th Conference on. IEEE, 2013.

[7] Lavrischeva, Ekaterina, and Alexei Ostrovski. "New Theoretical Aspects of Software Engineering for Development Applications and E-Learning." Journal of Software Engineering and Applications 6 (2013): 34.

[8] Alves, Luís M., Pedro Ribeiro, and Ricardo J. Machado. "Project-Based Learning: An Environment to Prepare IT." Overcoming Challenges in Software Engineering Education: Delivering Non-Technical Knowledge and Skills (2014): 230.

[9] Moorthy, Jayaletchumi Sambantha, Suhaimi bin Ibrahim, and Mohd Naz'ri Mahrin. "Developing Usable Software Product Using Usability Risk Assessment Model." International Journal of Digital Information and Wireless Communications (IJDIWC) 4.1 (2014): 95-102.

[10] VALENCIA, Luis Eduardo PELÁEZ, Lorena CARDONA BENJUMEA, and T. O. R. O. Alonso. "Relación entre la carta del proyecto del PMBOK (PMI) y SQA [The relationship between the Project Charter of PMBOK (PMI) and SQA]." Ventana Informática 29 (2014).

[11] Zhan, Dechen, Lanshun Nie, and Xiaofei Xu. "Computational Thinking and Its Impact on Software Engineering Education." Software Engineering Education for a Global E-Service Economy. Springer International Publishing, 2014. 29-40

[12] Shruti Patil and Roshani Ade. “Software Requirement Engineering Risk Prediction Model.” International Journal of Computer Applications 102.2(2014):1-6.