applied sciences

MDPI

Article

Secure Global Software Development: A Practitioners' Perspective

Mamoona Humayun [1,*], Mahmood Niazi [2,3], Mohammed Assiri [4,5] and Mariem Haoues [5]

[1] Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakaka 72388, Saudi Arabia
[2] Department of Information and Computer Science, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[3] Interdisciplinary Research Centre for Intelligent Secure Systems, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[4] Department of Computer Science, College of Sciences and Humanities-Aflaj, Prince Sattam bin Abdulaziz University, Al-Kharjj 16278, Saudi Arabia
[5] Department of Software Engineering, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia
* Correspondence: mahumayun@ju.edu.sa

Abstract: Global software development (GSD) is rapidly becoming standard practice in the software industry due to its many potential benefits. However, one of the biggest challenges in GSD projects is to explicitly include security in the different phases of the global software development life cycle (GSDLC). To make GSD projects secure and successful, it is necessary to identify secure software development (SSD) practices vital to GSD project success. This article aims to identify SSD practices critical for GSD projects. To do this, we selected 36 security practices vital to the security of non-GSD projects from existing scientific and grey literature on software security. From the identified security practices, we shortlisted the security practices which are critical for GSD projects based on practitioners' opinions using an online survey. Fifty-four GSD practitioners participated in this survey. Participants who evaluated these practices were asked to score each SSD practice on a four-point scale to indicate its relevance to GSD projects. The results obtained from the survey uncovered critical SSD practices that are primarily applicable to GSD projects. Our findings reveal variations of opinion among GSD practitioners with varying experience and company size regarding the importance of selected security practices for GSD. According to study findings, 16/36 practices are critical for GSD projects. These identified security practices belong to various phases of GSDLC.

Keywords: global software development; secure software development; empirical investigation; SSD practices

Citation: Humayun, M.; Niazi, M.; Assiri, M.; Haoues, M. Secure Global Software Development: A Practitioners' Perspective. *Appl. Sci.* **2023**, *13*, 2465. https://doi.org/10.3390/app13042465

Academic Editor: Paolino Di Felice

Received: 26 January 2023
Revised: 13 February 2023
Accepted: 13 February 2023
Published: 14 February 2023

1. Introduction

GSD is a method in which groups of knowledge workers from many parts of the globe work together to develop software that businesses may sell [1,2]. It provides several advantages to client organizations that outsource development work to vendor companies, including cost savings, 24/7 development, and access to global resources [3,4]. GSD is not a simple undertaking, and it has several intrinsic difficulties resulting from temporal, organizational, sociocultural, and geographic distances, as shown in Figure 1 [1,5–8]. GSD operates at different functional levels, including country, organization, and team, so it is critical to understand and assess GSD challenges [5,9–11]. One of the challenges is SSD since teams are spread, and security responsibilities are distributed among these dispersed teams [12,13].

Although a wide range of software development activities is outsourced, recent research reveals that security is one of the variables leading to outsourcing failure [14–18]. This is unsurprising, given that integrating security into the whole SDP significantly influences all SDPs' efficacy, including GSD [19–21]. This research aims to give software practitioners, customers, and suppliers a set of best practices to help them manage security in global projects. Identifying these practices will help GSD businesses prepare for security management from a global perspective. This will make it easier to complete GSD initiatives and foster the establishment of long-term ties across geographically dispersed enterprises.

Figure 1. Key difficulties faced in GSD.

Paper Contribution

To leverage the potential of GSD, it is inevitable to address the security issues involved in GSDLC. To fill this gap, this study aims to elicit security requirements for SDLC and evaluate the importance of selected security practices for GSD projects. To compile the list of possible security practices, we have previously figured out the security practices for SDLC in our earlier research [22]. Additionally, we looked into grey literature to get an idea of what experts are saying. Thirty practices were selected from our previous analysis, and six additional practices were added from the grey literature for a total of 36 security best practices for GSD. The complete list of selected practices is given in Appendix A Table A1 of this paper. This study examines if the standard security practices identified for use in non-global projects can also be used in GSD projects. To determine the value of a particular practice for inclusion in GSDLC, we assessed each practice based on its importance to GSDLC. According to the literature on GSD, to maintain security in GSDLC, not only is the security of information communication necessary but incorporating security into GSDLC is also inevitable for the success of GSD projects. To achieve the desired objective, we have defined the following research questions

- RQ1: What are the most critical security practices for GSD projects?
- RQ2: Is there a correlation between the size of the GSD organization and identified security practices?
- RQ3: Is there a correlation between the practitioners' experience and identified security practices?

The rest of this paper is laid out as follows: Section 2 provides context for the research. In Section 3, we detail our research methodology. The findings of the study are presented

in Section 4, and Section 5 provides an analysis of the findings. The last section of the paper discusses implications for further research. Acronyms used in this research are defined in full in Table 1.

Table 1. List of acronyms.

Acronyms	Used for
AES	Advance encryption standard
FAHP	Fuzzy analytical hierarchy process
GSD	Global software development
GSDLC	Global software development lifecycle
IT	Information technology
ITOOP	Information technology offshore outsourcing process
RE	Requirement engineering
ROI	Return on investment
SAM	Security assurance model
SDLC	Software development lifecycle
SDP	Software development process
SLR	Systematic literature review
SSD	Secure software development
SSDLC	Secure software development lifecycle

2. Background and Related Work

According to prior research, the proportion of software projects delivered on schedule and under budget increased over time [23]. Despite this progress, numerous projects ran into the schedule and budget constraints or were only partly finished. The complexity and change management made to the SDP are two of the most common causes of project failure. This complexity is heightened when multinational corporations produce software in a dispersed environment. Security is vital for the success of software development, which is a crucial component of every project. According to research [4,7,24], due to globalization, GSD businesses must strengthen GSDLC processes to deal with various roles, cooperation requirements, improved decision-making, changing domain knowledge, cultural understanding, and organizational structures. To strengthen security in GSD, we are interested in identifying various practices which can be incorporated into GSDLC.

2.1. Software Development Security Practices

The identified 36 security practices in this research correlate to the five phases of the SDLC: requirement, design, coding, testing and integration, and deployment. Ten of these practices pertain to the requirement phase; eight pertain to software design; seven pertain to secure coding; five pertain to increasing the security of the testing and integration phase; and six pertain to improving the security of the software deployment phase. So far, we have not come across any study that particularly implemented security best practices in a GSD setting. There are, however, several studies on SSDLC for non-outsourced projects [25–28]. Researching and identifying security practices critical for GSD projects is vital because various GSD companies have failed to achieve the expected results due to several issues. One of the causes of such failures is frequently related to security issues.

2.2. Selection Criteria for Choosing Security Practices for GSD

Experts say the "degree of relevance" of a certain security practice (high to zero) may be used as a criterion for assessing the degree of relevance of specific security practice for a GSD project [29,30]. Researchers and practitioners may use the degree of relevance of security practices to understand better the applicability of different security approaches in various phases of GSD projects.

2.3. Related Work

Various research on SSD has been conducted during the previous two decades, but none specifically focused on SSD in GSD. Existing research addresses GSD's secure communication or focuses primarily on integration failure. Some of these studies are discussed in the following sections.

Ghmaei et al. [31] proposed a Blockchain approach for the security of GSD projects. To determine the influence of Blockchain on GSD initiatives, the authors conducted interviews with academia professionals and case studies with industry practitioners. They identified ten essential aspects of GSD that might be efficiently addressed by using Blockchain technology in GSD. The findings of academic researchers and industry practitioners were compared, and the results ($W = 0.86$, $p = 0.005$) revealed a high agreement between academic researchers' and industry practitioners' knowledge. Furthermore, based on the outcomes of both investigations, a hypothetical model was built that revealed a favorable association between Blockchain deployment and the GSD domain.

The elements that contribute to integration failure in GSD projects were thoroughly investigated in research [32]. An in-depth evaluation of the existing literature was conducted. Furthermore, the authors performed an industry survey to better understand the elements contributing to integration failure. This study made a significant contribution to the development of a precise taxonomy of 40 integration failure causes. A deeper understanding of the interactions between the different components is made possible by categorization, which aids in developing a comprehensive solution to integration difficulties in the context of GSD.

The article [33] addresses the security of GSD requirement information, which presents a solution to the primary challenge. According to this paper, the most pressing problem is the hacking of sensitive customer information, which has the potential to cause significant financial and societal damage. As a result, this article delivers cloud security via data encryption and the deployment of a tool over the cloud, which will give considerable protection to the whole global content management system. The study's major findings are provided in terms of how hackers penetrate such systems and what countermeasures must be taken. The algorithmic development provides random information storage at multiple cloud nodes to safeguard clients' data files, which is essential for security reasons.

Several risk issues related to outsourcing have been outlined in paper [34], with security and privacy being one of these considerations. This study provides a methodology for analyzing the primary risk variables that must be considered when selecting whether or not to outsource IT tasks to a third-party offshore location. In addition, some of the precautionary steps the organization should implement to mitigate or limit these risks were mentioned. The study presents a synthesis and analysis of the numerous perspectives on offshore IT outsourcing that have been expressed in the literature on various aspects of the risks associated with this kind of outsourcing.

According to the paper [35], information security is critical when outsourcing to other countries. This paper aims to identify information security risks and provide protections for IT offshore outsourcing. To begin, information security risks and protections associated with IT offshore outsourcing are identified via a literature study and interviews with subject matter experts. And an ITOOP model was designed to logically connect these information security concerns based on flow and job analysis in the client and vendor environments. Additionally, safeguards are built to defend against information security threats by associating them with certain security risks. The ITOOP model developed in this research will assist decision-makers in offshore IT outsourcing. It will also help identify potential security risks in offshore processes and incorporate prudent safeguard decisions to protect data and improve security levels.

The study [36] attempts to objectively evaluate and rank the risks that might have a detrimental influence on the software security elements of SDLC within the framework of GSD. To meet the research's aims, an industrial empirical study was undertaken to assess

the effect of software security vulnerabilities on each step of SDLC. In addition, the FAHP was used to prioritize the SDLC software security risk list. This study's findings and analyses give a ranked-based decision-making framework to aid practitioners in prioritizing the most significant security concerns.

The paper [37] examined the most popular software security models. It presents a new SAM for SDP that is flexible to all modern circumstances, with a focus on GSD vendor organizations. The SAM of SDP was created by examining eleven well-known development models and evaluating SLR and questionnaire survey findings. The SAM of Software Development has seven degrees of security assurance. The security assurance levels of SAM for software development are comprised of 388 practices and 46 key software security threats. The suggested SAM of Software development was evaluated using a Motorola-developed methodology that evaluates the current status of a company's software operations and identifies improvement opportunities. Three case studies on software development businesses were undertaken utilizing data from actual software development projects to analyze the outcomes of a practical experiment in each organization. The findings of the case studies demonstrate that the proposed SAM of SDP assists in measuring an organization's security assurance level. In addition, it may serve as a foundation for the development of new software security mechanisms by researchers.

The authors of paper [38] enable GSD on the cloud and explain and compare several GSD security issues. This study recommends cloud-computing as a solution to the numerous issues posed by GSD and explores a variety of encryption strategies for maintaining data security. This research uses AES to safeguard the data of global software developers in the cloud, allowing for secure communication and data exchange.

Important RE practices for GSD projects are outlined in the article [39]. This research collected data from 56 RE specialists of GSD projects using an online survey form. The survey comprised 66 RE practices recognized for non-GSD projects by Sommerville et al. On a four-point scale, participants were asked to assess the relevance of each RE practice within the context of GSD projects. This study established a set of six essential RE practices that are primarily concerned with the management of GSD. Standardizing requirement documents to eliminate requirements discrepancies and enhance communication in various and geographically dispersed GSD project contexts is a recurrent topic that emerges from the RE experts' examination of comments. The analysis revealed that not all 66 RE best practices apply to GSD projects. Developing and executing the situation-specific RE procedures for GSD projects, however, requires a solid grasp of the recognized RE practices.

After reviewing the literature on SSD in GSD, we discovered that most current research concentrates on typical GSD concerns e.g., secure communication, secure transmission, and storage of data, solutions to cultural and temporal issues, etc. Only a few studies have been conducted on privacy and security, but their primary emphasis has been on secure communication of information rather than SSD. To the best of our knowledge, no research has been conducted to identify SSD approaches for GSD. To fill this gap, we have presented a set of practices in our Secure GSDLC and verified these practices in real-world GSD situations in the next section. In Table 2, we provide a comparison of the above-mentioned studies to provide a state-of-the-art picture of the area under study.

Table 2. Comparison of existing studies.

Ref#	Problem	Paper Contribution	GSD/Non-GSD	Solution Provided	Research Methods Used
[31]	Security and management of GSD	Identified a total of 10 of the most crucial GSD issues that may be resolved successfully by putting blockchain technology to use.	GSD	BlockChain implementation	Interview+ case study
[32]	Integration failures	Exploring integration failure challenges	GSD	Taxonomy of 40 integration failure factors.	Review+ Industrial survey
[33]	Global Software Development Requirement Information.	Provides cloud security by encryption of data and tool deployment over the cloud	GSD	Secured Cloud Approach	Framework
[34]	GSD Risks assessment	Highlighted primary offshore IT outsourcing risk categories, addressed several risk variables within each category and gave a broad framework for studying risk factors.	GSD	provide a framework for risk assessment of offshore IT outsourcing	Review
[35]	Information security while outsourcing	Discovering information security risk factors and providing security practices for outsourcing	GSD	ITOOP model with information security risks and security solutions	Literature review+ Interviewing
[36]	GSD security	Identification of security risks	GSD	Ranked-based decision aiming framework for security risks	Industrial empirical study
[37]	Security Attacks	Analyzed existing development models	GSD	Security assurance model for GSD	3 case studies
[38]	Secure data sharing in GSD	Facilitate GSD in the cloud	GSD cloud	AES Encryption	Experiment
[39]	RE in GSD	Identified RE practices for GSD security	GSD	Analyzed the impact of company size, developer expertise, and company type on identified GSD practices	Online survey questionnaire

3. Proposed Methodology

To know whether the SSDLC practices used for non-global projects are also suitable for GSD practices, we followed the three-step methodology mentioned in Figure 2. In the first stage, we identified the security challenges faced in all phases of SDLC and solutions to mitigate these challenges. Next, we posed research questions to determine whether the identified security practices work well for GSD projects. Finally, we shortlisted the security practices that must be used in the GSD project lifecycle to make it secure. This selection was made on the basis of the replies submitted. The responses of 54 GSD security specialists were examined, and security measures with a frequency of at least 40 percent were selected as essential GSD security practices. By 40%, we mean that more than 40% of the questioned experts thought the practice to be essential.

Below we describe these steps in detail

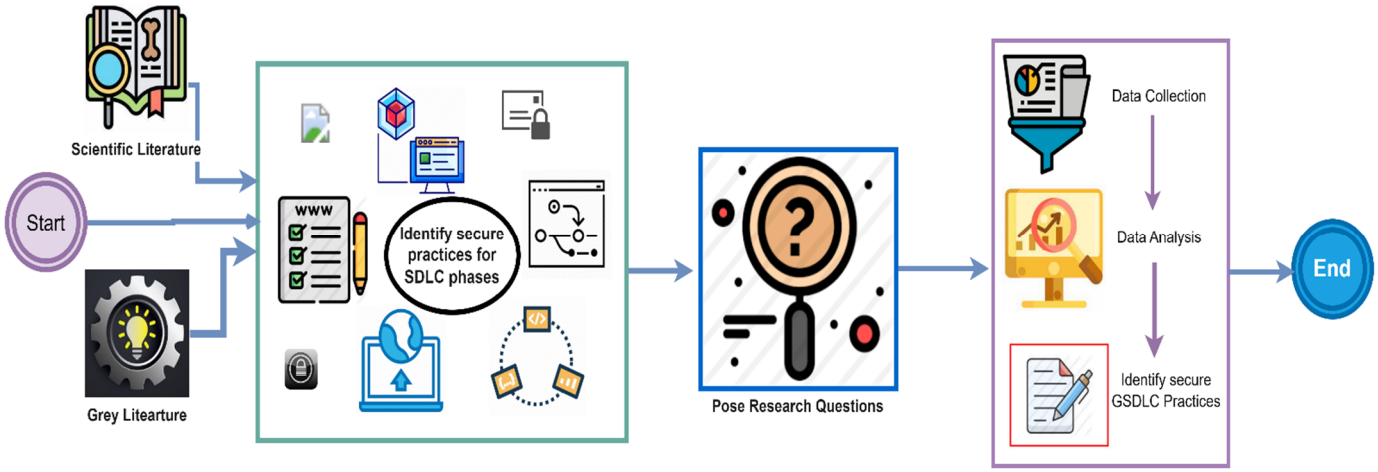

Figure 2. Research methodology process.

3.1. Practice Identification

As stated earlier, the SSDLC practices used in this study were mainly adopted from our previous work done in the paper [22]. However, we also reviewed the grey literature to improve the practice list and add the practitioners' opinions. Thus, a total of 36 practices were used in this research, from which 30 practices were adopted from our previous study and six new practices were added from the grey literature, the complete list of practices is given in Appendix A Table A1. Additionally, we included the option "other" in the poll to allow respondents to add additional security practices utilized in their firms. The process of practice identification is further elaborated in Figure 2. According to Figure 2, both scientific and grey literature are screened to identify security practices. Once all the security practices are identified, each is evaluated against SDLC phases and added to the phase for which it is more suitable. In the end, the total number of practices belonging to each phase of SDLC is counted.

3.2. Data Collection

To collect data from a diverse population, we conducted an online survey to gather information from GSD software development practitioners about their experiences implementing various security practices in GSD projects. A survey is considered the most suitable data collection method when we have to collect self-reported information from many diverse participants [29,40]. Interviews, questionnaires, or a combination of the two are some of the data-gathering strategies used in survey research [41]. We employed the questionnaire approach to collect data from a vast and scattered audience regarding the applicability of generic or non-GSD security practices in GSD projects. The questionnaire was created using the 36 security practices identified in our previous study [22] and through a grey-literature review. The bulk of the survey's questions was closed-ended and intended to gather practitioners' perspectives on the significance of chosen GSD security practices. However, we provided the option "others" to the poll so that practitioners might identify any other security practice they believe to be significant for GSD projects except those mentioned in the questionnaire.

First, a pilot study including four GSD experts was done to verify the questionnaire's validity. In light of the finding gained through the pilot study, the questionnaire was fine-tuned. Finalized questions were separated into three sections: Section 1 focuses on a person's basic information, Section 2 focuses on demographic data, and Section 3 focuses on 36 SSDLC practices. On top of that, the survey's opening page included a summary of the study's goals and methods. Ethical considerations were also included in the questionnaire's introduction to convince participants that their data would be kept private. Participants were assured that their data would only be available to the study team by this

statement. It was made clear that the study team would not release the data in a way that may reveal the name of any participant or organization.

We aimed to reach a vast and diverse group of people worldwide. We came up with a novel way of obtaining GSD specialists' comments. Requesting participation in our survey was accomplished via two primary methods. To begin, we emailed the GSD experts directly using our email accounts. The second step was to join LinkedIn groups linked to GSD and seek GSD specialists relevant to our study by looking through their accessible profiles in the LinkedIn groups and collecting their email addresses. We sent the survey link to the participants who had been identified and asked them to fill it out following their company's development policies. A total of 69 replies were submitted, with 15 being deemed incomplete and hence removed from consideration. The recommended GSD practices in GSD settings were evaluated based on 54 responses in this research.

All 36 SSDLC practices were ranked against four evaluations adopted from previous research [39,42]. The detail of the assessment is given below.

Highly important (HI): As part of the organization's GSD process, this practice has a stated standard and must be followed.
Medium important (MI): This indicates that the practice is commonly used in the organization's GSD process, although it is not a mandated part of that process.
Less Important (LI): In certain GSD projects, the practice has been implemented and is considered to be of low importance.
Not important (Z): In GSD initiatives, the practice of zero importance (Z) is never or seldom implemented.

Each SSDLC practice on this evaluation list is given a numerical value ranging from "high" (the highest value) to "zero," indicating the relative significance experts attach to the activity based upon past GSD initiatives. For this study, we drew on the expertise of 54 GSD specialists. A wide range of GSD/outsourcing experience was represented by the experts, whose tenure ranged from a few months to more than a decade, on average. Sixty-six percent of those in attendance worked for large, global corporations. Business and safety-critical applications are two of the main focus areas for most participating firms. Of the 54 professionals surveyed, 43% work for big corporations (those with more than 200 employees), 50% work for medium-sized corporations (those with 100 to 200 employees), and 7% work for small corporations (staff size between 20 and 100).

3.3. Data Analysis

The degree of relevance (high, medium, low, zero) in each answer was tallied to examine the importance of each specified Security practice. We used the statistical Chi-Square test to compare the relevance of often occurring security practices with the size of the respondents' companies and practitioners' experience. This method assisted us in determining the association between security policies and firm size, security policies, and the practitioner's experience. The chi-square test examines whether a discrepancy between actual data and predicted data is the result of chance or a connection between the variables being studied. Therefore, a chi-square test is a great choice for helping us comprehend and interpret the relationship between our two category variables. The details of the respondents' demographic are given in Figure 3.

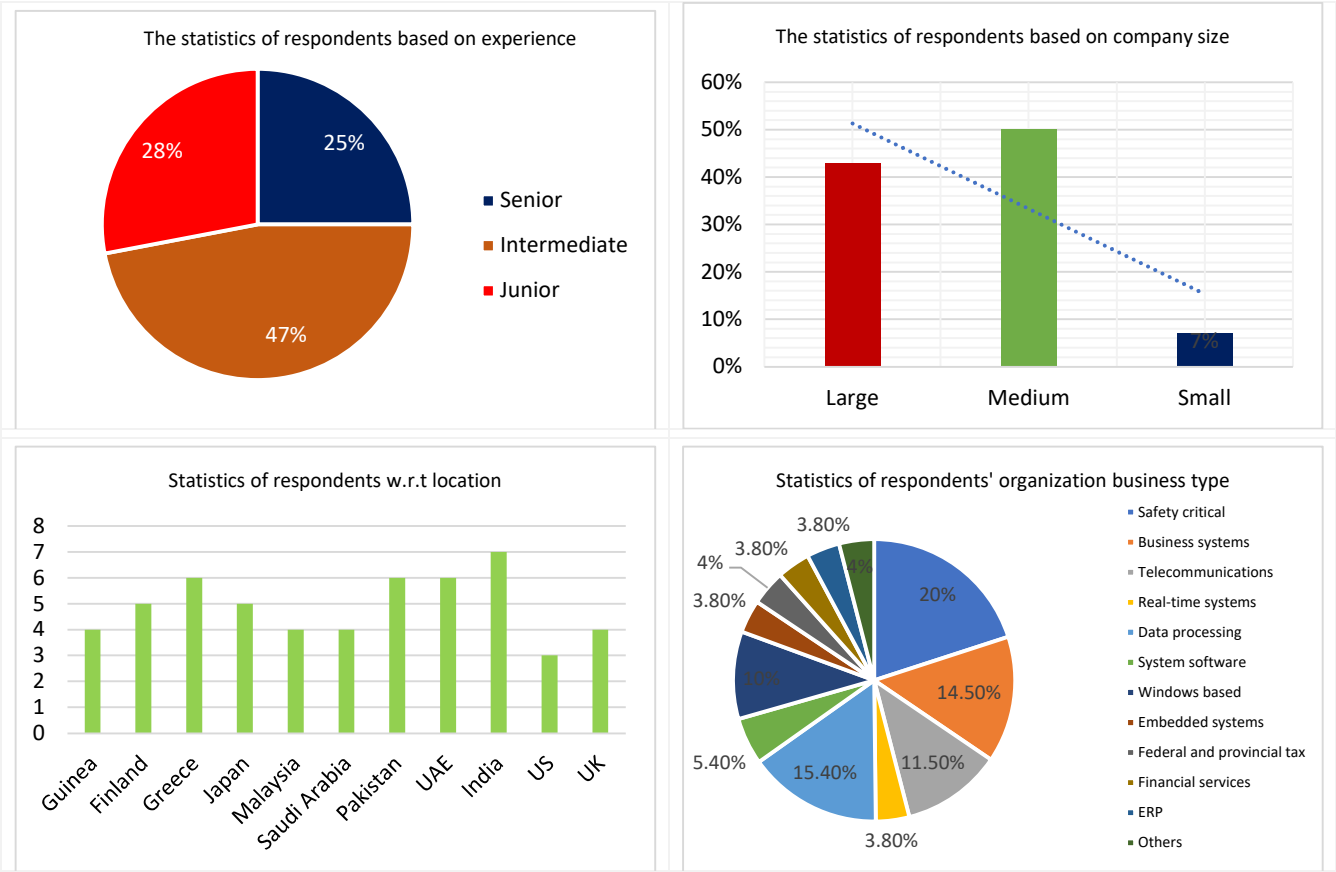

Figure 3. Details of respondents.

4. Results and Analysis

This section aims to answer the posed research questions by doing a detailed statistical analysis of the collected data through a questionnaire. Below we describe each research question in detail.

RQ1: What are the most critical security practices for GSD projects?

Fifty-four GSD security professionals participated in this poll and shared their thoughts on the 36 security practices for GSD projects. Based on their experience, we grouped these specialists into three categories namely; senior, intermediate, and junior. Junior experts were those with fewer than five years of experience. Experts with 5 to 10 years of experience were labeled intermediate, while experts with more than ten years of experience were designated as senior. Twenty-five percent (25 percent) of the specialists were junior practitioners. Forty-seven percent (47%) of the experts were intermediate practitioners. Twenty-eight percent (28%) of the experts were senior practitioners. This suggests a varied pool of GSD specialists with a decent dispersion and representation. The replies of the 54 GSD security experts were analyzed, and security practices with a frequency of more than 40% (22 and above) were chosen as crucial GSD security practices. By 40% we mean that the practices deemed very significant by more than 40% of the polled experts were considered important. Other researchers have used similar scales to benchmark their results [29,39]. Table 3 summarizes the most significant GSD security practices, according to practitioners.

Our research reveals that RE8 (perform requirement prioritization and categorization) is the most critically significant RE activity. The stakeholders' temporal; geographical; and sociocultural distance makes it challenging to implement this RE technique in GSD projects. In GSD, it is pretty uncommon for the development team to have trouble getting in touch with the system's stakeholders. Careful preparation is required to provide

effective communication between system stakeholders and the development team; allowing all parties involved in the system's creation to actively contribute to the prioritizing and categorization of requirements. Video conferencing, periodic on-site visits by important project participants located in different locations, etc., are just a few examples of the many methods that may be used in combination to facilitate this interaction. The second critical requirement identified by the GSD practitioners is identifying requirement dependencies (RE3). Because of GSD's iterative and incremental nature, determining which features to add in each iteration and which criteria to prioritize is essential to maximizing stakeholder satisfaction and ROI.

Table 3. Significant GSD security practices.

PID	Practice Name	Freq	SDLC Phase
RE8	Perform Requirement prioritization & classification	39	RE
RE3	Identify requirement dependencies	34	RE
RE7	Elicit security requirements	27	RE
RE6	Identify possible risks	24	RE
RE4	Identify threat	23	RE
D7	Apply the multilevel security concepts of defense in depth.	23	Design
D1	Utilize the economy of mechanism idea to make your design simple	22	Design
D8	Perform a secure design review to validate the design	22	Design
C5	Always validate input before accepting it	23	Coding
C1	Use a secure coding checklist and best practices to do secure coding.	22	Coding
C6	Use sanitization techniques in coding	22	Coding
T3	Perform functional testing	32	Testing
T2	The results of the requirement phase should be used to develop test cases.	27	Testing
T5	Perform integration testing	22	Testing
DP2	Follow the change management process	33	Deployment
DP1	Document change management process	26	Deployment

It was determined that the most vital practice during the design process was implementing the in-depth defense concept (D7), which entails many layers of protection. Due to the geographically dispersed nature of GSD projects' teams, a multilevel security approach is essential for protecting the confidentiality, integrity, and availability of critical data throughout transmission. When it comes to coding, the practitioners ranked input validation (C5) as the most vital practice. As the development team is dispersed over many geographic regions and security is an issue, each input received from any source must be vetted before proceeding. Functional testing (T3) was considered the highly critical practice of the testing phase. This testing seeks to establish whether each application feature conforms to the program requirements. The result of each function is compared to its corresponding requirement to see whether it fulfills the end user's expectations [43]. In GSD projects, distinct modules or the whole project are produced by distributed teams; hence, functional testing is essential to guarantee that all modules integrate correctly and perform properly. Following the change management process (DP2) was judged by GSD practitioners to be the most crucial deployment practice. The company must establish the change management strategy with the approval of all stakeholders. This strategy must be executed to ensure customer happiness. Figure 4 depicts the frequency of GSD security practices deemed to be of the utmost importance by practitioners who participated in the assessment.

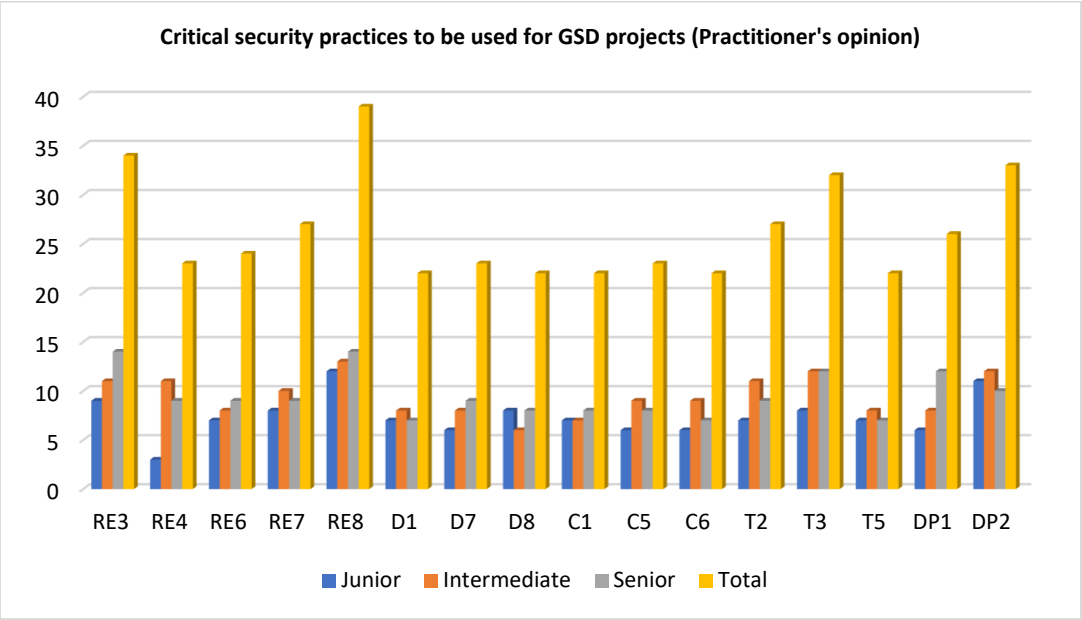

Figure 4. Important GSD security practices with high frequency.

RQ2: Is there a correlation between the size of the GSD organization and identified security practices?

The GSD specialists who participated in this research come from a diverse range of businesses of various sizes. Some come from very tiny organizations with only a handful of workers, while others come from huge companies with hundreds of individuals in their workforce. To classify the businesses according to their size, we used the organizational size concepts presented in papers [29,39]. We classified businesses according to their workforce size as follows: small (20 to 99 workers), medium (100 to 199 employees), and large (200 or more employees). The responses from GSD industry professionals working for firms of these three sizes were recorded. There are 54 participants, 4 of whom are specialists from small businesses, 27 from medium-sized businesses, and 23 from large businesses. Throughout their careers, some practitioners moved from one company to another several times; nonetheless, we considered their comments based on the size of the companies now represented by the respondents.

Figure 5 shows the frequency of employees from varying company sizes who consider the selected GSD security practices highly important. According to the findings presented in Figure 5, there is a disparity between the significance of a particular practice when the size of the company varies. For instance, only one-fourth (25%) of the respondents from small companies thought that RE3 was extremely important, while 19/27 (56%) of the respondents from medium companies and 14/23 (61%) of the respondents from large companies thought that it was extremely important. In the same way, variation exists in the opinions of experts from different categories (small, medium, large) for the remaining secured GSD practices. We utilized a Chi-square test of independence to investigate whether or not there was a correlation between the size of GSD companies and highly important GSD security practices. To do so, we formulated the following null and alternate hypotheses.

H_0= There is a correlation between company size and identified security practices.

H_1= There is no correlation between company size and identified security practices.

The formula used to calculate Chi-sqr is shown in Equation (1).

$$\chi^2 = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{(O_{i,j} - e_{i,j})^2}{e_{i,j}} \quad (1)$$

where

$$e_{i,j} = \frac{\sum_{k-1}^{c} O_{i.j} * \sum_{k-1}^{r} O_{k,j}}{N} \quad (2)$$

where $e_{i,j}$ shows expected values while $\sum_{k-1}^{c} O_{i.j}$ and $\sum_{k-1}^{r} O_{k,j}$ represent the sum of the ith column and the sum of the kth row, respectively, and N represents the total number. The observed and expected values are shown in Table 4.

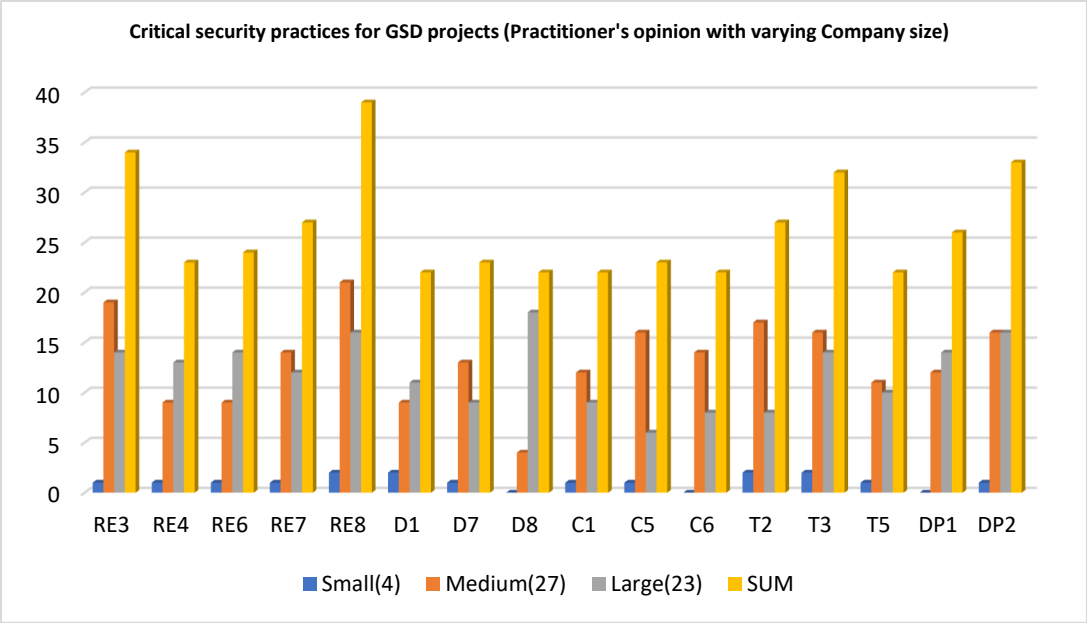

Figure 5. Critical security practices for GSD projects (opinion of practitioners with varying company size).

Table 4. Observed and expected values of selected GSD security practices by practitioners from varying size GSD companies.

GSD Security Practices	Observed Values			Expected Values		
	Small(4)	Medium(27)	Large(23)	Small(4)	Medium(27)	Large(23)
RE3	1	19	14	1.372922	17.12114	15.50594
RE4	1	9	13	0.928741	11.58195	10.48931
RE6	1	9	14	0.969121	12.08551	10.94537
RE7	1	14	12	1.090261	13.5962	12.31354
RE8	2	21	16	1.574822	19.63895	17.78622
D1	2	9	11	0.888361	11.07838	10.03325
D7	1	13	9	0.928741	11.58195	10.48931
D8	0	4	18	0.888361	11.07838	10.03325
C1	1	12	9	0.888361	11.07838	10.03325
C5	1	16	6	0.928741	11.58195	10.48931
C6	0	14	8	0.888361	11.07838	10.03325
T2	2	17	8	1.090261	13.5962	12.31354

T3	2	16	14	1.292162	16.11401	14.59382
T5	1	11	10	0.888361	11.07838	10.03325
DP1	0	12	14	1.049881	13.09264	11.85748
DP2	1	16	16	1.332542	16.61758	15.04988

When doing the Chi-square test, at least 80% of the cells must have an expected value of 5 or above. This assumption is not fulfilled in our case; therefore, we merged the first two columns of observed and expected values as mentioned in the papers [44,45]. The merged observed and expected values are given in Table 5. The requirement that at least 80% of the cells have an anticipated value of 5 or above has now been met. Hence, we calculate the Chi-Sqr value based on the data from Table 5.

Table 5. Observed and expected values of selected GSD security practices by combining. Column 1 and column 2 of expected and observed values.

GSD Security	**Observed Values**		**Expected Values**	
Practices	**S+M (31)**	**Large (23)**	**S + M (31)**	**Large (23)**
RE3	20	14	18.49406176	15.50594
RE4	10	13	12.51068884	10.48931
RE6	10	14	13.05463183	10.94537
RE7	15	12	14.68646081	12.31354
RE8	23	16	21.21377672	17.78622
D1	11	11	11.96674584	10.03325
D7	14	9	12.51068884	10.48931
D8	4	18	11.96674584	10.03325
C1	13	9	11.96674584	10.03325
C5	17	6	12.51068884	10.48931
C6	14	8	11.96674584	10.03325
T2	19	8	14.68646081	12.31354
T3	18	14	17.40617577	14.59382
T5	12	10	11.96674584	10.03325
DP1	12	14	14.14251781	11.85748
DP2	17	16	17.95011876	15.04988

Using the formula of equation 1, $\chi^2 = 0.07211$ where $d.f = (r-1)*(c-1) = (16-1)*(2-1) = 15$ and $\alpha = 0.05$.

The calculated value for a chi-square is 0.07211 at 15 degrees of freedom. At the same time, the value of the chi-square corresponding to 15 d.f is 24.996 in the Chi-square table, which is much greater than the calculated value. Therefore, evidence supports the claim that there is a link between company size and identified security practices.

RQ3: Is there a correlation between the practitioners' experience and identified security practices?

We also used the Chi-Square test to find the link between practitioners' experience and identified security practices. Following null and alternate hypotheses were formulated to test this claim.

H_0 = There is a correlation between practitioners' experience and identified security practices.

H_1 = There is no correlation between practitioners' experience and identified security practices.

The benefits of using the Chi-test in this situation are many including the fact that it is not sensitive to the shape of the distribution of the data, that it can be used in studies where parametric assumptions cannot be met, that it is easy to compute, that it provides useful and specific information, and that it can be easily adapted to data from studies

involving two or more groups. The formula for calculating the Chi-square test is given in Equation (1). The observed and expected values used for the calculation of Chi-sqr are given in Table 6.

Table 6. Observed and expected values of selected GSD security practices by GSD practitioners with varying experience.

Observed Values				**Expected Values**		
	Junior	**Intermediate**	**Senior**	**Junior**	**Intermediate**	**Senior**
RE3	9	11	14	9.529691	12.19477	12.27553
RE4	3	11	9	6.446556	8.249406	8.304038
RE6	7	8	9	6.726841	8.608076	8.665083
RE7	8	10	9	7.567696	9.684086	9.748219
RE8	12	13	14	10.93112	13.98812	14.08076
D1	7	8	7	6.166271	7.890736	7.942993
D7	6	8	9	6.446556	8.249406	8.304038
D8	8	6	8	6.166271	7.890736	7.942993
C1	7	7	8	6.166271	7.890736	7.942993
C5	6	9	8	6.446556	8.249406	8.304038
C6	6	9	7	6.166271	7.890736	7.942993
T2	7	11	9	7.567696	9.684086	9.748219
T3	8	12	12	8.969121	11.47743	11.55344
T5	7	8	7	6.166271	7.890736	7.942993
DP1	6	8	12	7.287411	9.325416	9.387173
DP2	11	12	10	9.249406	11.8361	11.91449

$\chi^2 = 0.9999$ where $d.f = (r-1) * (c-1) = (16-1) * (3-1) = 30$ and $\alpha = 0.05$.

The calculated value for a chi-square is 0.999982858 at 30 degrees of freedom. While the value of the chi-square corresponding to 30 d.f is 44.77 in the Chi-square table, which is much greater than the calculated value. Consequently, the assertion is supported by evidence that there is a link between practitioners' experience and identified security practices

5. Discussion/Summary of Findings

Fifty-four GSD specialists participated in this research and offered input based on their expertise about the relevance or significance of identified security practices for GSD initiatives. The highlighted critically significant security practices (from practitioners' viewpoints) may be used by GSD organizations and practitioners to modify and improve the situation-specific security procedures for their GSD initiatives. If at least 40% of the GSD experts rated a security practice as very significant, we regarded it as a crucial security practice. Other studies [39,42] have also utilized this criterion. To that end, we recommend that GSD organizations, if they are not already doing so, include these crucial security procedures in their GSDLC. The results of the study are discussed below, along with their relevance to the three research questions (RQ1-RQ3).

RQ1: What are the most critical security practices for GSD projects?

Using the previously indicated criteria (of at least 40% of the GSD specialists), we identified sixteen of the thirty-six key security practices for GSD projects to answer RQ1. These critical security practices are shown in Table 3. Five GSD security practices (identify requirement dependencies, identify threats, identify possible risks, elicit security requirements, and perform requirement prioritization and classification) relate to the RE phase of GSDLC. Our results show that requirement dependencies identification, risk and threat

identification, security requirement elicitation, and requirement prioritization are critical RE practices that must be followed to ensure the security of GSDLC. Meanwhile, the other three practices (economy of mechanism, defense in depth, and secure design review) are related to the security of the design phase of GSDLC. The development team should keep their design as simple as possible to better identify security risks/threats.

Further, a multilevel security mechanism should be adopted to ensure in-depth defense, and a design review should be done before moving toward implementation to ensure the security of the design phase. Regarding the implementation phase security of GSD projects, the development team should follow sanitization techniques, secure coding checklist and practices, and every input must be validated before acceptance. Testing of GSD projects, one of the crucial phases for managing security, should be done very carefully. The results of the requirement phase should be used to develop test cases. Further, functional and integration testing must be performed to ensure security. Lastly, the organization should have a mechanism for documenting and following the change management process in the deployment phase of GSDLC.

RQ2: Is there a link between the size of the GSD organization and identified security practices?

Our research shows that the significance of a given security measure changes significantly with organization size. For example, just 25% of respondents from small organizations rated RE3 as highly essential, whereas 56% of respondents from medium-sized businesses and 61% of respondents from big businesses gave it top marks. The same variation exists among the respondents from varying size companies about the importance of remaining security practices. To determine whether there exists a consensus among the respondents from varying company sizes regarding the importance of selected secure GSD practices, we used the Chi-Square test. The results demonstrate a correlation between business size and the prevalence of certain security measures.

RQ3: Is there a link between the practitioners' experience and identified security practices?

The respondents involved in this study belong to three categories: junior, intermediate, and senior, based on their experiences. A total of 14 out of 54 respondents were categorized as junior based on their year of work experience, while 25 out of 54 and 15 out of 54 were classified as intermediate and senior respectively. If we examine the data in Figure 4, there exists a discrepancy of opinion between practitioners with varying experience. To confirm this variation, we used the chi-square test and our results show a link between practitioners' expertise and identified GSD security practices.

5.1. Proposed Framework

This research work not only contributes by answering the above-mentioned questions, rather we have proposed an initial framework, as shown in Figure 6, to extract critical security practices for GSD projects. The initial proposed framework will help GSD researchers and practitioners to identify and use suitable security practices for their GSD projects based on the project's nature and complexity. We will conduct several case studies in the future to evaluate and further improve this proposed framework. Figure 6 depicts the suggested structure for detecting GSD security practices, which consists of four steps. In step one, the scientific and gray literature must be examined for identifying GSD security practices. In phase 2, these practices must be categorized according to the SDLC phase to which they belong. In the third step, selected practices are evaluated depending on the business characteristics. Phase 4 concludes with the extraction and storage of these practices in an organizational repository for future use.

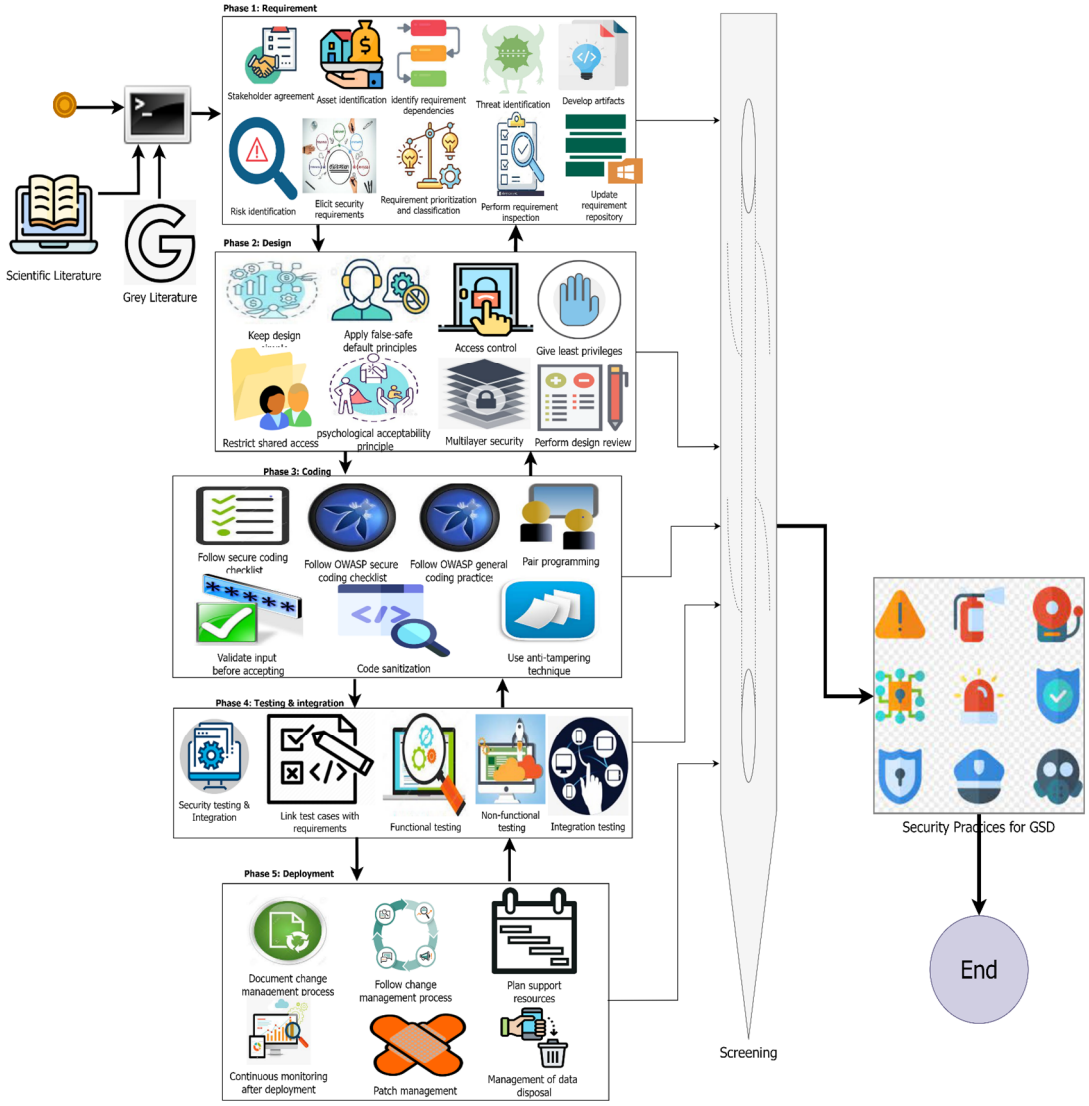

Figure 6. Proposed framework for identification of security practices for GSDLC.

5.2. Limitations of the Study

This research gathered data from 54 GSD specialists using a questionnaire. A common limitation of questionnaires is that they are closed-ended, requiring respondents to choose only one answer from a list. This sort of closed-ended questioning may affect the results of the survey. To address this issue, we included open-ended questions in the survey, asking GSD experts to enumerate any other GSD practices that they believe are critical for GSD projects but were not previously included in the survey. In addition, the study does not link the various outsourcing methods and project areas to specific security measures. Only the size of a corporation is provided as background information. This article reports on research that may be used by GSD businesses to adapt their context-specific security procedures and models rather than having to start from scratch.

Internal validity makes faith in the overall evaluation of the outcomes possible. Experts in GSD were consulted as well as 36 security practices were used to create the questionnaire. Pilot research confirmed the questionnaire's validity, and the findings were found to be satisfactory. The goal of establishing external validity is to ensure that research findings may be applied to settings that differ from those in which they were first collected. This research has certain limitations, one of which is the limited number of small business participants (4 out of 54). Our conclusions have external validity since the findings are based on the observations of 54 experts from 11 countries, covering the maximum

spectrum of the customer. Although 54 people with GSD participated in this research, it does not mean they represent the opinions of all professionals in these 11 countries. But we think they are a good representation of the whole.

6. Conclusions and Future Work

Due to its multiple potential advantages, GSD is quickly becoming a standard practice in the software industry. To maintain the security and success of GSD projects, it is vital to identify SSD practices that are critical to the performance of GSD initiatives. As a contribution to this goal, this article identifies and evaluates the value of significant security practices for GSD projects, based on the views of GSD practitioners gathered via an online poll. The results of the study reveal the following facts; first, more than 40 percent of respondents of the poll believed that 16 of the 36 listed security practices are crucial for GSD. Second, firm size influences the value of chosen security practices, since practitioners from companies of diverse sizes do not agree on the significance of selected security practices for GSD. Third, the practitioner's experience does influence the significance of chosen security practices, since the findings do not indicate an agreement among practitioners with varied experiences on the significance of selected security practices for GSD. This research has contributed in the following ways: first, essential SDLC security practices were identified. Next, security practices for GSDLC were narrowed down based on the opinions of practitioners. Third, the influence of firm size and practitioner opinion on selected practices was assessed. Finally, a preliminary framework was presented for the identified GSDLC-critical security activities. According to the study's findings, the following security practices are crucial for GSD security: Requirement prioritization and classification, identification of requirement dependencies, elicitation of security requirements, identification of possible risks and threats, defense in depth, the economy of mechanism, Secure design, input validation, use of a secure coding checklist and secure coding practices, code sanitization techniques, functional testing, and utilization of reusable software components.

In the future, we plan to implement the proposed framework in a real-life software project to further strengthen its validity.

Author Contributions: Conceptualization, M.H. (Mamoona Humayun); formal analysis, M.H. (Mamoona Humayun), M.A. and M.H. (Mariem Haoues); funding acquisition, M.A. and M.H. (Mariem Haoues); methodology, M.H. (Mamoona Humayun) and M.N.; supervision, M.N.; writing—original draft, M.H. (Mamoona Humayun); writing—review and editing, M.N., M.A., and M.H. (Mariem Haoues). All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444)

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. List of identified security practices for GSD.

P-ID	Practice Name	SDLC phase
RE1	Agreement on requirement definitions is required among all parties.	RE
RE2	Identify the assets which are critical and vulnerable	RE
RE3	Identification of requirement dependencies	RE
RE4	Threats identification	RE
RE5	Development of corresponding artifacts	RE

RE6	Identification possible risks	RE
RE7	Elicitation of security requirements	RE
RE8	Requirement prioritization and classification	RE
RE9	Requirement inspection	RE
RE10	Updating requirement repository regularly	RE
D1	Utilize the economy of mechanism idea to make your design as simple as possible.	Design
D2	To ensure that failure of any action will prohibit dangerous operation, use false-safe default principles.	Design
D3	To ensure that every object is authorized, use access control mechanisms.	Design
D4	Reduce privileges to protect the system from security threats.	Design
D5	Use the least common method to limit access to shared resources.	Design
D6	Follow the principle of psychological acceptability to automatically include basic security	Design
D7	Utilize the defense-in-depth concept, which includes multilevel of security	Design
D8	Perform Secure design review to validate design	Design
C1	Use the secure coding checklist and best practices to do secure coding.	Coding
C2	abide by the OWASP secure coding guidelines and checklists	Coding
C3	observe the OWASP coding standards	Coding
C4	If you can, try pair programming.	Coding
C5	Never accept input without first validating it.	Coding
C6	Utilize sanitization methods while coding.	Coding
C7	Utilize anti-tampering strategies like obfuscation to protect code.	Coding
T1	Perform secure testing and integration	Testing
T2	Generate test cases using the output of requirement phase	Testing
T3	Perform functional testing	Testing
T4	Perform nonfunctional testing	Testing
T5	Perform integration testing	Testing
DP1	Document change management process	Deployment
DP2	Follow change management process	Deployment
DP3	Plan support resources	Deployment
DP4	Continually check the deployed system for any unknown vulnerabilities	Deployment
DP5	Organize patch management	Deployment
DP6	Management of disposal of data	Deployment

P-ID = practice ID, RE = requirement, D1 = design practice one, C1 = coding practice one, T1 = testing practice one and DP1 = deployment practice one.

References

1. Manjavacas, A.; Vizcaíno, A.; Ruiz, F.; Piattini, M. Global software development governance: Challenges and solutions. *J. Softw. Evol. Process* **2020**, *32*, e2266.
2. Nicolás, J.; De Gea, J.M.C.; Nicolas, B.; Fernandez-Aleman, J.L.; Toval, A. On the risks and safeguards for requirements engineering in global software development: Systematic literature review and quantitative assessment. *IEEE Access* **2018**, *6*, 59628–59656.
3. Humayun, M.; Jhanjhi, N. Exploring the relationship between GSD, knowledge management, trust and collaboration. *J. Eng. Sci. Technol.* **2019**, *14*, 820–843.
4. Yaseen, M.; Ali, Z. Success factors during requirements implementation in global software development: A systematic literature review. *Int. J. Comput. Sci. Softw. Eng.* **2019**, *8*, 56–68.
5. Gupta, R.K.; Venkatachalapathy, M.; Jeberla, F.K. Challenges in adopting continuous delivery and DevOps in a globally distributed product team: A case study of a healthcare organization. In Proceedings of the 2019 ACM/IEEE 14th International Conference on Global Software Engineering (ICGSE), Montreal, QC, Canada, 25–26 May 2019; pp. 30–34.

6. Sievi-Korte, O.; Beecham, S.; Richardson, I. Challenges and recommended practices for software architecting in global software development. *Inf. Softw. Technol.* **2019**, *106*, 234–253.
7. Vizcaíno, A.; García, F.; Guzmán, I.G.R.D.; Moraga, M.Á. Evaluating GSD-aware: A serious game for discovering global software development challenges. *ACM Trans. Comput. Educ.* **2019**, *19*, 1–23.
8. Akbar, M.A.; Sang, J.; Khan, A.A.; Hussain, S. Investigation of the requirements change management challenges in the domain of global software development. *J. Softw. Evol. Process* **2019**, *31*, e2207.
9. Akbar, M.A.; Sang, J.; Nasrullah; Khan, A.A.; Mahmood, S.; Qadri, S.F.; Hu, H.; Xiang, H. Success factors influencing requirements change management process in global software development. *J. Comput. Lang.* **2019**, *51*, 112–130.
10. Almufareh; Fahaad, M.; Humayun, M. Improving the Safety and Security of Software Systems by Mediating SAP Verification. *Appl. Sci.* **2023**, *13*, 647.
11. Saleem, N.; Mathrani, S.; Taskin, N. Understanding the different levels of challenges in global software development. In Proceedings of the 2019 ACM/IEEE 14th International Conference on Global Software Engineering (ICGSE), Montreal, QC, Canada, 25–26 May 2019; pp. 76–77.
12. Vallon, R.; da Silva Estácio, B.J.; Prikladnicki, R.; Grechenig, T. Systematic literature review on agile practices in global software development. *Inf. Softw. Technol.* **2018**, *96*, 161–180.
13. Khan, R.A.; Khan, S.U. A preliminary structure of software security assurance model. In Proceedings of the 13th International Conference on Global Software Engineering, New York, NY, USA, 27–29 May 2018; pp. 137–140.
14. Shan, Z.; Ren, K.; Blanton, M.; Wang, C. Practical secure computation outsourcing: A survey. *ACM Comput. Surv.* **2018**, *51*, 1–40.
15. Zhang, Y.; Deng, R.H.; Liu, X.; Zheng, D. Outsourcing service fair payment based on blockchain and its applications in cloud computing. *IEEE Trans. Serv. Comput.* **2018**, *14*, 1152–1166.
16. Benil, T.; Jasper, J. Cloud based security on outsourcing using blockchain in E-health systems. *Comput. Netw.* **2020**, *178*, 107344.
17. Doomun, M.R. Multi-level information system security in outsourcing domain. *Bus. Process Manag. J.* **2008**, *14*, 849–857.
18. Wong, W.K.; Cheung, D.W.; Hung, E.; Kao, B.; Mamoulis, N. Security in outsourcing of association rule mining. In Proceedings of the 33rd International Conference on Very Large Data Bases, Vienna, Austria, 23–27 September 2007; pp. 111–122.
19. Wu, Y.; Tayi, G.K.; Feng, G.; Fung, R.Y. Managing Information Security Outsourcing in a Dynamic Cooperation Environment. *J. Assoc. Inf. Syst.* **2021**, *22*, 2.
20. Feng, N.; Chen, Y.; Feng, H.; Li, D.; Li, M. To outsource or not: The impact of information leakage risk on information security strategy. *Inf. Manag.* **2020**, *57*, 103215.
21. Benaroch, M. Cybersecurity risk in IT outsourcing—Challenges and emerging realities. In *Information Systems Outsourcing*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 313–334.
22. Humayun, M.; Jhanjhi, N.Z.; Almufareh, M.F.; Khalil, M.I. Security Threat and Vulnerability Assessment and Measurement in Secure Software Development. *CMC-Comput. Mater. Contin.* **2022**, *71*, 5039–5059.
23. Beecham, S.; Clear, T.; Lal, R.; Noll, J. Do scaling agile frameworks address global software development risks? An empirical study. *J. Syst. Softw.* **2021**, *171*, 110823.
24. Jain, R.; Suman, U. A Systematic Literature Review on Global Software Development Life Cycle. *ACM SIGSOFT Softw. Eng. Notes* **2015**, *40*, 1–14.
25. Farhan, A.S.; Mostafa, G.M. A methodology for enhancing software security during development processes. In Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 25–26 April 2018; pp. 1–6.
26. Dodson, D.; Souppaya, M.; Scarfone, K. Mitigating the risk of software vulnerabilities by adopting a secure software development framework (ssdf). *Natl. Inst. Stand. Technol.* **2020**, 4232020. https://doi.org/10.6028/NIST.CSWP.04232020.
27. Fujdiak, R.; Mlynek, P.; Mrnustik, P.; Barabas, M.; Blazek, P.; Borcik, F. Managing the secure software development. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; pp. 1–4.
28. de Vicente Mohino, J.; Higuera, J.B.; Higuera, J.R.B.; Montalvo, J.A.S. The application of a new secure software development life cycle (S-SDLC) with agile methodologies. *Electronics* **2019**, *8*, 1218.
29. Khan, S.; Niazi, M.; Ahmad, R. Empirical investigation of success factors for offshore software development outsourcing vendors. *IET Softw.* **2012**, *6*, 1–15.
30. Niazi, M.; Wilson, D.; Zowghi, D. Critical success factors for software process improvement implementation: An empirical study. *Softw. Process Improv. Pract.* **2006**, *11*, 193–211.
31. Akbar, M.A.; Al-Sanad, A.; AlSanad, A.A.; Ghmaei, A.; Shafiq, M.; Kamal, T. Towards efficient and secure global software development using blockchain. In Proceedings of the Evaluation and Assessment in Software Engineering, New York, NY, USA, 15–17 April 2020; pp. 493–498.
32. Zafar, A.A.; Saif, S.; Khan, M.; Iqbal, J.; Akhunzada, A.; Wadood, A.; Al-Mogren, A.; Alamri, A. Taxonomy of Factors Causing Integration Failure during Global Software Development. *IEEE Access* **2017**, *6*, 22228–22239.
33. Patil, S.; Ade, R. Secured Cloud Support for Global Software Requirement Risk Management. *Int. J. Softw. Eng. Appl.* **2014**, *5*, 23–29.
34. Taafti, M.H. Risks factors associated with offshore IT outsourcing. *Ind. Manag. Data Syst.* **2005**, *105*, 549–560.
35. June, W.; Jason, O.; Meiga, L.-N. Information Technology Offshore Outsourcing Security Risks and Safeguards. *J. Inf. Priv. Secur.* **2010**, *6*, 29–46.

36. Khan, R.A.; Khan, S.U.; Akbar, M.A.; Alzahrani, M. Security risks of global software development life cycle: Industry practitioner's perspective. *J. Softw. Evol. Process* 2022, *early review*.
37. Khan, R.A.; Khan, S.U.; Alzahrani, M.; Ilyas, M. Security assurance model of software development for global software development vendors. *IEEE Access, volume 10,* pp. 58458 - 58487**, 2022**.
38. Usman, M.; Usman, A. Ensuring Data Security by AES for Global Software Development in Cloud Computing. In Proceedings of the 2014 International Conference on IT Convergence and Security (ICITCS), Beijing, China, 28–30 October 2014.
39. Khan, H.U.; Niazi, M.; El-Attar, M.; Ikram, N.; Khan, S.U.; Gill, A.Q. Empirical Investigation of Critical Requirements Engineering Practices for Global Software Development. IEEE Access 2021, 9, 93593–93613.
40. Kitchenham, B.; Pfleeger, S.L. Principles of survey research part 6: Data analysis. ACM SIGSOFT Softw. Eng. Notes 2003, 28, 24–27.
41. Lethbridge, T.C.; Sim, S.E.; Singer, J. Studying software engineers: Data collection techniques for software field studies. Empir. Softw. Eng. 2005, 10, 311–341.
42. Niazi, M.; El-Attar, M.; Usman, M.; Ikram, N. An empirical study identifying high perceived value requirements engineering practices in global software development projects. In Proceedings of the 7th International Conference on Software Engineering Advances (ICSEA), Lisbon, Portugal, 18–23 November 2012; pp. 283–288.
43. Jindal, T. Importance of Testing in SDLC. *Int. J. Eng. Appl. Comput. Sci.* **2016**, *1*, 54–56.
44. McHugh, M.L. The chi-square test of independence. *Biochem. Med.* **2013**, *23*, 143–149.
45. López-Chau, A.; Rodriguez-Mazahua, L.; García-Lamont, F.; Quintana-López, M.; Rojas-Hernández, C.A. Dichotomization of Multilevel Variables to Detect Hidden Associations. *Appl. Sci.* **2022**, *12*, 12929.