❒   1598

A systematic mapping study of security, trust and privacy in clouds

Isaac Odun-Ayo[1], Oladapo Alagbe[2], Jamaiah Yahaya[3]
[1,2]Department of Computer and Information Sciences, Covenant University, Ota, Nigeria
[3]Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi 43600, Malaysia

Article Info	ABSTRACT
	Cloud computing thrives around trust and security in the relationship between cloud providers and users of their services. The objective was the conduct of a systematic mapping study of cloud computing security, trust and privacy. The research was executed using three classes of facets, namely topic, contribution, and research based on the systematic mapping process. The result shows that privacy issues and challenges on metric had 4.76% of the publications. On cloud trust in the domain of tool, the publications were 8.75%. The publications on design within the domain of model stood at 12.38%, and publications on privacy issues and challenges in the area of process were 8.57%. Furthermore, there were more articles published on privacy issues and challenges within the domain of evaluation research with 10.43%. The publications on design based on validation research made up 7.83% of the study. More papers were also published on frameworks and techniques within the domain of solution research with 5.22% each. There were more articles published on privacy issues and challenges with regards to philosophical research with 4.35%. Shortcomings in the fields of security, trust and privacy in the cloud, were identified through this study, which should motivate further research.

Corresponding Author:

Isaac Odun-Ayo
Department of Computer and Information Sciences
Covenant University
Ota, Nigeria
Email: isaac.odun-ayo@covenantuniversity.edu.ng

1.   INTRODUCTION

"A parallel and distributed set of associated and virtualized computer systems which are provisioned progressively and introduced as multiple unified computing resources dependent on service level agreements between cloud service providers (CSPs) and clients is known as cloud computing" [1]. Cloud security is essential to safeguard the cloud infrastructure and protect the data and application from unauthorized access. Cloud security is unique because of the core technology of the cloud, which is virtualization. Also, multi-tenancy, which allows users to share resources at proximity, can lead to vulnerability. There are also issues of trust management, despite CSPs making sure to give productive and guaranteed services on the cloud [2].

The cloud user also expects that information kept with the CSPs will not be available to a third party. The issue of trust between a customer and consumer is good for the cloud market place. Three essential models of cloud offerings exist, which are, software as a serve (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The SaaS is the process whereby the cloud service provider offers software

and database services to the user on the internet through a web browser, thereby eliminating upgrade and license issues. The PaaS is the process of releasing the cloud infrastructure to the user to enable the development and deployment of applications. Also, the IaaS enables the CSP to use the internet to provide storage, network, and compute resources to the clients. The client has management of the operating system and storage. Also, cloud computing is vast, and a wide range of aspects exist, such as management optimization and identity management, which require extensive review. Such matters are associated with the focus of this study either implicitly or explicitly [3], [4].

Furthermore, the cloud has four models of deployment namely private, public, community, and hybrid clouds. Individual organizations own and host private clouds on their premises. Major CSPs own public clouds with large data centers in several geographical locations. For the community clouds, they are hosted and shared by institutions involved in similar activities. Hybrid clouds consist of more than one cloud deployment type.

There are lots of publications that cover cloud security, trust and privacy. A few of such papers are discussed subsequently. Though the concerns about security in traditional network systems are also applicable to the cloud, cloud computing usage brings about new vectors that make attacking them possible, and even easier to carry out [5]. There are security challenges related to resources allocation, multi-tenancy, system monitoring and logs, and solutions to these challenges include; virtualization, security risk assessment and developing outsourcing risk control [5]. One of the major issues that affect cloud business adoption include privacy and data security, which results from the nature of information sources and the process of data collection from multiple sources [6]. Solutions to privacy issues include the use of anonymity-based methods, and privacy preservation authorization system [6].

To ensure data security, CSPs must utilize additional time and take vigorous measures, for example, encryption of information during transmission and storage, restricting admittance to information, consistent survey of security dangers, and the execution and implementation of the results from audits of the system [7]. Furthermore, preventing vulnerabilities from hackers and protection of customer data using appropriate laws is essential [7]. Trust is the confidence in or reliance on another entity; it can be considered one of the most fundamental solutions to security issues on the cloud [8]. The cloud providers can achieve certainty among their clients by ensuring that their activities are certified as compliant to organizational requirements and safeguards [8]. A very important aspect of life that requires security and privacy is in the area of health care. A lot of health information have been compromised and leaked. Mobile applications in emergency health care help maintain patient confidentiality and manage patient records including data storage. Developing a mobile cloud computing application for emergency health care enhances the aspect of trust and privacy on the cloud. Health care data can futher be safeguarded from leakages that comprises confidentiality [9]. Due to the issues of multitenancy, utilization of virtual machines (VM) on the cloud has security implications. There are many vulnerabilities in the use of cloud hypervisor, and the VMs and adversaries exploit the vulnerabilities of cloud hypervisor, taking them over for malicious purposes [10].

Deployment of cloud capabilities provides enhanced, protected, and trusted facilities and services. However, because of an absence of standard services, secure service level agreements, and security in the cloud, organizations and establishments are hesitant to migrate their information or data to the cloud [11]. Also, health records are crucial in any hospital system, but they are coming under increased attacks. These records contain private and sensitive patient information, and a breach in their confidentiality, integrity or privacy can lead to dire consequences on both the patients, caregivers, and the medical facilities, such as defamation, discrimination, lawsuits, and other stressful conditions [12]. If data is not stored securely in the cloud, it can be compromised, leading to severe consequences. The use of models such as the modified RSA public key cryptosystem can help mitigate against existing security flaws of the current security models in the cloud environment and thereby guarantee the security of data in cloud environments [13]. These issues and more make security, trust and privacy in the cloud an exciting area worth researching on. When writing an article or even conducting research, the researcher has to consider a specialized domain of focus. Such considerations involve extensive studying to ensure further understanding of the selected topic. This extensive studying mostly deals with perusing through multiple conference proceedings, journals and books. The need to look through computerized libraries, go to workshops, conferences, classes, and seminars, to recognize a point of convergence of research could also exist. Additionally, researchers can gather interest in certain areas through the observation of certain phenomena within environments. From all of these, it is evident that the processes involved in determining a research topic can be quite burdensome.

Security, trust, and privacy have attracted some of the largest publications in cloud computing. It may interest researchers to want to have an overview of the kinds of publications and the areas covered; a map can be used to facilitate this. The systematic mapping process categorizes publication based on a structure and scheme built in the area of interest and the presentation of the results as a map. The systematic mapping process, although not as rigorous as a systematic literature review, is more coarse-grained. This

publication makes use of three facets, namely the topic, research, and contribution. The topic facet identifies vital topics in the area of cloud security and privacy; the research facet deals with the classification of research, and the contribution facet relates to issues like method. The need for more research in the areas of security, trust and privacy in cloud services, is the primary motivator for this work. Therefore, the challenge this study aims at addressing is the determination of the domains where a shortage of research exists, and highlighting them for upcoming researchers. This paper seeks to carry out a systematic mapping study of cloud computing security, privacy, and trust. The primary output of this review paper is the visual map that contains percentages showing the degree of research done in different research domains, for example, frameworks and models within this domain of study. Subsequent portions of this paper are arranged in the following manner. Section 2 looks at related work. Section 3 focuses on materials and methods. Section 4 presents the results and discussion, while section 5 is the conclusion with suggestions for further research.

2.   RELATED WORK

K. Petersen, S. Vakkalanka, and L. Kuzniarz [14] proposes the need to assess how researchers attempt systematic mapping and decide the manner that the rules should be reviewed as informed by key takeaways from systematic maps and guidelines which exist for writing systematic literature review. The authors led a systematic mapping study of systematic maps while considering a few guidelines that govern the acts of systematic review papers. They found that in most of the conducted studies, numerous rules were used and consolidated. This approach prompted various methods of leading systematic mapping studies. T. Kosar, S. Bohra, and M. Mernik [15] focuses on the description of the rules that govern a systematic mapping study as associated with domain-specific languages (DSL). Their study focused on an upgraded understanding of the DSL area of study, along side an emphasis on research trends and future leanings. Their study ranges from July 2013 through October 2014, and laid emphasis on three rules for conducting a systematic review, which are planning the review process, conducting it, and communicating its result.

I. Odun-Ayo *et al.,* [16] led a systematic mapping study of cloud policy languages and programming models. Their study used ideas from [11]. This mapping study gives six classes of study within the regions of accountability and reliability, framework, paradigms, privacy, security and survey. The consequences of the chosen studies were also implemented on the contribution facet, regarding tool, method, and model. Likewise, the chosen studies were applied to the research facet that addressed evaluation, validation, solution, experience and opinion research. C. R. Fernandez-Blanco *et al.,* [17] conducted a power systems model mapping. They achieved this by providing a power systems model overview, and determining how such models are used by European organizations, in light of a review of their features, while identifying modelling gaps. Two hundred twenty-eight (228) questionnaires were sent out for elicitation of information from power experts, while eighty-two (82) surveys were responded to and used for the final mapping.

C. Griffo, J. P. A. Almeida, and G. Guizzardi [18] dealt with a systematic mapping of the legal core ontologies literature. The research was focused on "legal theory and concepts". Additionally, the studies utilized in the research were grouped as a result of their contributions concerning language, tool, method, and model. They also performed recognition of the legal theories that were used in the building process of legal core ontologies. Focus was determined with a specific advice on the use of two ontologies, alongside an assessment of all selected research for cogent deductions about legal and ontological research. I. Odun-Ayo *et al.,* [19] is a systematic mapping review of cloud computing services with a focus on virtualization, containerization, composition, and orchestration. The classification scheme within this systematic mapping review was also examined, and six considerations in cloud computing services were identified. These considerations included virtualization, centralization, composition, orchestration, rationalization and deployment. The chosen studies were then used on the contribution facet with a focus on metrics, tool, method, and model. The chosen studies were additionally applied to the various categories of research such as experience, evaluation of opinion, solution research and validation.

M. Alavi and D. E. Leidner [20] presents an extensive assessment of knowledge management within an organization while focusing on the prospective part IT plays in knowledge management. Several vital matters that related to knowledge management processes, and the role Information Technology will play in driving and supporting these processes, were also discussed. Emphasis was also placed on the need to promote the formation, storage, transmission and utilization of knowledge in organizations. I. Odun-Ayo *et al.,* [21] presents a systematic mapping study with a focus on the design and models of deployment of the cloud. The paper presents a classification scheme that addresses design and models of deployment by discussing design, service deployment, implementation, configuration, privacy and security. These chosen topics were administered to the contribution facet according to metrics, tools, methods, and models. Also, they were used for various research types concerning evaluation, experience, opinion validation and solution research.

According to S. K. Boell and D. Cecez-Kecmanovic [22], in their paper addressed the usefulness of and constraints to Information System and Social Science Systematic Literature Review. The authors believe that the broad idea that a Systematic Literature Review provides a complete and exceptional method for literature review is both controversial and deplorable. In their critique and approval of this position, they resolved that care and restraint is employed in the process of systematic literature review selection, as an important undertaking with literature and the scholarly nature of academic work could be undercut. P. Brereton *et al.,* [23] discussed the discoveries made from the application of the process of systematic literature review to the domain of software engineering. This review process, and also the quantity of reviews performed by the paper's authors and others, were extracted and discussed. Finally, the assessment of a number of lessons on how applicable this practice is to software engineering, was conducted.

Cloud related mobile application testing systematic mapping study was conducted in [24]. Security, compatibility, functional and GUI testings were discussed relative to cloud-based testing. The studies selected were then implemented on the contribution facet with a focus on metrics, tool, method, and model. They were also implemented on various aspects such as experience, opinion evaluation, validation and solution research. Finally, using some contribution category consideration, Testing-as-a-Service was examined. The author of H. M. Cooper [25], in his paper, examined how research reviews have to provide consideration to the detailed philosophy that is expected from a primary researcher. Research review was additionally conceptualized as a scientific and logical enquiry which consists of five phases that equal those primary researches specifically, problem formulation, collection of data, data point's evaluation, data analysis and their interpretations, and finally, the results presentation. Sources of variance, potential threats to validity and every other function pertaining to each stage was discussed.

Useful insights for the execution of a literature review were provided to researchers in [26]. The authors suggested the synthesis of trends and patterns during the preparatory stages of literature review writing. Some of these steps include the consideration of purpose and voice before the commencement of writing, the consideration of the reassembly of notes, and also the creation of topical outlines which trace literature review arguments. These should provide the requirements and steps used for the development of a detailed and concise literature review. B. Kitchenham *et al.,* [27], an assessment of systematic literature review impact was conducted. These impacts were the suggested software engineering methods which are evidence-based, for the aggregation of evidence. The authors utilized manual searches of ten Journals and four conference proceedings to conduct their assessment. Cumulatively, twenty studies were found to be relevant, eight of which dealt with research trends, and not evaluation of technique. Furthermore, seven systematic literature reviews dealt with estimation of cost. Out of all the systematic literature reviews that were assessed, three scored lower than 2 out of a maximum of 4. This scoring points to an acceptable overall quality of reviews.

I. Odun-Ayo *et al.,* [28], a systematic mapping study of mobility and efficiency in cloud computing utilization, which was based on concepts from [11], was conducted. This study presented five topics of study in the areas of architecture, computation offload, efficient transmissions, allocations, collaborative mobile cloud, and fault tolerance and data storage regarding the aspects of the research selected. The chosen aspects were then implemented on the contribution facet with a focus on tool, method, and model. They were also implemented on the various categories of research such as experience, evaluation, opinion, validation and solutions research. J. Vom *et al.,* [29] harped upon the significance of literature review to scientific enquiry. It further emphasized the importance of thorough literature searches as significant issues that can ensure that useful literature reviews will be discovered. The authors also stated the challenges of searching through literature within the continuously growing and fluid context of information system. They also made recommendations regarding how the challenges could be addressed. They suggested practical guidelines and checklists that researchers could utilize in planning and organizing their literature searches.

The work in S. M. Rosli, M. M. Rosli, and R. Nordin [30] is a recommender system mapping study for blood glucose levels in gestational diabetes mellitus patients. The search for primary studies focused on a defined method, data collection, recommender system for blood glucose, blood glucose and variables prediction models. Analysis of the blood glucose recommender system was carried out based on the topics of machine learning, context awareness, hybrid filtering, AI, rough set theory and data mining.

The work in Y. Yan, H. Xiahong and W. Wanjun [31] is about location-based services (LBS) and protection of privacy in mobile cloud computing (MCC). Location-based services are presently being utilized on moving objects in the areas of transportation and safety. The paper emphasized the need to provide location-based services, especially within cloud environments. The suggested framework can promote confidentiality under privacy protection, especially in the cloud mobile computing environment. The work in K. S. Gururaj and K. Thippeswamy [32] is a cloud-based secured framework for utilization in an online voting system. The paper examined the present trend of accessing information from remote locations, which has attendant challenges on data access, especially on the cloud. This publication introduced a technology-

based infrastructure that can mitigate the challenges. The proposed secure cloud-based framework that can be used for online voting was implemented and also tested using some cryptographic algorithms.

3.   RESEARCH METHOD
3.1. Review stage
Systematic mapping studies provide visual outlays of the outcomes of rigorous reviews of papers within domains of enquiry. The specifications on systematic mapping studies from [14], [27] were used to accomplish this study. A systematic study is a reproducible process for the extraction and interpretation of publications that are present and are on a particular research objective [33]. Although systematic mapping processes are not as rigorous as systematic literature reviews, however, it offers a more coarse-grained overview [14]. Figure 1 depicts some critical steps found within general systematic mapping studies. The first step in this process is the definition of questions that dictate the research scope. Next comes the search for primary studies for all papers available within the domain of study. Following that is the screening of all the papers, thereby determining those that are relevant to the study. A method of classification is then developed through the use of essential wording processes on abstracts from relevant publications. Finally, the data extraction process culminates in the form of a systematic map. These steps are utilized in this paper for the development of a systematic map for cloud security, trust and privacy.
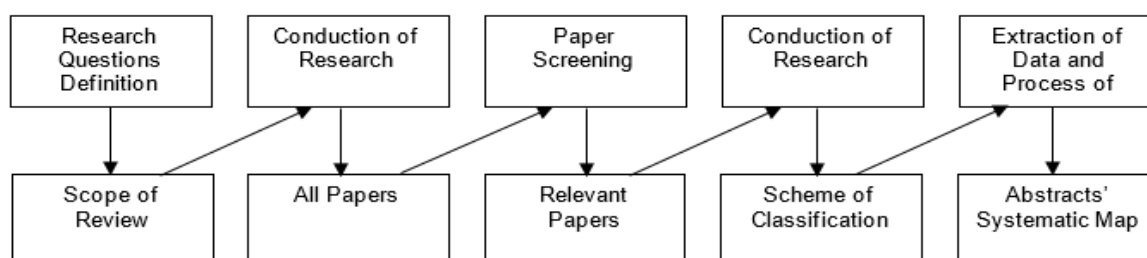

Figure 1. The systematic mapping process [14]

− Abstract
− Keywording
− Scheme of classification
    a. Articles
    b. Articles classification into the schemes
    c. Scheme update
− Systematic map

3.2. Research questions definition
Systematic maps are meant for the provision of overviews of the quality and category of work that has been done within a selected domain of enquiry. They may also be necessary when determining where such work was done; challenges identified determine the type of research questions that will be used for a study. The research questions utilized in this study include:
a. RQ 1: What aspects of security, trust and privacy in the cloud are identified, and how many publications deal with the various aspects?
b. RQ 2: What categories of publications are made in those domains, and what evaluations and innovations do they provide?
c. RQ3: What approaches to research do these studies utilize, and what improvements were provided?

3.3. Conduct of primary studies
Primary studies searches usually serves as the beginning of a review. This exploration for the primary study is done through the analysis of major digital libraries in the related field. This primary search then focuses on exploring literature that is relevant, from online repositories via search queries. Afterwards, a backward snowballing is utilized in enhancing the search process [34]. Occasionally manual searches can also be carried out on conference and journal materials. Publications utilized for this study were obtained through the exploration of major scientific digital repositories. However, primary studies from books and

other printed sources were not utilized in this search. The primary studies process for this work was done on five primary databases as a result of the high impact factors from the various conference and journal publications. Table 1 contains the five major digital libraries used.

Table 1. Systematic mapping study electronic databases

Electronic databases	URL
ACM	http://dl.acm.org/
IEEE	http://ieeexplore.ieee.org/xplore
SCIENCE DIRECT	http://www.sciencedirect.com/
SPRINGER	http;//www.springerlink.com/
SCOPUS	https://www.scopus.com/

This study's search query was fashioned with regards to population intervention comparisons and their results. Exploration keywords were extracted from this study's title structure. The query utilized is as follows:

(TITLE (security AND trust) OR TITLE (trust AND privacy) OR TITLE (privacy AND security) OR TITLE (privacy AND trust AND security)) AND TITLE (cloud).

The search for primary studies was conducted using the custom query above, for document metadata. For this study on security, trust, and privacy; all the search results out of the five chosen digital repositories relating to cloud computing and computer sciences were utilized. The criteria for selection for our papers, as depicted by the prerequisites of the research destination and questions, led to the consideration of 115 publications as relevant to this study, out of an introductory interest containing 1670 publications. This period covered in this study was from 2010 through 2018.

3.4. Screening of papers for inclusion and exclusion

The objective of the selection criteria was the location and inclusion of all publications which were necessary for the successful conduct of the study. Criteria for Inclusion and exclusion were utilized in the elimination of all articles that did not meet the focus of the study. Also, publications that were irrelevant to the search queries were eliminated. Some abstracts contained relevant but insufficient information, therefore, such were excluded. This study also omitted prefaces, presentation slides, tutorials, briefs, summaries, editorials and panel discussions. The focus of this study was security, trust and privacy; the inclusion and exclusion criteria are as indicated in Table 2.

Table 2. Inclusion and exclusion criteria

Criteria for inclusion	Criteria for exclusion
Abstract clearly discusses trust, privacy and security.	The abstract does not fall within the cloud computing domain.
Also, the discussion is in cloud computing or related field.	Cloud security, trust or privacy is not discussed by the abstract.

3.5. Abstracts keywording

Abstract keywording is a significant portion of a systematic mapping study. The keywording of abstracts improves the composition of the scheme for classification. The systematic mapping process is used for the development of this scheme. Keywording was critical in reducing the time used to evolve a classification scheme. An analysis of themes, which aimed at the identification, analyses and reporting of topics within the domain being considered, was used for the classification scheme building [35]. During the keywording of abstracts, concepts, main contributions and the domains of focus which showed the identified research questions, were identified from the abstracts of selected papers. A significant quantity of concepts and methods were identified during from the chosen studies that addressed cloud security, privacy and trust. Subsequently, keyword choice for the classification scheme preparation is enabled via this process. According to the thematic analysis approach which was utilized in the structuring of a significant degree of understanding of the research, a keyword combination was extracted from the various studies. The keywording process included examining the abstracts of primary studies to extricate ideas and keyword in line with the field of study. This also involved knowing the context of the study. After extracting the concepts and keywords, they were gathered to give needed understanding into the various categories and contribution

of the articles. The process discussed above was utilized to evolve the scheme of classification for this study and the following categories used in this study.

However, it was sometimes necessary to go beyond the abstracts of the articles thereby looking at introductions and conclusions of such articles to guarantee the selection of reliable keywords for all attached papers. A keyword cluster was utilized to develop the classes of this study which was eventually used for the systematic map creation. Three facets were utilized for this paper on cloud security, trust and privacy. The first was the topic category; these are the topic extracted in the form of concepts and keywords with the classification process. The second was the contribution facet; these constitute the type of contribution to the study in the form of metrics, method, model, process and tool as enunciated in [10]. The third was related to the type of research that was carried out

3.6. Research facet with categories and description

The research facet made up the third category of this study. The classification of research approach discussed in [36] was used for the research facet. The approach includes the following categories and descriptions [36].

a. Validation research: the techniques utilized are distinct, though not executed yet. They are found at their trial stages.
b. Evaluation research: The procedures have been executed and evaluated; the results as far as upsides and downsides, are available
c. Solution proposal: The procedures involved provide uncommon solutions to problems. The applications of their advantages are also available.
d. Philosophical papers: The techniques suggest a different method of tackling issues regarding ideas and structures
e. Opinion papers: The techniques do not rely on existing research methodology; they merely express the viewpoint of their authors.
f. Experience papers: These reports state the individual encounters of the authors. They indicate how solutions were established

This research classification approach was determined to be sufficient and ideal for this study. It was relevant to the classification scheme. Therefore, all the primary studies were examined with respect to the various classes and depictions of the approaches to research classification. The result of these activities was used as the research class for this investigation.

3.7. Data extraction and mapping studies

As part of the systematic mapping process, appropriate publications are arranged according to classification schemes. This is a subset of the classification phase. This stage was utilized for data extraction from different articles added to the study. The extraction processes determined the results of the scheme of classification. New classes were included as a result of the process, some old ones were joined to form new ones, and those that were determined to be irrelevant, were expunged. This process was done using a Spreadsheet from Microsoft Excel. There was a table in the spreadsheet that contained every class within the scheme of classification. After that, the occurrences of publication topics within the spreadsheet tables were integrated into individual tables that contained either the topic/contribution or topic/research issues. The focus of the analyses was the presentation of paper frequencies as a result of the outcomes from the spreadsheet. The aim was to see the portions of security, trust and privacy in the cloud that had more emphasis placed on. This revealed gaps or shortages in publications, creating a focus on areas requiring further studies. Based on the result obtained on the spreadsheet tables, a systematic map was created using the occurrences presented via a bubbles plot. This map involved an x-y scatter plot with bubbles where the categories intersected. The coordinate values of the scatter plot had bubble sizes which corresponded to the volume of papers within individual classes. There were two quadrants because of the three facets that were utilized during this entire process. A visual map was provided within every category, as a result of the study's focus. These maps were as a result of the occurrences of various topic categories that fell under either the contribution or research categories; as a result, simultaneous consideration of the various facets was simplified. Also, there was an inclusion of statistics summary, thereby providing clarity. In summary, a glimpse into the entire happenings in security, trust, and privacy in the cloud, is provided by the systematic map.

4. RESULTS AND DISCUSSION

This systematic mapping study of cloud security, trust, and privacy focused on an analysis of themes and classification. Sometimes it may be necessary to identify publications. Gaps were identified from the

analysis, by graphing using bubbles plots; this showed which aspect of the study had a shortage of publication. Also, the study showed areas that were covered adequately with regards to papers. In this systematic mapping study, various significant classifications were employed during the paper assessment. This assessment was then used to identify the frequencies of the paper categories and was then used for the map creation.

4.1. Topic and contribution facet

The contribution facet focuses on discussions within the following domains [24]:
−   Framework: This deals with a properly designed and itemized method that contains broad scope and purpose, and which focuses on several research questions or domains
−   Model: An abstraction view of a topic and challenges, instead of a concrete and distinct approach for solving the specific problem is provided
−   Tool: Concept evaluation using a particular tool is provided
−   Evaluation: A method for the empirical measurement of the proposed solution(s)
−   Metric: Frameworks for specific phenomena measurement is provided
−   Method: A specific objective with a restricted research question or purpose is focused on

The main category of this study, the topics category, had the following topics extracted during the cloud computing security, trust and privacy classification scheme:
−   Privacy issues and challenges
−   Frameworks
−   Cloud trust
−   Techniques
−   Design
−   Data security

The listing of primary studies which were utilized for topics checking purposes viz-a-viz the various categories of contributions is in Table 3. Additionally, Figure 2 is a chart of the percentage of topics in the contribution category. The contribution category or facet showed the various types of input made to the study's focus. The outcome showed that documents which reviewed models regarding cloud security, trust and privacy was 35.24% out of 105 papers within this category. Also, metric had 7.62%, tool had 19.05%, method had 18.1%, and process had 20%. Papers that discussed model contribution were 35.24% of the reviewed work in this facet. The distribution indicates that 10.48% of model contribution was on privacy issues and challenges. Another 10.48% was on the framework. Models contributed 0.95% each to cloud trust and techniques, models contributed 12.38% to the topics on design, and there was no contribution by model to data security.

Table 3. Primary studies for topic and contribution facet

| Contribution facet \ topic	Metric	Tool	Model	Method	Process
Privacy Issues and Challenges	42, 43, 61, 62, 69	72	1, 4, 6, 77, 79, 81, 96, 98, 102, 108, 113	63	19, 21, 22, 39, 41, 82, 86, 90, 93
Frameworks		10, 46, 48, 60	25, 27, 28, 33, 38, 65, 71, 74, 87, 92, 95		2, 101, 114
Cloud Trust		9, 12, 18, 26, 30, 36, 47, 49, 52	110	53, 73, 75, 83, 104,	
Techniques		5, 88	111	16, 20, 24, 50, 89, 91, 99	31, 32, 35, 84, 105, 106, 107
Design	51, 78	64, 67, 103, 109	7, 11, 23, 40, 44, 45, 55, 56, 57, 59, 70, 76, 100	85, 94, 97	
Data Security	80				17, 15,
Percentage	36.52%	27.83%	19.13%	6.96%	9.57%
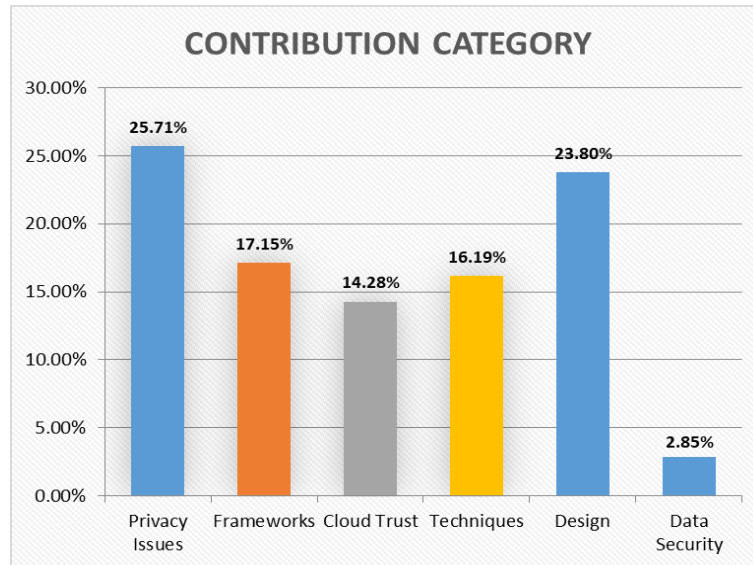
Figure 2. Percentage of topics in the contribution category

4.2. Topic and research facet

Table 4 contains the primary studies list used for the examination of the various topics against the types of research. Figure 3 contains the chart showing the percentage of topics in the research category. The outcome of the research category performed on cloud computing security, trust and privacy, is found on the x-axis of the right quadrant of Figure 4. The outcome shows that papers that were based on evaluation research were 36.52% of 115 papers in this category. Furthermore, validation research had 27.83%; solution had 19.13%; philosophical had 6.96%; experience had 9.57%, and there were no opinions on this study.

The discussion of valuation research made up 36.52% of the publications on cloud computing security, trust and privacy that were reviewed. The rundown indicates that 10.35% of the discussion on evaluation research focused on privacy issues and challenges, 6.96% considered framework, 5.09% was on cloud trust, 5.22% focused on techniques, 7.83% dealt with design and there were no papers on data security. Figure 4 shows the aspects of the various research topics and facets that are remaining.
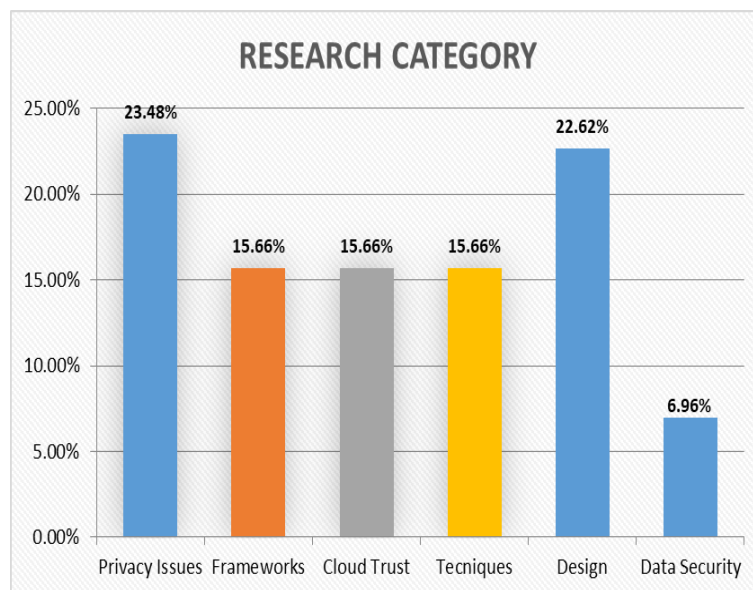

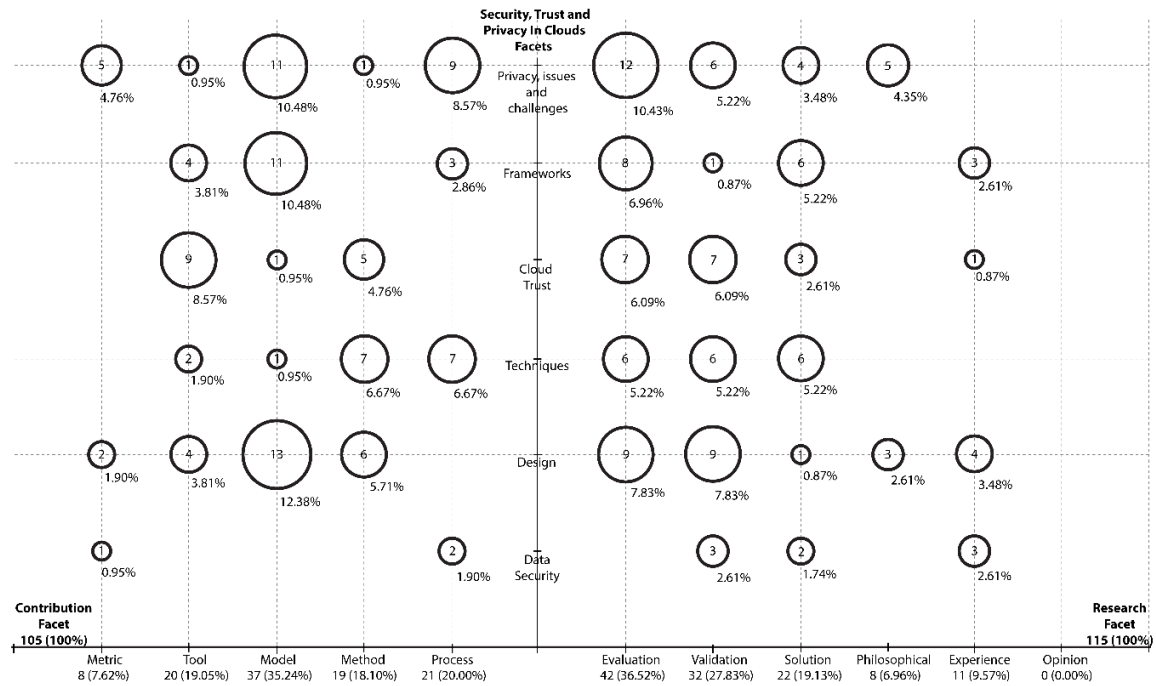Figure 3. Percentage of topics in the research category

Figure 4. Bubble map on cloud security, trust, and privacy

Table 4. Primary studies for topic and research facet

Research Facet Topic	Evaluation	Validation	Solution	Philosophical	Experience	Opinion
Privacy Issues and Challenges	1, 6, 19, 21, 22, 39, 93, 96, 98, 102, 108, 113	41, 42, 43, 61, 62, 63,	4, 69, 72, 77,	79, 81, 82, 86, 90		
Frameworks	28, 33, 38, 46, 65, 74, 101, 114,	71	2, 25, 27, 92, 87, 95		10, 48, 60	
Cloud Trust	3, 26, 73, 75, 104, 110, 112	9, 12, 18, 36, 47, 83, 115	30, 49, 53		52	
Techniques	5, 32, 84, 91, 99, 106,	14, 16, 88, 89, 105, 107,	20, 24, 31, 35, 50, 111,			
Design	7, 34, 40, 51, 54, 55, 58, 64, 78	11, 44, 45, 67, 76, 94, 97,103, 109	70	56, 57, 85	23, 59, 66, 100	
Data Security		13, 17, 15	8, 68		29, 37, 80,	
Percentage	36.52%	27.83%	19.13%	6.96%	9.57%	0.00%

4.3. Main findings

Two x-y scatter plots containing bubbles where the intersections of the topic and contribution facets lie, are contained within the first quadrant in Figure 4. The second quadrant of Figure 4 displays a visual representation of the topic and research facet intersection, via a two x-y scatter plot containing bubbles. As mentioned earlier, an identification of which category had been emphasized more during the study is made possible via the analysis.

a. From the first quadrant, it was shown that numerous publications regarding privacy issues and challenges existed within the domain of metric with 4.76%; others on cloud trust within the domain of tool were 8.75% of the total number of publications; also, additional publications on design within the domain of model constituted 12.38% of the publications; more articles on technics within the domain of method made up 6.67%; and other publications on privacy issues and challenges in the area of process with 8.57%.

b. From the second quadrant of Figure 4, articles were published on privacy issues and challenges within the domain of evaluation research with 10.43%; some publications on design concerning validation research

made up 7.83%; other publications on frameworks and techniques within solution research domain with 5.22% each; and more articles published on privacy issues and challenges in respect to philosophical research.

c. On the other hand, the domain of techniques had the least number of publications for validation research at 0.87%, and the lowest number of design in solution research was 0.87%. Also, no publications were found on data security with respect to evaluation research; there were no publications identified on frameworks, cloud trust, techniques and data security in terms of philosophical research. No papers were seen on privacy issues and challenges and techniques on experience research. There were no opinions on all aspect of the study on security, trust and privacy in clouds.

d. Furthermore, there were no publications on frameworks, cloud, trust and techniques in the area of metric. No articles were identified regarding data security with respect to tool and model. Also, no articles were identified for framework and data security. Finally, no papers were published on cloud trust and design in the area of process.

The aesthetics of systematic maps makes them signifies their usefulness, and they can quickly pique readers' interests. This usefulness is because the systematic maps help to summarize result and offer them to researchers by combining the categories on the systematic map. Also, it allows simultaneous views of both sides of the map. Gaps within domains of interest are easily identified when a systematic mapping study is combined alongside a successive systematic literature review. However, standalone systematic mapping studies are unique in their own rights.

The systematic map is useful because researchers at all levels and practitioners in various industries can utilize the information presented as a Launchpad for further research. Cloud Computing security, trust and privacy related topic classes considering privacy issues and challenges, frameworks, cloud trust, and data security were provided by this study. Furthermore, a discussion of these study classes can be reviewed based on either tool, model, method, metric, and process, or evaluation, validation, solution, philosophical, or opinion research. Therefore, further research is recommended on them. The primary studies list that is provided can further guide future researchers. This study shows the inexhaustible and continuous nature of research work.

5.   CONCLUSION

Cloud computing is evolving at a dynamic rate. More resources are being made available to the users by the cloud providers. This rate of evolution, in turn, is encouraging more individuals and organization alike to utilize cloud resources. Such kind of interactions will require adequate security, privacy and trust on the part of CSPs. This has informed lots of research in privacy, security and trust in the cloud. Despite the numerous publications available, there are shortages in some areas pointed out with the use of bubble plots; hence revealing some research gaps in this field of study. Some aspects, where inadequate emphasis had been placed on previously, regarding cloud security, privacy and trust, were identified by this study as a result of the classifications used within the scheme. This paper contributes to knowledge through its indication of the various portions of the study where shortcomings were found. These identified gaps and shortcomings indicate the need for further research. They should serve as a general signpost for topics where more research can be conducted on, in areas of security, privacy and trust in the cloud. This study could also be further validated, and contradictory items resolved through additional research. In conclusion, a systematic map of cloud security, privacy and trust, which could be of immense benefits to the cloud community is created via this study. The study should support researchers in unveiling the major shortcomings of cloud security, privacy and trust that previous researchers have not had the opportunity of exploring. Thus, contributing to cloud computing knowledge.

ACKNOWLEDGMENT

REFERENCES

[1]   R. Buyya, C. S. Yeo, S. venugopal, J, Brobeg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype and reality for delivering computing as the 5th utility," *Future generation computer system*, vol. 25, no. 6, pp. 599-616, 2009, doi: 10.1016/j.future.2008.12.001.

[2]   Isaac Odun-Ayo and B. Ehi, "Cloud Trust Management - Issues and Developments," in *Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science*, San Francisco, USA, 2018, vol. 1, pp. 369-374.

[3]   I. Odun-Ayo, B. Odede, and R. Ahuja, "Cloud Management Optimization - Issues and Developments," *International Conference on Computational Science and Its Applications.* Springer, Cham, San Francisco, USA, 2018, pp. 357-362, doi: 10.1007/978-3-319-95171-3_54.

[4]   T. Abayomi-Zannu and I. Odun-Ayo, "Cloud Identity Management-A Critical Analysis," Lecture Notes in *Engineering and Computer Science: Proceedings of the International Multi Conference of Engineers and Computer Scientists 2019 IMECS 2019*, Hong Kong, 2019, pp. 170-175.

[5]   V. Jain and V. Sharma, "Survey and analyzing security challenges and privacy in cloud computing," *International journal of computer science and information technology and security*, vol. 3, no 5, pp. 316-321, 2013.

[6]   Prasanna Balasooriya, Santoso Wibowo, and Marilyn Wells Mobile and wireless technology "Data security and privacy in the cloud: Driving to the next era of technology with confidence", 2017.

[7]   J. Ayoade, "Enhancing cloud computing with security trust model," *Asia Pacific Journal of Contemporary Education and Communication Technology (APJCECT)*, vol. 3, no. 1, 2017.

[8]   A. Glolami and E. Laure, "Security and privacy of sensitive data in cloud computing: A survey of recent developments," *David C. Wyldetal (Eds): NETSOM, NCS, WIMONI, CSELT, SPM-2015,* pp. 131-150, 2015, doi: 10.5121/csit.2015.51611.

[9]   S. A. Hameed, A. Nirabi, M. H. Habaebi, A. Haddad, "Application of mobile cloud computing in emergency health care," *Bulletin of Electrical Engineering and Informatics (BEEI)* , vol. 8, no. 3, pp. 1088-1095, 2019.

[10]   N. Chandrakala and B. T. Rao, "Migration of Virtual Machine to improve the Security in Cloud Computing," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 1, pp. 210-219, 2018, doi: 10.11591/ijece.v8i1.pp210-219.

[11]   S. Bhatia, and J. Malhotra, "CSPCR: Cloud Security, Privacy and Compliance Readiness-A Trustworthy Framework," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 5, pp. 3756-3766, 2018, doi: 10.11591/ijece.v8i5.pp3756-3766.

[12]   R. Ganiga, R. M. Pai, M. M. P. Manohara, and R. K. Sinha, "Security framework for cloud based Electronic Health Record (EHR) system," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 455-466, 2020, doi: 10.11591/ijece.v10i1.pp455-466.

[13]   Y. K. Kumar, and R. M. Shafi, "An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem", *International Journal of Electrical and Computer Engineering*, vol.10, no.1, pp. 530-537, 2020, doi: 10.11591/ijece.v10i1.pp530-537.

[14]   K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Information and Software Technology*, vol. 64, pp. 1-18, 2015, doi: 10.1016/j.infsof.2015.03.007.

[15]   T. Kosar, S. Bohra, and M. Mernik, "Protocol of a systematic mapping study for domain-specific languages," *Journal of Information and Software Technology 21(C).* pp. 77-91, 2016.

[16]   I. Odun-Ayo, R. Goddy-Worlu, J. Yahaya, and V. Geteloma, "A systematic mapping study of cloud policy languages and programming models," *Journal of King Saud University–Computer and Information Sciences*, 2019, doi: 10.1016/j.jksuci.2019.05.003.

[17]   C. R. Fernandez-Blanco, F. Careri, K. Kavvadias, I. H. Gonzalez, A. Zucker, and E. Peteves, "Systematic mapping of power system models: Expert survey," EUR 28875 EN, *Publications Office of the European Union*, Luxembourg, 2019, doi:10.2760/422399, JRC109123, 2017.

[18]   C. Griffo, J. P. A. Almeida, and G. Guizzardi, "A systematic mapping of the literature on legal core ontologies," in *Brazilian Conference on Ontologies, ONTOBRAS 15, CEUR Workshop Proceedings*, 1442, 2015.

[19]   I. Odun-Ayo, V. Geteloma, I. Eweoya, and R. Ahuja, "Virtualization, Containerization, Composition, and Orchestration of Cloud Computing Services," In *International Conference on Computational Science and Its Applications*, Springer, Cham, 2019, pp. 402-417.

[20]   M. Alavi and D. E. Leidner, "Knowledge management and knowledge management systems: Conceptual foundations and research issues," *MIS Quarterly*, vol. 25, no. 1, pp. 107-136, 2001, doi: 10.2307/3250961.

[21]   I. Odun-Ayo, R. Goddy-Worlu, V. Samuel, and V. Geteloma, "Cloud Design and Deployment Models: A Systematic Mapping Study," *BMC Research Notes*, vol. 12, no. 1, p. 436, doi: 10.1186/s13104-019-4474-y.

[22]   S. K. Boell and D. Cecez-Kecmanovic, "On being 'Systematic' in literature reviews," in *Formulating Research Methods for Information Systems*, pp. 48-78, 2015, doi: 10.1057/9781137509888_3.

[23]   P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, vol 80, no. 4, pp. 571-583, 2007, doi: 10.1016/j.jss.2006.07.009.

[24]   B. I. Ya'u, N. Salleh, A. Nordin, N. B. Idris, H. Abas, and A. A. Alwan, "A systematic mapping study on cloud-based mobile application testing," *Journal of Information and Communication Technology*, vol. 18, no. 4, pp. 485-527, 2019, doi: 10.32890/jict2019.18.4.5.

[25]   H. M. Cooper, "Scientific guidelines for conducting integrative research reviews," *Review of educational research*, pp. 291-302, 1982.

[26]   J. L. Galvan and M. C. Galvan, "Writing literature reviews: A guide for students of the social and behavioral sciences," *Routledge*, 2017

[27]   B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and, S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Information and Software Technology*, vol. 51, vol. 1, pp. 7-15, 2009, doi: 10.1016/j.infsof.2008.09.009.

[28]   I. Odun-Ayo, G. W. Rowland, B. Sherrene, And G. Victor, "A Systematic Mapping Study of mobile and Efficient use of cloud," *ICIC express letters. Part B, Applications : an international journal of research and surveys*, vol. 10, no. 9, pp. 797-804, 2019.

[29]   J. Vom, Brocke, A. Simons, K. Riemer, B. Niehaves, R. Plattfaut, and A. Cleven, "Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search," in *Information Systems Research, CAIS*, vol. 37, p. 9, 2015, doi: 10.17705/1CAIS.03709.

[30]   S. M. Rosli, M. M. Rosli, and R. Nordin, "A mapping study on blood glucose recommender system for patients with gestational diabetes mellitus," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 4, pp. 1489-1495, 2019, doi: 10.11591/eei.v8i4.1633.

[31]   Y. Yan, H. Xiahong and W. Wanjun, "Location-Based Services and Privacy Protection under Mobile Cloud Computing*," Bulletin of Electrical Engineering and Informatics*, vol. 4, no. 4, pp. 345-354, 2015.

[32]   K. S. Gururaj and K. Thippeswamy, "Cloud based secured framework for implementation of online voting system," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 1, pp. 328-335, 2019, doi: 10.11591/ijeecs.v15.i1.pp328-335.

[33]   A. B. Muhammad and M. Ali Babar, "A systematic mapping study of software architectures for cloud-based systems," *Software system section*, IT University of Copenhagen. 2014.

[34]   C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," In *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, pp. 1-10, 2014, doi: 10.1145/2601248.2601268.

[35]   V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77-101, 2006, doi: 10.1191/1478088706qp063oa.

[36]   R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirement engineering paper classification and evaluation criteria: A proposal and a discussion," *Requirement engineering*, vol. 11, no. 1, pp. 102-10, 2006, doi: 10.1007/s00766-005-0021-6.

BIOGRAPHIES OF AUTHORS

Isaac A. Odun-Ayo was born in Ilesha, Nigeria in 1962. He received the BS, MS and Ph.D degrees in Computer Science from the University of Benin, Benin City, Nigeria. Between 2010 and 2013 he was a faculty and Director Information and Communication Technology at the National Defence College, Abuja, Nigeria. He joined the faculty of Covenant University, Ota, Nigeria as a Senior Lecturer in October 2016. He is the author of one book and more than 40 journal and conference articles in Cloud Computing. His research interests include cloud computing, human resource management, e-governance and software engineering. Dr. Odun-Ayo is a recipient of the National Productivity Order of Merit Award, Nigeria for his contribution to computing. He is a member of the Nigeria Computer Society (NCS), Computer Professionals of Nigeria (CPN), International Association of Engineers (IAENG), Institute of Electrical and Electronics Engineers (IEEE) and Member Information Science Institute (ISI).

Oladapo A. Alagbe is a research assistant and a postgraduate student at the Department of Computer and Information Sciences, Covenant University, with a focus on Management and Information Systems. He received a B.Tech in Computer Science from Ladoke Akintola University of Technology (LAUTECH), Ogbomosho. He is passionate about Mobile, Fog and Cloud Computing, Cyber Security and how they affect organizatons

Jamaiah Yahaya is Associate Professor at Faculty of Information Science and Technology (FTSM), The National University of Malaysia (UKM) since July 2011. Prior that she worked as a senior lecturer in School of Computing, Northern University of Malaysia (UUM) and a system analyst at University of Science Malaysia. Her bachelor degree was BSc in Computer Science and Mathematics from University of Wisconsin-La Crosse, USA (1986), MSc in Information System from University of Leeds, UK (1998), and PhD in Computer Science from The National University of Malaysia (UKM) (2007). Her PhD thesis was the development of software certification model, and later, she continued her PhD research as a post-doctoral fellow in UKM (2008). Currently, she is the head of the PhD program in FTSM, UKM. Her research interests are software quality, software development and management, and software assessment and impact. She is an active researcher with more than 100 publications in international journals and proceedings for the last five years.