Factors for Better Adoption of Information Security on Custom-Made Software at SMEs: A Systematic Review and Framework

Fatimah Alghamdi[a,1], **Moutasm Tamimi** [b,2], **Nermin Hamza** [c,1,3]

[1]Faculty of Computing and Information, King Abdul-Aziz University Jeddah, KSA
[2]Zarqa University, Jordan
[3] Faculty of Computing and Information, King Abdul-Aziz University Jeddah, KSA, Faculty of Graduate Studies for Statistical Research, Cairo University, Egypt

Abstract
Investigations on information security factors re- main elusive at small and medium enterprises (SMEs), es- specially for custom-made software solutions. This article aims to investigate, classify, adopt factors from recent literature addressing information security resources. SMEs al- ready have information security in place, but they are not easy to adopt through the negotiation processes between the in-house software development companies and custom-made software clients at SMEs. This article proposes a strategic framework for implementing the process of adoption of the information security factors at SMEs after conducting a systematic snapshot approach for investigating and classifying the resources. The systematic snapshot was conducted using a search strategy with inclusion and exclusion criteria to retain 128 final reviewed papers from a large number of papers within the period of 2001-2022. These papers were analyzed based on a classification schema including management, organizational, development, and environmental categories in software development lifecycle (SDLC) phases in order to define new security factors. The reviewed articles addressed research gaps, trends, and common covered evidence-based decisions based on the findings of the systematic mapping. Hence, this paper boosts the broader cooperation between in-house software development companies and their clients to elicit, customize, and adopt the factors based on clients' demands.

Keywords:
Information Security, Custom-Made Software, SME, SDLC, ICCAIS

1. Introduction

Over the last few decades, software companies have pro- duced different types of secure software enterprises (SE)[1] such as packaged software (PS) and bespoke software (BS) enterprises. PS is ready-made software that is developed to meet the needs of a large number of customers with similar functionalities[2,3]. While the BS (that is, custom-made or tailored software) is developed for specific customers with specific functionalities[4,5]. At in-house software develop- ment companies, there are challenges involving the informa- tion security requirements upon to the type of enterprises[4– 7], upon to the size of enterprises either at SMEs or at large projects[8–10]. It is clear that the lack of categorized secu- rity resources[10], misunderstanding security demands, un- willingness to adopt security practices. At in-house software development companies, there are attempts on increasing the adoption of security practices, but having limitations on the adoption process of information security (IS) resources[6, 11,12] for BS enterprises at SMEs [13] hinders the optimum selection and implementation security standards. Another limitation is the negotiation gap between in-house software development companies and customers for security require- ments elicitation (SRE) to meet expectations and results as needed to grantee a higher level of confidentiality, integrity, and availability, especially when the customer's background about the importance of adopting security practices is weak. Or that the customer does not believe in the security risks at SMEs for explanation identify, authenticate, authorize, and audit the security principles for secure success practices. This article is an extension of a previously published Inter- national Conference on Control, Automation Information Sciences (ICCAIS) conference paper that investigated in- formation security factors (ISFs) for custom-made software during the requirements phase of the software development life cycle (SDLC) at SMEs [14]. The extensions of our pre- viously published paper focus on the investigations of ISFs in all of the SDLC phases based on four categories; man- agement categories, organizational categories, development categories, and environmental categories. We have extended the classifications based on security services and systematic mapping summaries to include the requirement, design, im- plementation, verification, release, and maintenance phases. We also propose a strategic framework for influencing on adoption the ISFs on the BS enterprises at SMEs. Research questions cover the purpose of this article, as shown in the following:

RQ1: What are the recent investigations at in-house software development companies on Information Security?

Manuscript received February 5, 2023
Manuscript revised February 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.2.7

RQ2:What are the research gaps, trends, and evidence-based decision making from the previous investigations on the SDLC?
RQ3:How the extracted factors can be adopted through the agreement of SRE at small BS enterprises?
The remaining research is organized as follows, materials and methods are presented in section 2. In section 3, the find- ings of the systemic snapshot approach are presented with a critical discussion of the results. In section4, the conceptual framework is addressed. A conclusion is given in section 5.

2. Material and Method

This section describes a Systematic Snapshot Mapping (SSM) based on augmented categories and factors at SMEs[2,5, 14] based on a classification schema. This methodology deals with a large number of research papers that organize and ex- tract systematically the unstructured resources. As described by Tamimi et al.[5,15] , and Alghamdi, F. et al.[14] this methodology enables researchers to make decisions inde- pendently instead of having to follow distributed random data in many papers. This method begins with processes on a search strategy, data source, inclusion and exclusion pro- cesses as shown below.

2.1 Search Strategies

Our search strategy combines relevant, specific keywords and search strings, which are used to cover a diversity of in- formation security (IS) investigations for custom-made soft- ware at SMEs. Keywords for IS are combined with other relative keywords and search strings, such as “custom soft- ware”, the names of SDLC phases, and the names of security services. “AND and OR” operators are used to optimize the results of research library search engines. Next, we changed the positions of the identified keywords and replacing the “AND” and “OR” operators to capture more relevant re- search. Fig.1shows combinations of primary and secondary keywords and strings on the search engines.

2.2 Data Source and Retrieval

We utilized combinations of search strings in the search en- gines of the digital libraries such as IEEE Xplore, ACM, SpringerLink, and other digital libraries. Each database en- abled us to identify date ranges for published papers, com- monly used keywords, and papers in different qualities. Welimited our search to papers published between 2001 and 2022. The initial outcomes were reviewed through the titles, abstracts, and keywords of papers. To extract the relevant papers from huge resources, we conducted an inclusion and exclusion process to limit the outcomes in Fig.2. The inclu- sion process began with reviewing titles and abstracts of the collected around (2130 papers). The titles review enabled
us to exclude papers that were not relevant to our research (890 papers). Next, we identified papers that were written in English, unduplicated, and published in well-known jour- nals and conferences. The extract of 240 papers afterwards. The exclusion process began with ignoring the studies that were not in the research domains of software engineering and computer science. Studies that were presented as books, reports, posters, presentations were also excluded. Finally, full-text read with deliberations were excluded the (128 pa- pers).

3. Results

This section demonstrates the systematic investigation about the most common IS literature. Once the data were collected, the extraction of results was based on a classification schema. The schema contained four main categories: management, organizational, development, and environmental categories, as shown in Fig.3.

The classification was relied on Tamimi et al.[2,5,15, 16] that conducted several studies on a custom-made soft- ware, and packaged software enterprises in development per- spectives, and Alghamdi et al. [14]also conducted a study on secure BS. To produce the security factors in the SDLC phases at SMEs as shown in the given tables (I, II, III, IV, V, VI) below to answer the RQ1.

3.1 Security Investigations in Planning Phase

Security Requirements Specifications in the Planning phase (SecRSP) is a part of the software engineering process that ensures a highly secure level of adopting material resources and specifications across which should be specified, man- aged, and evolved. The increase of the level of customers’ confidence during negotiations with in-house software de- velopment companies on the security factors. Our investiga- tions focused on security requirement principles, manage- ments, goals, security requirement assurances, and other as- pects. TABLE1demonstrates the findings of the SecRSP.

("Information Security" OR "Security") "AND ("Custom software" OR "tailored enterprise" OR "bespoke software") or ("Requirement" OR "Development" OR "Implementation" OR "Design" OR "Verification" OR "Testing" OR "Release" OR "Deployment" OR" Maintenance") OR ("challenges" OR "problems") OR ("guidelines" OR "practices") OR ("management", "ISO management") OR (Security Services) ("Confidentiality" OR "Integrity" OR "Availability" OR "Authorization" OR "Authentication" OR "Risk Management" OR "Security Management") AND ("small and medium enterprise" OR "SMEs")

Fig. 1 Search Strategies combinations

Table 1 FINDINGS OF SECURITY INVESTIGATIONS IN THE PLANNING PHASE

Factors	Sub-factor	Goal	References
Project management	Identify security assets.	To define the responsibilities of appropriate asset protection.	[17–21]
	Unify security requirement based on security models.	To follow the standardizations of security planning processes.	[17,19,22, 23]
	Assign and enforce responsibilities and standards.	To ensure the availability and continuity of services.	[18]
	Manage the conflict of security requirements.	To avoid the higher risks of conflicted security requirement.	[20,24]
	Elect a suitable recourse to support security-related APIs.	To facilitate the process of adoption the security in development phase.	[20,25]
Change management	Study the change of security requirements.	To understand the contingency plans for changes in security requirements.	[26,27]
	Analyze security changes in the business operational environment.	To deal with the changes in the security demands in a flexible management.	[26,28,29]
Data management	Manage scenarios of data flow.	To avoid overflow of sensitive data and chance to breach.	[17,30]
Project team competence	Assign a security management team.	To simply manage the roles and changes of accesses control.	[31,32]
	Evaluate the team response from adopting security requirements.	To increase the awareness about security practices.	[33,34]
Top management support	Assign the regulatory of privacy, laws, policies, and constraints.	To govern the project and to guide the developers about the secure project.	[18,22,35, 36]
	Assign security awareness training	To improve the knowledge to custom-made systems owners about the security impacts.	[18,36]
Education and training	Re-skill security teamwork	To increase the appropriate knowledge and skills of security issues	[33?]
Enterprise system	Plan to identify security measures	To understand the process of detecting the weakness.	[37–39]
Organization characteristics	Study the clients' purpose of IS	To understand the demand of IS from clients.	[19]
	Study the organization checklist security authorizations	To assign role and responsibilities.	[19]
Strategy and methodology	Analyses former implementation security strategies.	To understand the process of detection previous defects.	[40,41]
Software development	Develop security practices during requirement phase.	To determine the internal and external risk resources.	[21]
	Build reusable repository of threats	To reduce the risks of the identified repository of threats.	[42]
Monitoring	Determine the likelihood of occurrence in security management.	To specify the potential risks of security management.	[43–47]
User involvement	Assess client feedback about security requirements	To identify the degree of acceptance and service level agreement from clients.	[18,48]
Environment	Define and analyze the infrastructures and platforms of the organization.	To understand the operational environment.	[18]

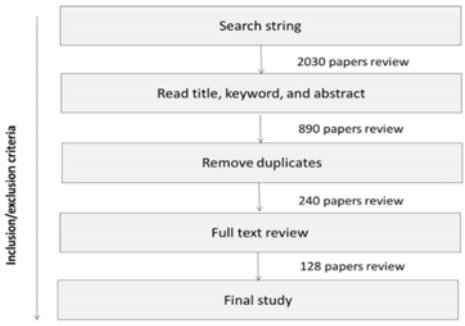

Fig. 2 Data Source and Retrieval Processes Findings

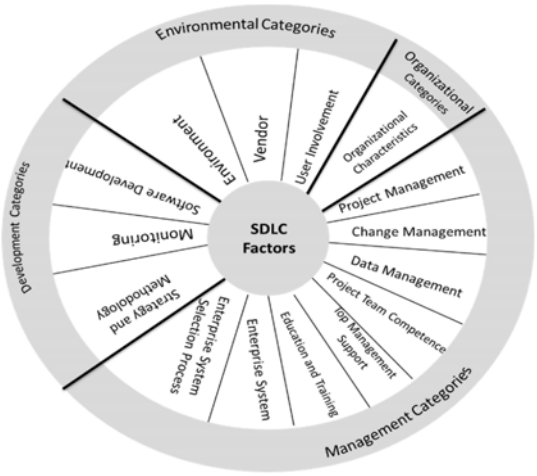

Fig. 3 SDLC Factors [2,5,15]

3.2 Security Investigations in the Design Phase

Security Requirements Specifications in the Design phase (SecRSD) aims to present management aspects, guidelines, practices, and measures to boost the secure design to cus- tomers with less of potential risks and vulnerabilities. In terms of small BS development, the SecRSD is identified, analyzed and classified the 128 papers in TABLE2.

3.3 Security Investigations in Implementation Phase

Secure Software Implementation Specification (SSIS) helps developers to achieve a higher level of secure source coding through the adoption of standards of guidelines and prac- tices at the implementation phase. In terms of custom-made software development, SSIS must be negotiated with cus- tomers. TABLE3shows the contributions in SSIS that we analyzed and classified from the 128 papers we gathered.

3.4 Security Investigations in Verification and Validation Phase

Security Requirements Specifications in Verification and Val- idation phase (SecRSV) tests the performance of the threat environments. Security testing is performed by inspectors to examine the level of software security quality as identi- fied with the customers. During secure verification, the goals must be achieved without bugs that influence on the security quality. TABLE4shows the contributions of SecRSV that we analyzed and classified from the 128 gathered papers.

3.5 Security Investigations in Release and Deployment Phase

Security Requirements Specifications in the Deployment phase (SecRSDep) specify the process of converting the secure im- plementation to a secure post-production secure manner. Af- ter ensuring a secure implementation, projects are deployed based on SecRSDep. To contribute in this phase, we ana- lyzed and classified the 128 gathered papers as shown in TABLE5.

3.6 Security Investigations in Maintenance Phase

Security Requirements Specifications in the Maintenance phase (SecRSM) specify the resources of modifying, repairing, and upgrading the security functionalities to newly secure func- tionalities. To contribute in SecRSM, we analyzed and clas- sified the 128 gathered papers as shown in TABLE6.

3.7 Findings of Systematic Mapping Summary

After the comprehensive classification at each phase in SDLC, the mapping of the classification answered the RQ2 by pre- senting the number of papers were focused on the manage- ment category (77 research papers), the development cate- gory (75 research papers). The lowest number of research papers addressed the organizational category (10 research papers). The strengths and weaknesses in the coverage of issues related to information security are shown in Fig.4. shows a bubble chart to display the number of used research papers for each SDLC phase and factor. Fig.4summarizes our primary results by illustrating the previous research con- tributions, trends, and gaps among the analyzed studies.

There were gaps in the design and verification phases, especially in the support of top management, project team competence, enterprise system selection process, organiza- tional characteristics, and vendors. The design stage increases on the verification phase the majority of gap research was covered in factors related to change management, data man- agement and user involvement. The majority of gap research

Table 2 FINDINGS OF SECURITY INVESTIGATIONS IN THE DESIGN PHASE

Factors	Sub-factor	Goal	References
Project management	Manage the resources processes to address the cybersecurity.	To align the cybersecurity with overall business goals.	[49–51]
Education and training	Strong attention to imply deadlock protections.	To increase the knowledge of processes operation situations.	[52,53]
Software development	Develop secure software architecture modeling.	To satisfy with SMEs technological requirements.	[19,54–56]
	Develop a client/ server security architecture.	To avoid loss of protection without privacy protection measures	[57,58]
	Develop a clear data flow mechanism.	To protect confidential data at different stages in the system.	[30]
	Develop a prototype design for role/user assignment.	To ensure the accuracy of security level acceptance according to role/user assignments.	[59]
	Customize a pluggable authentication module.	To allow the independently of the underlying authentication scheme.	[60,61]
	Design an integrity model.	To identify the connection between integrity violations	[62]
	Design a service modeling approach.	To improve the capabilities of achieving appropriate levels of service production.	[63,64]
Enterprise system	Track the flow of information between different components of the system's architecture.	To understand the process of avoiding or detecting the buffer overflow.	[65,66]
Strategy and methodology	Study a strategy threat modeling.	To avoid the evolution of vulnerabilities into threats by mapping the security vulnerabilities and apply security countermeasures.	[67–69]
	Study long review process of security design strategies.	To achieve best practices of guidelines practices in the security principles.	[70,71]
	Study the entry point's practices.	To reduce the chance for exploited threats.	[72,73]
Monitoring	Develop design review.	To detect any unintended error or threats	[70,74]
Environment	Analyses external and internal environment design.	To avoid the attack pattern that exploited specific infrastructure or platforms.	[18,75]

was covered in factors related to the enterprise system, strat- egy and methodology and environment. However, this study proposes a conceptual framework for the adoption of IS fac- tors between in-house software development companies and BS software clients at SMEs in security perspectives.

4. Information Security Adoption Framework at SMEs

This section purposes a strategic framework for adopting IS factors during SDLC (ASF-SDLC). This framework an- swers the RQ3 by providing clear processes to boost the ro- bustness and effectiveness of understanding, eliciting, and adopting based a level of negotiations on the security spec- ifications. It assumes that customers and in-house software development companies are the participants who are agree- ing on the security level for developing a custom-made soft- ware at SMEs. The proposed framework is formed by three stages: pre-adoption, adoption, and post-adoption. These stages manage the initial, middle, and final agreement of adoption as shown in Fig.5.

4.1 Pre-Adoption Stage

This stage is the initial negotiation between customers and in-house software development companies on the adoption of IS factors in the planning and design phases of the SDLC. To guarantee the initial outputs, there are resources in TA- BLE1and TABLE2that feed the control activity for the first stage. This control activity is measured by matching the acceptance percentage of IS resources between customers and in-house software development companies. Fig.6shows the pre-adoption stage.

4.2 Adoption Stage

This stage deals with IS factors in the implementation and verification phases of the SDLC. To guarantee the middle- security agreement, there are resources in TABLE3and TABLE4that feeds the control activity in the framework. This control activity can be measured by matching the ac- ceptance percentage on the IS resources between customers and in-house software development companies. Fig.7shows the adoption stage.

Table 3 FINDINGS OF SECURITY INVESTIGATIONS IN THE IMPLEMENTATION PHASE

Factors	Sub-factor	Goal	References
Project management	Manage the roles of security team development members.	To improve the accuracy of team obligations	[36,76]
	Manage appropriate access control.	To ensure confidentiality by distributing the privileged access to the authority's staff	[77,78]
	Assign a code integrity manager.	To manage the roles of ensuring the integrity of code coverage	[79]
Change management	Manage the changes of IS experts.	To manage the process of having alternative security resources	[34]
	Assign a process to change unsafe functions.	To reduce the risks of chances a dependent function from the whole system	[80,81]
Data management	Develop a data transmission protection technique.	To manage the roles of data controller for identifying which exposed place is targeted to attack	[82]
	Assign data protection mechanisms and strategies.	To ensure a higher level of a sensitive data protection during transitions	[82]
Education and training	Train the developer to practice secure development.	To enhance the developer skills and productivity to achieve a secure quality of software.	[10,83]
Enterprise system selection process	Make continues justification process to additional secure functionality.	To provide the ability of generating an activity log, general overview and summary of activities.	[84]
	Strong attention to use cryptographic algorithms.	To improve the understanding of adopting an algorithm for the sensitive data.	[22]
Organization's characteristics	Discover the potential security patches and cyber-attacks.	To provide higher level of adoption the security detection and monitoring techniques	[85–88]
Software development	Develop the organization checklist authorizations.	To improve the authorized access to the information at the organization	[89,90]
	Implement an appropriate method for authenticating users.	To ensure a higher level of correctness of entry data and stored data with a legitimate access	[91]
	Perform exception handling during coding.	To increases the predictability of software behavior.	[22]
	Develop secure functions practices.	To avoid malicious code in order to improve the data protection	[81,92]
Strategy and methodology	Study the masking and transmitted data modulating strategy.	To reduce the likelihood of a third party being able to deduce information from communication channel	[93]
	Study static secure code analysis strategies.	To understand the process of detecting and eliminating the security bugs through coding	[35,40,76]
Monitoring	Review the unintended denial of services operations.	To prevent unauthorized users to control the information	[94,95]
	Control the denied default access.	To ensure that access to information is permitted	[77]

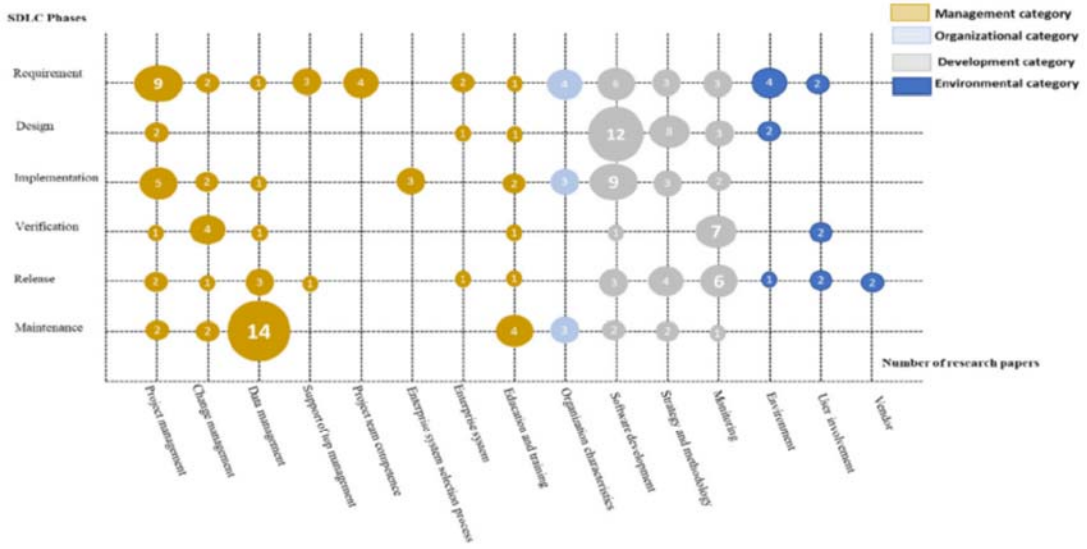

Fig. 4 Systematic Mapping Summary of Information Security Investigations

Table 4 FINDINGS OF SECURITY INVESTIGATIONS IN THE VERIFICATION AND VALIDATION PHASE

Factors	Sub-factor	Goal	References
Project management	Assign trusted third party for penetration testing.	To discover other possibilities are not expected for the internal party	[22]
Change management	Perform the security regression testing.	To ensure that the changes of requirements in the system are still secured.	[96]
	Manage the unintended consequences of environmental changes.	To deal with the critical stress faults that cause interruption of stability and reliability	[97,98]
	Manage the security mutation testing.	To detect different patterns of security vulnerabilities	[22]
Data management	Check the security validation data with the integration testing.	To reduce the exception of handling the threats in the system.	[99]
Education and training	Study users trust after releasing the acceptance security testing.	To ensure the user acceptance for the identified security features	[100]
Software development	Develop a custom risk assessment approach.	To deal with risks based on the custom security demands from clients	[36]
Monitoring	Perform the automation security testing tools.	To scan the resources for detecting the known vulnerabilities and network weakness	[101–103]
	Perform the static code analysis tools.	To detect vulnerabilities and bug before code integration	[35]
	Check the code security review and code security editing report.	To practice formal security detection and solving issues	[104]
User involvement	Study the behavior of the users through the acceptance testing.	To understand and analyze the customer satisfaction feedback.	[105]

Table 5 FINDINGS OF SECURITY INVESTIGATIONS IN THE VERIFICATION AND VALIDATION PHASE

Factors	Sub-factor	Goal	References
Project management	Manage the security auditing reports.	To organize the operational information from unauthorized parties after final security review	[106]
Change management	Manage the change of privacy and policies.	To keep supporting the changes of customer demands	[107]
Data Management	Study the influence of data between the released components.	To deal with a wide range of security system depending upon different contexts	[108]
Support top management	Assign a suitable security certification.	To manage the process of obtaining a security certificate to the customers from the third-party	[109]
Software development	Develop available released components methods.	To ensure availability of continuous service in regard with newly released components.	[18]
	Develop a deployment process to certificate-based authentication.	To grant a higher level of accurate digital certificate.	[110–113]
Strategy and methodology	Develop a strategy of practicing the digital signature technique.	To ensure the availability of the authenticated transmitted data	[114–117]
	Study techniques for avoiding impersonation.	To save the content of message by known the parties by using non-repudiation	[118–120]
Monitoring	Check security certificates validity.	To reduce the risk of security breaches that come from the lack of real-time revoked certificates.	[121]
	Study the availability of Service Level Agreements (SLAs) and Operational Level Agreements (OLAs).	To determine the gaps in services availability	[63]
	Monitor alpha security release with end-of-life date.	To ensure that the potential users have inserted the data without security bugs.	[106]
	Monitor the authorization checklist.	To ensure the authority for intended person	[89,90]
	Monitor the availability of audit log.7 To check the progress of path threats.		[22]
	Monitor the Dos.deny checklist.	To track the IP number of DoS.	[122,123]
Education and training	Develop custom user security awareness.	To avoid the risk associated with misuse/abuse of custom infrastructure cases.	[100,124]
Enterprise system	Pay attention to secure setup pre-requisite.	To check the run of security functions before the final installation.	[106]
User involvement	Study the user interaction of security practices.	To gather a knowledge-based risk transmitted practices from the users.	[125]
	Study a plurality of factor-based data instances.	To define the identity of a corresponding user.	[126]
Environment	Study the security laws and cultural regulations.	To ensure the ethics of laws and regulations upon to the custom software.	[18,127]

Table 6 FINDINGS OF SECURITY INVESTIGATIONS IN THE VERIFICATION AND VALIDATION PHASE

Factors	Sub-factor	Goal	References
Project management	Manage update software patch.	To perform the improvement on the functionalities having detected security risks.	[22,128]
Change management	Study the security upgrades on the upgraded infrastructures.	To govern the security based on a new challenges and updates.	[22,34]
	Manage the process of restructuring the old source code to secure coding.	To migrate the legacy functionalities to new secure functionalities.	[22]
Data management	Manage the impact from data migration on the third-parties.	To avoid any possible threats in the process of loss or leakage of data migration.	[100,129]
Education and training	Train the end-users on new or existing security features.	To increase awareness of security adopting to the end-users.	[22,130–133]
Organization characteristics	Study the behavior of end-users from upgraded security features.	To study the impact of end-users interaction on the third-parties.	[22,134,135]
Software development	Develop a mechanism for secure code restructuring.	To enhance the security performance from a legacy system to a new system.	[136]
	Develop a custom adoptive maintenance.	To meet the modifications in the authorization and authentication checklists.	[107,136]
	Develop a custom perfective maintenance.	To meet the justification, planning, and development of new secure software versions.	[136]
Strategy and methodology	Study a secure strategy for the rollback and recovery.	To provide the ability to make a secure reaction with rollback and recovery.	[22,137]
Monitoring	Monitor the logs and alerts files during the maintenance.	To make sure of tacking the reaction of changes on the system.	[22]

4.3 Post-Adoption Stage

The last stage of adoption of the IS factors in the release and maintenance phases. To guarantee the final-security agree- ment output, there are resources in TABLE5and TABLE6 that feed the control activity in the framework. This control can be measured by matching the acceptance percentage of IS resources between customers and in-house software de- velopment companies. Fig.8shows the post-adoption stage.

4.4 Security Adoption Agreement Validity

The ASF-SDLC framework provides rules and equations to estimate the percentage of compliance with the Security Adoption Agreement (SAA) in all of the stages. Table7 presents the Matching Cases between customers' security Demands (Ds) and in-house software development companies' security specifications from the existing resources in TABLES1,2,3,4,5, and6to define the percentage of Se- curity Adoption Agreement Level (SAAL).

In-house software development company is responsible of classifying the matching of *Ds* with the existing resources of security specifications in each stage at AFS-SDLC. There are four main following rules below to classify the demands for each matching case degree, i:Number of demand,i 1, 2, . . , n, Di(w):the weight of the number of demand.

***Ds*(*i*) ∈*SMR* →(1 <*Di*(*w*)≤3) ∴ *theDs*(*i*)*classifiestoDSMR*(*i*)**

– $Ds(i) \in MR \rightarrow (0.5 < Di(w) \leq 1) \therefore theDs(i)classifiestoDMR(i)$

– $Ds(i) \in UMR \rightarrow (0 < Di(w) \leq 0.5) \therefore theDs(i)classifiestoDUM$

– $Ds(i) \in UR \rightarrow (Di(w)=0) \therefore theDs(i)classifiestoDUR(i)$

There are given equations that help for estimating the

– average power of SAAL: To estimate the average of Pre-Adoption Security Adop- tion Agreement Level (SAALP), the equation is:

– $$\mathbf{SAALP\_AVG}(\mathrm{Ds}) = (\sum_{D=1}^{n}(D\mathrm{SMR} * 3) + \sum_{D=1}^{n}(D\mathrm{MR} * 1) + \sum_{D=1}^{n}(D\mathrm{UMR} * 0.5) + \sum_{D=1}^{n}(D\mathrm{UR} * -0.5)) / \sum_{D=1}^{n} Ds . \quad (1)$$

– To estimate the average of Adoption Security Adoption Agreement Level (SAALA), the same previous equation is:

$$\mathbf{SAALA\_AVG}(\mathrm{Ds}) = (\sum_{D=1}^{n}(D\mathrm{SMR} * 3) + \sum_{D=1}^{n}(D\mathrm{MR} * 1) + \sum_{D=1}^{n}(D\mathrm{UMR} * 0.5) + \sum_{D=1}^{n}(D\mathrm{UR} * -0.5)) / \sum_{D=1}^{n} Ds . \quad (2)$$

–

– To estimate the average of Post-Adoption Security Adop- tion Agreement Level (SAALPt), the same previous equa- tion is:

$$\mathbf{SAALPt\_AVG}(\mathrm{Ds}) = (\sum_{D=1}^{n}(D\mathrm{SMR} * 3) + \sum_{D=1}^{n}(D\mathrm{MR} * 1) + \sum_{D=1}^{n}(D\mathrm{UMR} * 0.5) + \sum_{D=1}^{n}(D\mathrm{UR} * -0.5)) / \sum_{D=1}^{n} Ds \quad (3)$$

– The equation of estimating the average percentage of SAAL in the overall phases at the AFS-SDLC frame- work is:

$$\mathbf{SAAl\_avg}\ (\boldsymbol{Ds}) = \sum_{D=1}^{3} (\mathrm{SAALP\_AVG} + \mathrm{SAALA\_AVG} + \mathrm{SAALPs\_AVG})_{Ds} / 3 \quad (4)$$

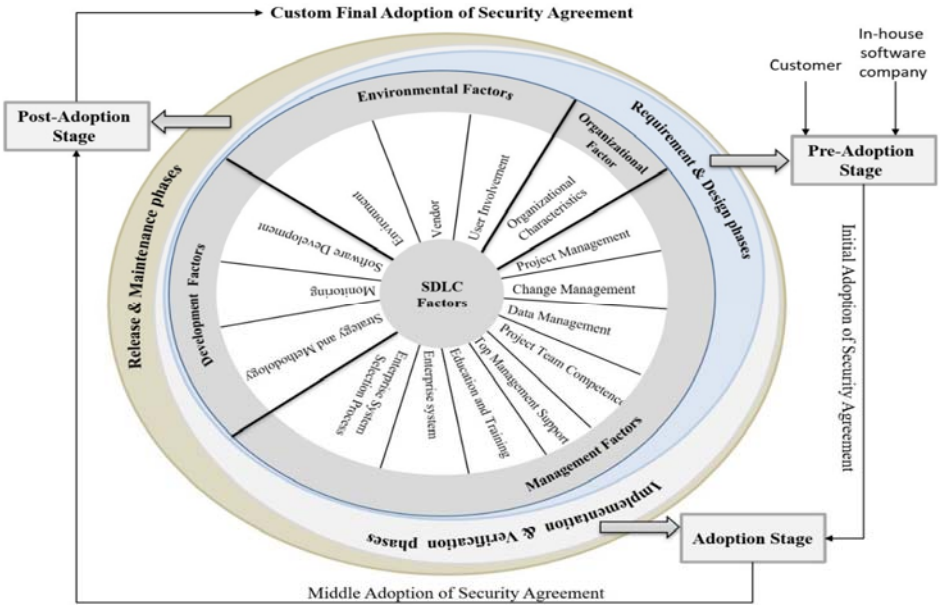

Fig. 5 A Simplified AFS-SDLC framework

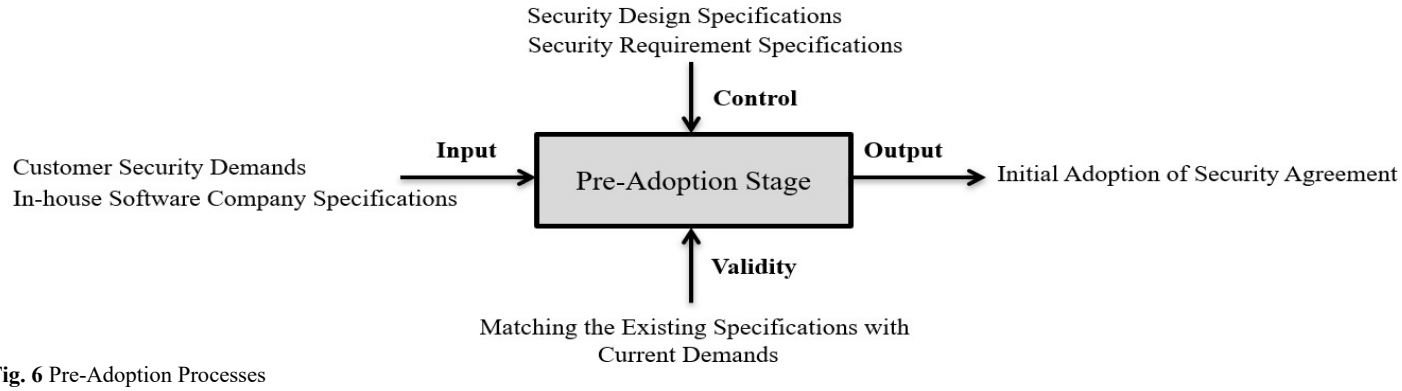

Fig. 6 Pre-Adoption Processes

Table 7 MATCHING CASES RULES

Matching Cases Degree	Weight (w)	Symbol	SAAL
Strongly Matched with existing resources	3	SMR	$1 < Ds \leq 3$
Matched with existing resources	1	MR	$0.5 < Ds \leq 1$
Undecided Matching with existing resources	0.5	UM	$0 < Ds \leq 0.5$
Unmatched with Existing Resources	-0.5	R	$Ds = 0$
		UR	

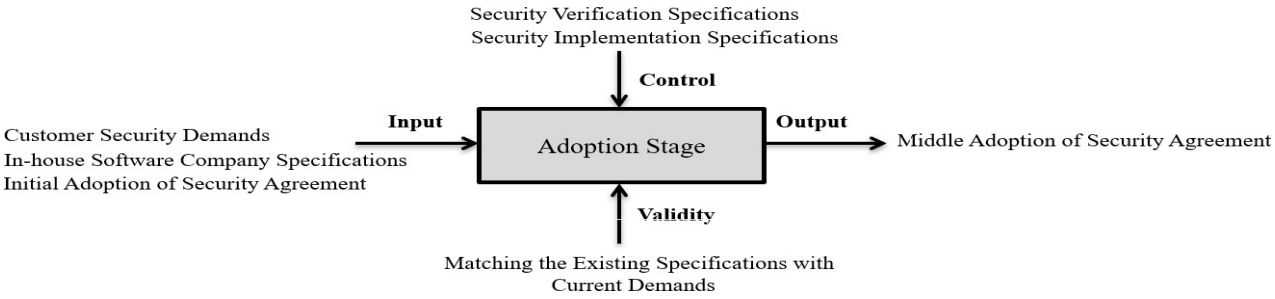

Fig. 7 Adoption Processes

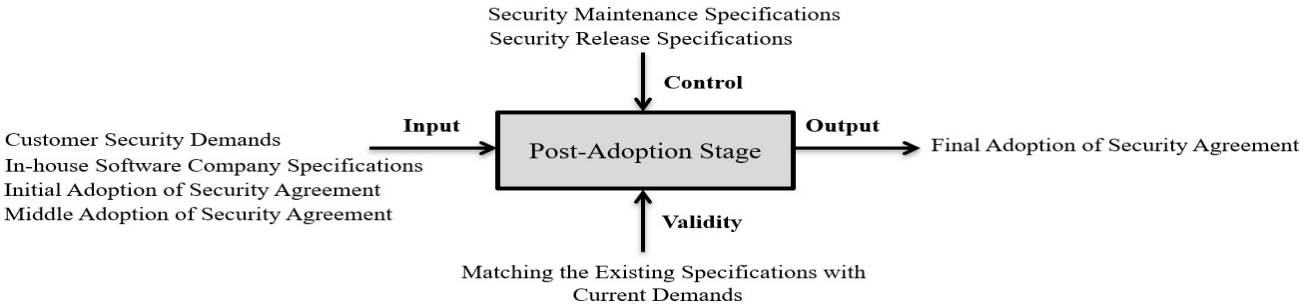

Fig. 8 Adoption Processes

For implementation, the experiment below investigates how in-house software development companies estimate the cus- tomer's security demands after the custom adoption. Sup- pose a customer has 20 Ds in the Pre-adoption phase (5 Ds belong to DSMR, 8 Ds belong to DMR, 5 Ds belong to DUMR, and 2 Ds belong to DUR), suppose a customer has 16 Ds in the Adoption phase (2 Ds belong to DSMR, 3 Ds belong to DMR, 4 Ds belong to DUMR, and 7 Ds belong to DUR), and finally, suppose a customer has 10 Ds in the Post-adoption phases (4 Ds belong to DSMR, 2 Ds belong to DMR, 2 Ds belong to DUMR, and 2 Ds belong to DUR). In the pre-adoption phase:

$SAALP_AVG(20) = ((5*3)+(8*1)+(5*0.5)+(2*-0.5))/(20)$a number of highly ranked digital libraries, that were pub-the obtained result is (1.22) which belongs to SMR match-lished between 2001 and 2022. The scanning process was ing case degree. In the adoption:

$SAALA_AVG(16) = ((2*3)+(3*1)+(4*0.5)+(7*-0.5))/(16)$dressing security issues within the context of information the obtained result is (0.46) which belongs to UMR match- security factors at SMEs for custom-made software clients ing case degree. In the post-adoption:

$SAALPT_AVG(10) = ((4*3)+(2*1)+(2*0.5)+(2*-0.5))/(10)$tic snapshot mapping revealed that a significant number of the obtained result is (1.4) which belongs to SMR matching case degree. Finally, the

$SAAl_avg(20+16+10Ds) = ((1.22)+(0.46)+(1.4))/3.$

The final result is 1.02 which shows that the average of 46 demands in the Strongly Matching with existing resources. Hence, this result helps the decision makers in the project management and top management support to decide with customers about the average power of having custom de- mands which can be adopted from existing security resources.

5. Conclusion

In this article, we present biases, trends, and gaps in security resources at SMEs by conducting a systematic snapshot mapping review. We gathered recent research papers from studies were reviewed in the planning phase with 36 papers, the next highest numbers of papers were in the design and implementation phases respectively by 29, 27 papers. In the release phase, 25 papers were reviewed. In the verification phase, 16 papers were reviewed. The fewest papers were re-viewed during the maintenance phase with 12 papers. Fi- nally, this article proposes a strategic framework for improv- ing the process of adoption of the security

Manuscript received February 5, 2023
Manuscript revised February 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.2.7

factors between clients and in-house software companies at SMEs. The pro- posed framework meets a variety of customers' security de- mands with the in-house software development companies' during the negotiations to elicit the best practices on the agreement.

Research Data Policy and Data Availability Statements

No new data were generated or analysed in support of this research.

Compliance with Ethical Standards

1- There is no conflicts of interest
2- This Research doesn't involve human participants or animals
3- There is no informed consent.

References

[1] Y. Barlette and V. V. Fomin, "The adoption of infor- mation security management standards: A literature re- view," in Information Resources Management: Concepts, Methodologies, Tools and Applications: IGI Global, 2010, pp. 69-90.

[2] M. Tamimi and I. Jebreen, "A Systematic Snapshot of Small Packaged Software Vendors' Enterprises," Interna- tional Journal of Enterprise Information Systems (IJEIS), vol. 14, no. 2, pp. 21-42, 2018.

[3] S. U. Khan, M. Niazi, and R. Ahmad, "Critical success factors for offshore software development outsourcing vendors: A systematic literature review," in Global Soft- ware Engineering, 2009. ICGSE 2009. Fourth IEEE International Conference on, 2009: IEEE, pp. 207-216.

[4] G. Kalus and M. Kuhrmann, "Criteria for software pro- cess tailoring: a systematic review," in Proceedings of the 2013 International Conference on Software and System Process, 2013, pp. 171-180.

[5] M. Tamimi, F. Alghandi, and A. Yaseen, "A SYSTEM- ATIC SNAPSHOT REVIEW OF CUSTOM-MADE SOFTWARE ENTERPRISES FROM THE DEVELOP- MENT PERSPECTIVES," International Journal of In- formation Systems Management Research Develop- ment (IJISMRD), vol. 9, no. 1, pp. 1-22, 2019, doi: 10.24247/ijismrdjun20191.

[6] V. Dimopoulos, S. Furnell, M. Jennex, and I. Kritharas, "Approaches to IT Security in Small and Medium Enter- prises," in AISM, 2004, pp. 73-82.

[7] K. Alnafjan, "An empirical investigation into the adop- tion of Software Engineering Practice in Saudi Ara- bia," International Journal of Computer Science Issues (IJCSI), vol. 9, no. 3, p. 328, 2012.

[8] B. W. Boehm and P. N. Papaccio, "Understanding and controlling software costs," IEEE transactions on soft- ware engineering, vol. 14, no. 10, pp. 1462-1477, 1988.

[9] P. Morrison, D. Moye, R. Pandita, and L. Williams, "Mapping the field of software life cycle security met- rics," Information and Software Technology, vol. 102, pp. 146-159, 2018.

[10] D. Geer, "Are companies actually using secure develop- ment life cycles?," Computer, vol. 43, no. 6, pp. 12-16, 2010.'

[11] M. Tamimi, A. Alzahrani, R. Aljohani, M. Alshahrani, and B. Alharbi, "Security Review based on ISO 27000/ ISO 27001/ ISO 27002 Standards: A Case Study Re- search," International Journal of Management and Ap- plied Science, vol. 5, no. 8, pp. 120-123, 2019.

[12] D.-L. Huang, P.-L. P. Rau, G. Salvendy, F. Gao, and J. Zhou, "Factors affecting perception of information secu- rity and their impacts on IT adoption and security prac- tices," International Journal of Human-Computer Stud- ies, vol. 69, no. 12, pp. 870-883, 2011.

[13]J. H. Sinard and P. Gershkovich, "Custom software de- velopment for use in a clinical laboratory," Journal of Pathology Informatics, vol. 3, 2012.

[14] F. Alghamdi, N. Hamza, and M. Tamimi, "Factors that Influence the Adoption of Information Security on Re- quirement Phase for Custom-Made Software at SMEs," in 2019 2nd International Conference on Computer Ap- plications Information Security (ICCAIS), 2019: IEEE, pp. 1-6.

[15] T. Moutasm and J. Issam, "A Systematic Snapshot of Small Packaged Software Vendors' Enterprises," in Re- search Anthology on Recent Trends, Tools, and Impli- cations of Computer Programming, A. Information Re- sources Management Ed. Hershey, PA, USA: IGI Global, 2021, pp. 1262-1285.

[16] I. Jebreen, M. Tamimi, H. Almajali, and F. Janabi, "In- tegration Testing in Small Packaged Software Vendors: A Systemic Snapshot," in Proceedings of the 2nd Inter- national Conference on E-Education, E-Business and E-Technology, 2018, pp. 106-110.

[17] D. Mellado, C. Blanco, L. E. Sánchez, and E. Fernández-Medina, "A systematic review of security re- quirements engineering," Computer StandardsInter- faces, vol. 32, no. 4, pp. 153-165, 2010.

[18] P. Williams, "Information security governance," Infor- mation security technical report, vol. 6, no. 3, pp. 60-70, 2001.

[19]H. El-Hadary and S. El-Kassas, "Capturing security re- quirements for software systems," Journal of advanced research, vol. 5, no. 4, pp. 463-472, 2014.

[20]I. A. Tondel, M. G. Jaatun, and P.H. Meland, "Security requirements for the rest of us: A survey," IEEE software, vol. 25, no. 1, pp. 20-27, 2008.

[21]C. Onwubiko and A. P. Lenaghan, "Managing security threats and vulnerabilities for small to medium enter- prises," in 2007 IEEE Intelligence and Security Informat- ics, 2007: IEEE, pp. 244-249.

[22]R. L. Jones and A. Rastogi, "Secure coding: building security into the software development life cycle," Infor- mation Systems Security, vol. 13, no. 5, pp. 29-39, 2004.

[23]S. Myagmar, A. J. Lee, and W. Yurcik, "Threat mod- eling as a basis for security requirements," in Sympo- sium on requirements engineering for information secu- rity (SREIS), 2005, vol. 2005: Citeseer, pp. 1-8.

[24]D. Mairiza and D. Zowghi, "An ontological frame- work to manage the relative conflicts between secu- rity and usability requirements," in 2010 Third Inter- national Workshop on Managing Requirements Knowl- edge, 2010: IEEE, pp. 1-6.

[25]Y. Acar, C. Stransky, D. Wermke, M. L. Mazurek, and S. Fahl, "Security developer studies with github users: Ex- ploring a convenience sample," in Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), 2017, pp. 81-95.

[26]G. Sindre and A. L. Opdahl, "Eliciting security require- ments with misuse cases," Requirements engineering, vol. 10, no. 1, pp. 34-44, 2005.

[27]C. Buschow and M. Suhr, "Change management and new organizational forms of content creation," in Media and change management: Springer, 2022, pp. 381-397.

[28]S. Snowden, J. Spafford, R. Michaelides, and J. Hop- kins, "Technology acceptance and m-commerce in an op- erational environment," Journal of Enterprise Informa- tion Management, vol. 19, no. 5, pp. 525-539, 2006.

[29]G. Rezaei and M. R. Hashemi, "An SDN-based Fire- wall for Networks with Varying Security Requirements," in 2021 26th International Computer Conference, Com- puter Society of Iran (CSICC), 2021: IEEE, pp. 1-7.

[30]R. Mitra, "Security Level Identification and Secure Software Design of Safety Critical Embedded Systems: Methodologies and Process," in INCOSE International Symposium, 2017, vol. 27, no. 1: Wiley Online Library, pp. 1300-1313.

[31]K. Popovi c´ and Ž. Hocenski, "Cloud computing secu- rity issues and challenges," in The 33rd International Convention MIPRO, 2010: IEEE, pp. 344-349.

[32]A. Verma and S. Kaushal, "Cloud computing security issues and challenges: a survey," in International Confer- ence on Advances in Computing and Communications, 2011: Springer, pp. 445-454.

[33]H. Hashimi, A. Hafez, and M. Beraka, "A novel view of risk management in software development life cycle," in 2012 12th International Symposium on Pervasive Sys- tems, Algorithms and Networks, 2012: IEEE, pp. 128- 134.

[34]F. Mijnhardt, T. Baars, and M. Spruit, "Organiza- tional characteristics influencing SME information se- curity maturity," Journal of Computer Information Sys- tems, vol. 56, no. 2, pp. 106-115, 2016.

[35]M. Essafi, L. Labed, and H. B. Ghezala, "S2d-prom: A strategy oriented process model for secure software development," in International Conference on Software Engineering Advances (ICSEA 2007), 2007: IEEE, pp. 24-24.

[36]S. Al-Dhahri, M. Al-Sarti, and A. A. Aziz, "Information Security Management System," International Journal of Computer Applications, vol. 158, no. 7, pp. 29-33, 2017.

[37]N. D'Apuzzo, "3D body scanning technology for fash- ion and apparel industry," in Videometrics IX, 2007, vol. 6491: International Society for Optics and Photonics, p. 64910O.

[38]G. Virone, N. Noury, and J. Demongeot, "A system for automatic measurement of circadian activity deviations in telemedicine," IEEE

Transactions on Biomedical En- gineering, vol. 49, no. 12, pp. 1463-1469, 2002.
[39]Y. Cherdantseva and J. Hilton, "A reference model of information assurance security," in 2013 Interna- tional Conference on Availability, Reliability and Secu- rity, 2013: IEEE, pp. 546-555.
[40]M. U. A. Khan and M. Zulkernine, "On selecting appro- priate development processes and requirements engineer- ing methods for secure software," in 2009 33rd Annual IEEE International Computer Software and Applications Conference, 2009, vol. 2: IEEE, pp. 353-358.
[41]G. Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspec- tives," Information Systems Journal, vol. 11, no. 2, pp. 127-153, 2001.
[42]E. B. Fernandez, "A Methodology for Secure Software Design," in Software Engineering Research and Practice, 2004, pp. 130-136.
[43]D.-M. Zhao, J.-H. Wang, J. Wu, and J.-F. Ma, "Us-ing fuzzy logic and entropy theory to risk assessment of the information security," in 2005 International Confer- ence on Machine Learning and Cybernetics, 2005, vol. 4: IEEE, pp. 2448-2453.
[44] L. Wallace, M. Keil, and A. Rai, "How software project risk affects project performance: An investigation of the dimensions of risk and an exploratory model," Decision sciences, vol. 35, no. 2, pp. 289-321, 2004.
[45]L. Wallace and M. Keil, "Software project risks and their effect on outcomes," Communications of theACM,vol. 47, no. 4, pp. 68-73, 2004.
[46]M. S. Saleh and A. Alfantookh, "A new comprehensive framework for enterprise information security risk man- agement," Applied computing and informatics, vol. 9, no. 2, pp. 107-118, 2011.
[47]S. Islam and W. Dong, "Human factors in software se- curity risk management," in Proceedings of the first in- ternational workshop on Leadership and management in software architecture, 2008: ACM, pp. 13-16.
[48]M. Sulayman, C. Urquhart, E. Mendes, and S. Seidel, "Software process improvement success factors for small and medium Web companies: A qualitative study," Infor- mation and Software Technology, vol. 54, no. 5, pp. 479- 500, 2012.
[49]S. Mittal, P. K. Das, V. Mulwad, A. Joshi, and T. Finin, "Cybertwitter: Using twitter to generate alerts for cyber- security threats and vulnerabilities," in 2016 IEEE/ACM International Conference on Advances in Social Net- works Analysis and Mining (ASONAM), 2016: IEEE, pp. 860-867.
[50]R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. Cano, "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)," in 2017 International Conference on Informa- tion Systems and Computer Science (INCISCOS), 2017: IEEE, pp. 253-259.
[51]D. J. Sebastian and A. Hahn, "Exploring emerging cy- bersecurity risks from network-connected DER devices," in 2017 North American Power Symposium (NAPS), 2017: IEEE, pp. 1-6.
[52]D. Krenczyk and A. Dobrza ńska-Danikiewicz, "The deadlock protection method used in the production sys- tems," Journal of Materials Processing Technology, vol. 164, pp. 1388-1394, 2005.
[53]D. Krenczyk and B. Skolud, "Production preparation and order verification systems integration using method based on data transformation and data mapping," in In- ternational Conference on Hybrid Artificial Intelligence Systems, 2011: Springer, pp. 397-404.
[54]J. J. Pauli and D. Xu, "Misuse case-based design and analysis of secure software architecture," in International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II, 2005, vol. 2: IEEE, pp. 398-403.
[55]M. Almorsy, J. Grundy, and A. S. Ibrahim, "Automated software architecture security risk analysis using formal- ized signatures," in 2013 35th International Conference on Software Engineering (ICSE), 2013: IEEE, pp. 662- 671.
[56]D. Xu and K. E. Nygard, "Threat-driven modeling and verification of secure software using aspect-oriented Petri nets," IEEE transactions on software engineering, vol. 32, no. 4, pp. 265-278, 2006
[57]D. Concha, J. Espadas, D. Romero, and A. Molina, "The e-HUB evolution: from a custom software architecture to a software-as-a-service implementation," Computers in Industry, vol. 61, no. 2, pp. 145-151, 2010
[58]M. J. Callaghan, J. Harkin, E. McColgan, T. M. McGin- nity, and L. P. Maguire, "Client–server architecture for collaborative remote experimentation," Journal of Net- work and Computer Applications, vol. 30, no. 4, pp. 1295-1308, 2007.
[59]D.-R. Liu, M.-Y. Wu, and S.-T. Lee, "Role-based autho- rizations for workflow systems in support of task-based separation of duty," Journal of systems and software, vol. 73, no. 3, pp. 375-387, 2004.
[60]H. Studiawan, C. Payne, and F. Sohel, "Graph clustering and anomaly detection of access control log for forensic purposes," Digital Investigation, vol. 21, pp. 76-87, 2017.
[61]V. Amrutiya, S. Jhamb, P. Priyadarshi, and A. Bhatia, "Trustless Two-Factor Authentication Using Smart Con- tracts in Blockchains," in 2019 International Conference on Information Networking (ICOIN), 2019: IEEE, pp. 66-71.
[62]W. Xu, X. Zhang, H. Hu, G.-J. Ahn, and J.-P. Seifert, "Remote attestation with domain-based integrity model and policy analysis," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 3, pp. 429-442, 2011.
[63]M. P. Papazoglou, P. Traverso, S. Dustdar, and F. Ley- mann, "Service-oriented computing: State of the art and research challenges," Computer, vol. 40, no. 11, pp. 38- 45, 2007.
[64]D. Fensel and C. Bussler, "The web service modeling framework WSMF," Electronic Commerce Research and Applications, vol. 1, no. 2, pp. 113-137, 2002.
[65]A. Chechulin, I. Kotenko, and V. Desnitsky, "An ap- proach for network information flow analysis for sys- tems of embedded components," in International Con- ference on Mathematical Methods, Models, and Archi- tectures for Computer Network Security, 2012: Springer, pp. 146-155.
[66]Y. Deng, J. Wang, J. J. Tsai, and K. Beznosov, "An ap- proach for modeling and analysis of security system ar- chitectures," IEEE Transactions on knowledge and data engineering, vol. 15, no. 5, pp. 1099-1119, 2003.
[67]W. Xiong and R. Lagerström, "Threat modeling–A sys- tematic literature review," Computers Security, vol. 84, pp. 53-69, 2019.
[68]R. Scandariato, K. Wuyts, and W. Joosen, "A descrip- tive study of Microsoft's threat modeling technique," Requirements Engineering, vol. 20, no. 2, pp. 163-180, 2015.
[69]D. Dhillon, "Developer-driven threat modeling: Lessons learned in the trenches," IEEE Security Privacy, vol. 9, no. 4, pp. 41-47, 2011.
[70]P. H. Meland and J. Jensen, "Secure software design in practice," in 2008 Third International Conference on Availability, Reliability and Security, 2008: IEEE, pp. 1164-1171.
[71]A. Dautovic, R. Plosch, and M. Saft, "Automatic check- ing of quality best practices in software development documents," in 2011 11th international conference on quality software, 2011: IEEE, pp. 208-217.
[72]R. S. Geiger, N. Varoquaux, C. Mazel-Cabasse, and C. Holdgraf, "The types, roles, and practices of documen- tation in data analytics open source software libraries," Computer Supported Cooperative Work (CSCW), vol. 27, no. 3-6, pp. 767-802, 2018.
[72]R. S. Geiger, N. Varoquaux, C. Mazel-Cabasse, and C. Holdgraf, "The types, roles, and practices of documen- tation in data analytics open source software libraries," Computer Supported Cooperative Work (CSCW), vol. 27, no. 3-6, pp. 767-802, 2018.
[73]B. McFee, J. W. Kim, M. Cartwright, J. Salamon, R. M. Bittner, and J. P. Bello, "Open-source practices for music signal processing research: Recommendations for trans- parent, sustainable, and reproducible audio research," IEEE Signal Processing Magazine, vol. 36, no. 1, pp. 128-137, 2018.
[74]D. Quiñones and C. Rusu, "How to develop usabil- ity heuristics: A systematic literature review," Computer Standards Interfaces, vol. 53, pp. 89-122, 2017.
[75]M. A. Sharkh, M. Jammal, A. Shami, and A. Ouda, "Re- source allocation in a network-based cloud computing environment: design challenges," IEEE Communications Magazine, vol. 51, no. 11, pp. 46-52, 2013.
[76]S. Lipner, "The trustworthy computing security devel- opment lifecycle," in 20th Annual Computer Security Applications Conference, 2004: IEEE, pp. 2-13.
[77]A. Castaldo, G. De Luca, and B. Barile, "DOES INITIAL ACCESS TO BANK LOANS PREDICT START-UPS'FUTURE DEFAULT PROBABILITY? EVIDENCE FROM ITALY," Contemporary Economic Policy, 2020.
[78]P. B. Prince and S. J. Lovesum, "Privacy Enforced Ac- cess Control Model for Secured Data Handling in Cloud- Based Pervasive Health Care System," SN Computer Sci- ence, vol. 1, no. 5, pp. 1-8, 2020.
[79]E. Markakis et al., "Acceleration at the edge for support- ing smes security: The fortika paradigm," IEEE Commu- nications Magazine, vol. 57, no. 2, pp. 41-47, 2019.
[80]T. Brown, A. Kogan, Y. Lev, and V. Luchangco, "Inves- tigating the performance of hardware transactions on a multi-socket machine," in Proceedings of the 28th ACM Symposium on Parallelism in Algorithms and Architec- tures, 2016: ACM, pp. 121-132.
[81]H. Shahriar and M. Zulkernine, "Mitigating program se- curity vulnerabilities: Approaches and challenges," ACM Computing Surveys (CSUR), vol. 44, no. 3,

p. 11,2012.
[82]E. Kaynak, E. Tatoglu, and V. Kula, "An analysis of the factors affecting the adoption of electronic commerce by SMEs: Evidence from an emerging market," Inter-2005.
[83]A. K. Jain and D. Shanbhag, "Addressing security and privacy risks in mobile applications," IT Professional, vol. 14, no. 5, pp. 28-33, 2012.
[84]C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in 2010 INFOCOM IEEE conference on computer communica- tions workshops, 2010: IEEE, pp. 1-6.
[85]Y. Hashimoto et al., "Safety securing approach against cyber-attacks for process control system," Computers Chemical Engineering, vol. 57, pp. 181-186, 2013.
[86]D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An in- tegrated security system of protecting smart grid against cyber attacks," in 2010 Innovative Smart Grid Technolo- gies (ISGT), 2010: IEEE, pp. 1-7.
[87]M. Khouzani, S. Sarkar, and E. Altman, "Optimal dis- semination of security patches in mobile wireless net- works," IEEE Transactions on Information Theory, vol. 58, no. 7, pp. 4714-4732, 2012.
[88]B. Brykczynski and R. A. Small, "Reducing internet- based intrusions: Effective security patch management," IEEE software, vol. 20, no. 1, pp. 50-57, 2003.
[89]D. P. Gilliam, T. L. Wolfe, J. S. Sherif, and M. Bishop, "Software security checklist for the software life cycle," in WET ICE 2003. Proceedings. Twelfth IEEE Interna- tional Workshops on Enabling Technologies: Infrastruc- ture for Collaborative Enterprises, 2003., 2003: IEEE, pp. 243-248.
[90]S. Bellovin, "Security by checklist," IEEE Security Pri- vacy, vol. 6, no. 2, pp. 88-88, 2008.
[91]R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshe- hhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA), 2018: IEEE, pp. 1- 8.
[92]C. Jiang and P. Zhang, "VNE Solution for Network Differentiated QoS and Security Requirements from the Perspective of Deep Reinforcement Learning," in QoS- Aware Virtual Network Embedding: Springer, 2021, pp. 61-84.
[93]S. Bu and B.-H. Wang, "Improving the security of chaotic encryption by using a simple modulating method," Chaos, Solitons Fractals, vol. 19, no. 4, pp. 919-924, 2004.
[94]S. M. Farooq, S. Nabirasool, S. Kiran, S. S. Hussain, and T. S. Ustun, "MPTCP based mitigation of denial of service (DoS) attack in PMU communication net- works," in 2018 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), 2018: IEEE, pp. 1-5.
[95]P. Danzi, M. Angjelichinoski, Č. Stefanović, T. Drag-national marketing review, vol. 22, no. 6, pp. 623-640,
[96]M. Felderer and E. Fourneret, "A systematic classifica- tion of security regression testing approaches," Interna- tional Journal on Software Tools for Technology Trans- fer, vol. 17, no. 3, pp. 305-319, 2015.
[97]J. Highsmith and A. Cockburn, "Agile software devel- opment: The business of innovation," Computer, vol. 34, no. 9, pp. 120-127, 2001.
[98]K. Mohan, B. Ramesh, and V. Sugumaran, "Integrat- ing software product line engineering and agile develop- ment," IEEE software, vol. 27, no. 3, pp. 48-55, 2010.
[99]M. E. Delamaro, J. Maidonado, and A. P. Mathur, "In- terface mutation: An approach for integration testing," IEEE transactions on software engineering, vol. 27, no. 3, pp. 228-247, 2001.
[100]L. Shaul and D. Tauber, "CSFs along ERP life-cycle in SMEs: a field study," Industrial Management Data Sys- tems, vol. 112, no. 3, pp. 360-384, 2012.
[101]H. Holm, T. Sommestad, J. Almroth, and M. Persson, "A quantitative evaluation of vulnerability scanning," In- formation Management Computer Security, vol. 19, no. 4, pp. 231-247, 2011.
[102]J. Fonseca, M. Vieira, and H. Madeira, "Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks," in 13th Pacific Rim inter- national symposium on dependable computing (PRDC 2007), 2007: IEEE, pp. 365-372.
[103]U. Bayer, A. Moser, C. Kruegel, and E. Kirda, "Dy- namic analysis of malicious code," Journal in Computer Virology, vol. 2, no. 1, pp. 67-77, 2006.
[104]S. C. Talukder and M. M. Rahman, "Customer re- quirements oriented component based software develop- ment life cycle model," in 2015 International Conference on Computers, Communications, and Systems (ICCCS), 2015: IEEE, pp. 61-68.
[105]M. Geogy and A. Dharani, "Prominence of each phase in Software development life cycle contributes to the overall quality of a product," in 2015 International Con- ference on Soft-Computing and Networks Security (IC-SNS), 2015: IEEE, pp. 1-2.
[106]A.-K. Groven, K. Haaland, R. Glott, and A. Tan- nenberg, "Security measurements within the framework of quality assessment models for free/libre open source software," in Proceedings of the fourth european conference on software architecture: Companion volume, 2010: ACM, pp. 229-235.
[107]S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications, vol. 34, no. 1, pp. 1-11, 2011.
[108]J. E. Mateer and R. W. Jones, "Information systems, indirect risks and safety: An 8-step safety management process," in 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2018: IEEE, pp. 352-357.
[109]P. Chapman, "Are your IT staff ready for the pandemic-driven insider threat?," Network Security, vol. 2020, no. 4, pp. 8-11, 2020.
[110]A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. H. Park, "Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and No- tification in Intelligent Transportation Systems," IEEE Sensors Journal, 2020.
[111]G. K. Verma, B. Singh, N. Kumar, M. S. Obaidat, D. He, and H. Singh, "An efficient and provable certificate- based proxy signature scheme for IIoT environment," In- formation Sciences, vol. 518, pp. 142-156, 2020.
[112]H. Pan, Y. Zhu, Z. Pan, and X. Lu, "An efficient scheme of merging multiple public key infrastructures in ERP," in International Conference on Web-Age Informa- tion Management, 2005: Springer, pp. 919-924.
[113]H. Liu and H. Goto, "Certificate-based, disruption- tolerant authentication system with automatic CA certifi- cate distribution for Eduroam," in 2014 IEEE 38th In- ternational Computer Software and Applications Confer- ence Workshops, 2014: IEEE, pp. 169-173.
[114]U. Somani, K. Lakhani, and M. Mundra, "Implement- ing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Comput- ing," in 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010), 2010: IEEE, pp. 211-216.
[115]B. Gastermann, M. Stopper, A. Kossik, and B. Katal- inic, "Secure implementation of an on-premises cloud storage service for small and medium-sized enterprises," Procedia Engineering, vol. 100, pp. 574-583, 2015.
[116]N. Kundu, S. K. Debnath, D. Mishra, and T. Choud- hury, "Post-quantum digital signature scheme based on multivariate cubic problem," Journal of Information Se- curity and Applications, vol. 53, p. 102512, 2020.
[117]T. Kwon and J.-i. Lee, "Practical digital signature gen- eration using biometrics," in International Conference on Computational Science and Its Applications, 2004: Springer, pp. 728-737
[118]R. Kolluru and P. H. Meredith, "Security and trust management in supply chains," Information Manage- ment Computer Security, vol. 9, no. 5, pp. 233-236, 2001
[119]A. Ramtohul and K. Soyjaudah, "Information security governance for e-services in southern African develop- ing countries e-Government projects," Journal of Science Technology Policy Management, vol. 7, no. 1, pp. 26-42, 2016.
[120]M. Najjar, "A blue print practical implementation of PKI using open PGP at University of Tabuk," in 2013 Science and Information Conference, 2013: IEEE, pp. 358-362.
[121]D. Chadwick, A. Otenko, and E. Ball, "Role-based ac- cess control with X. 509 attribute certificates," IEEE In- ternet Computing, vol. 7, no. 2, pp. 62-69, 2003.
[122]R. Lippmann, S. Webster, and D. Stetson, "The ef- fect of identifying vulnerabilities and patching software on the utility of network intrusion detection," in Interna- tional Workshop on Recent Advances in Intrusion Detection, 2002: Springer, pp. 307-326.
[123]D. Novikov, R. V. Yampolskiy, and L. Reznik, "Arti- ficial intelligence approaches for intrusion detection," in 2006 IEEE Long Island Systems, Applications and Tech- nology Conference, 2006: IEEE, pp. 1-8.
[124]J. Witschey, S. Xiao, and E. Murphy-Hill, "Technical and personal factors influencing developers' adoption of security tools," in Proceedings of the 2014 ACM Work- shop on Security Information Workers, 2014: ACM, pp. 23-26.
[125]E. Albrechtsen and J. Hovden, "The information secu- rity digital divide between information security managers and users," Computers Security, vol. 28, no. 6, pp. 476- 490, 2009.
[126]R. Rivera-Castro et al., "Topology-Based Clusterwise Regression for User Segmentation and Demand Forecast- ing," in 2019 IEEE International Conference on Data Sci- ence and Advanced Analytics (DSAA), 2019: IEEE, pp. 326-336.
[127]B. Uchendu, J. R. Nurse, M. Bada, and S. Furnell, "De- veloping a cyber security culture: Current practices and future needs," Computers Security, vol. 109, p. 102387, 2021.
[128]O. Temizkan, R. L. Kumar, S. Park, and C. Subrama- niam, "Patch release

behaviors of software vendors in re- sponse to vulnerabilities: An empirical analysis," Journal of management information systems, vol. 28, no. 4, pp. 305-338, 2012.

[129]A. Khajeh-Hosseini, I. Sommerville, J. Bogaerts, and P. Teregowda, "Decision support tools for cloud migra-tion in the enterprise," in 2011 IEEE 4th International Conference on Cloud Computing, 2011: IEEE, pp. 541- 548.

[130]A. Kusumawati, "Information Security Awareness: Study on a Government Agency," in 2018 International Conference on Sustainable Information Engineering and Technology (SIET), 2018: IEEE, pp. 224-229.

[131]H. Aldawood and G. Skinner, "Educating and raising awareness on cyber security social engineering: A lit- erature review," in 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 2018: IEEE, pp. 62-68.

[132]R. Bitton, A. Finkelshtein, L. Sidi, R. Puzis, L. Rokach, and A. Shabtai, "Taxonomy of mobile users' se- curity awareness," Computers Security, vol. 73, pp.266- 293, 2018.

[133]P. Baillette, Y. Barlette, and A. Leclercq- Vandelannoitte, "Bring your own device in organi- zations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users," Interna- tional Journal of Information Management, vol. 43, pp. 76-84, 2018.

[134]H.-S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' infor- mation security practice behavior," Computers Security, vol. 28, no. 8, pp. 816-826, 2009.

[135]J. Shropshire, M. Warkentin, and S. Sharma, "Person- ality, attitudes, and intentions: Predicting initial adoption of information security behavior," Computers Security, vol. 49, pp. 177-191, 2015.

[136]F. F. H. Nah, S. Faja, and T. Cata, "Characteristics of ERP software maintenance: a multiple case study," Jour- nal of software maintenance and evolution: research and practice, vol. 13, no. 6, pp. 399-414, 2001.

[137]E. Meneses, O. Sarood, and L. V. Kalé, "Energy profile of rollback-recovery strategies in high performance com- puting," Parallel Computing, vol. 40, no. 9, pp. 536-547, 2014.